

# Passport Fraud:

are you who you say you are?



*So, are you who you say you are? Most likely you are, but what if you're not? More importantly, does it matter and what are the implications for airports, airlines and their employees? The introduction of biometric passports would indicate that most governments regard passport fraud as a very serious issue. Immigration authorities and Passport agencies worldwide are allocating significant resources to reducing the number of travel documents obtained with falsified identification, as well as detecting those forged after the fact.*

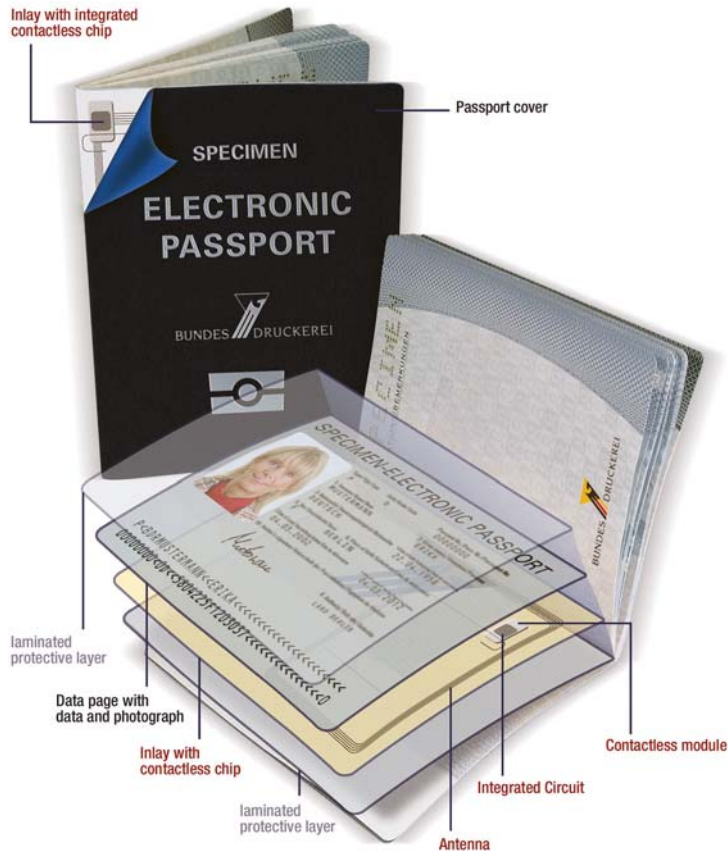
**Marcia Adair** reports.

**W**ith the advent of watermarks, holograms and other security features, it has become quite difficult to create passports from scratch. The next best method is to alter an existing document stolen from a tourist or bought on the black market. On older passports, the laminated photograph can be changed relatively easily by someone with the right equipment and a steady hand. The introduction of digitized photographs and biometrics, however, means forgery now requires specialist skills.

## **Biometric Passports**

Immigration departments around the globe, in the hope of greatly reducing passport fraud, have enthusiastically adopted biometric passports. The technology is still new and there are real limits to a biometric passport's actual usefulness, particularly when relying solely on the International Civil Aviation Organisation (ICAO) standard of facial recognition. Nevertheless, it is a significant step forward in the detection of forgeries.

In March 1998, Malaysia became the first country to use biometric information in its passports. As technology advanced and new security policies were developed, other countries considered adopting biometric identity documents. However, it wasn't until 2006 that the idea really became an international priority. The American Department of Immigration not only took the decision to include biometric information on all passports issued after 14th August 2006, but also compelled any of the twenty-seven selected countries that wished to remain part of the Visa Waiver Program to do the same. The new passports are machine readable and compliant with international standards as set out by the ICAO.



Source: Bundesdruckerei GmbH

► The contactless chip can be integrated into either the cover page or the data page.

A biometric passport is nearly identical to the previous passport design except for a small symbol on the front cover and a chip inserted on the inside back cover. The chip is non-contact, meaning it is read via radio waves, rather than requiring actual physical contact with the reader. This method of reading the passport has been the subject of much debate regarding its security, particularly in Europe where laws protecting a person's personal information are far more rigorous than in the United States.

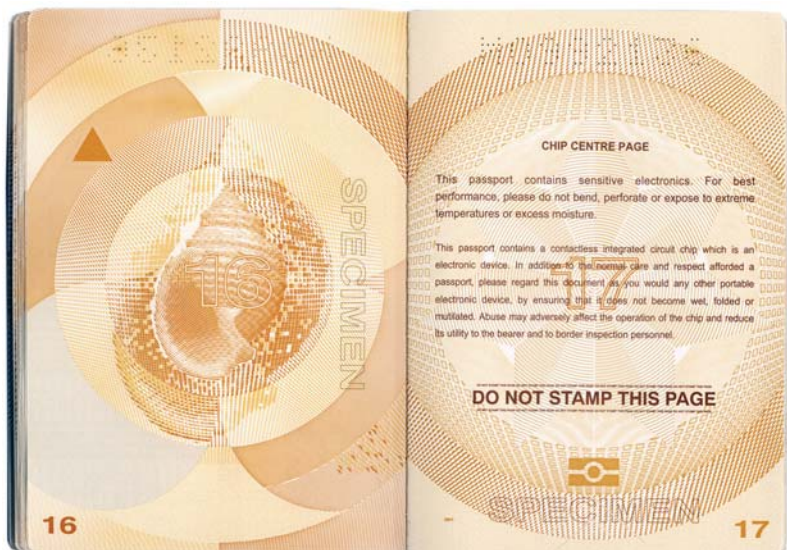
Digital encryption technology, called Public Key Infrastructure (PKI) in Britain, is used to prevent the encoded data from being altered, in much the same way that wireless internet users protect their network with a security key. The strength of this technology varies from country to country, even within Europe.

The Dutch biometric passport was cracked on 28th July 2005 just a few months after it was introduced, because the encryption key used sequential numbers and was

therefore not sufficiently random. Although it has not been tried in practice, theoretically, the biometric data on a Dutch passport can be read from up to 10 metres, stored and then decoded on a computer in less than two hours. The Dutch government has

since updated its technology to improve the integrity of its documents. American and British passports use a much stronger encryption method that has yet to be cracked. American passports also feature a mesh inside the covers intended to interfere with any unauthorised reading or skimming of personal information. Irish passports go one step further and require the machine readable zone (MRZ) to be scanned first in order to unlock the chip for reading.

Several manufacturers, including Adaptive Recognition Systems, Rochford Thompson and IPM International, provide readers to airports and other border control sites. The units are capable of being integrated into kiosks, e-Gates and self-service check-in desks. All are easily updatable to accommodate any technological or biometric enhancements such as fingerprints or iris scans. UV and IR illumination is also available to enable the detection of invisible security features such as watermarks. The Multi Reader manufactured by Adaptive Recognition is able to accommodate RFID technology, which requires the MRZ to be read in order to unlock the biometric information. Rochford Thompson has a separate module available that attaches via USB to its RTE8000 passport reader in order to enable RFID documents to be read. IPM's Read & Go machine functions similarly and allows biometric



Australian ePassport

passports to be checked without burdening security personnel or increasing passenger wait time.

## How To Get A Fake Passport

The preferred method of forging passports involves acquiring blanks from passport offices, consulates, embassies or, in Europe, from town halls. Once these are sourced, it is a simple matter of entering the correct information and inserting the appropriate photograph. It is more difficult than in years past but still relatively simple work for an experienced professional. The European practice of keeping blank passports in provincial town halls has resulted in a great many Belgian and Italian documents being stolen; Belgium has since centralised its passport offices to prevent this.

European passports are particularly coveted and command a very high price on the black market because their bearers can travel throughout the Western world without needing visas. This is why the United States required other nations to adopt biometric passports if they wished to remain on the non-visa list.

If forgery is not an option, it is possible to purchase passports issued by countries that no longer exist. The legal responsibility for a passport's legitimacy lies with the country that issues it and a few companies

have taken advantage of this loophole to sell documents from such non-existent countries as Rhodesia, Zanzibar, the British West Indies, Burma or Dutch Guiana. Privacy World, a Japanese company, also provides fake drivers licenses and gym memberships to further support the false identity. Camouflage passports, as they titled, are ostensibly for those that travel to countries where the possession of a Western passport is troublesome. The owner's real name and photograph are used and although they are instructed not to use the documents at border crossings, it is not too much of a stretch to imagine a harried immigration officer being fooled. To ensure authenticity, the passport contains various visas, entry/exit stamps and security holograms.

The major problem with biometric passports, aside from security issues, is that they do nothing to counter legitimate passports being obtained with false supporting documents. It is relatively straightforward for those that are familiar with the process and requires less specialised forgery skills than altering an existing document.

Most Western countries rely on the birth certificate, a weak document that is easily forged, to prove identity for other official documents. Once a person has acquired a false birth certificate, a driver's license, social security/national insurance number and various other forms of identification are within reach. These documents are then used to validate identity on the passport application.

This method of acquiring a passport is perhaps the most worrying for immigration and border control officials because it is so difficult to detect and there is no practical solution to combat it. Strengthening the feeder documents such as birth certificate or driver's license would require a whole-scale reform of the identity system from the ground up. It would cost billions, take years to complete and address the activities of a miniscule part of the overall population.

When expressed as a percentage, the number of fraudulent passports issued each year is negligible. When looking at what a small percentage equates to in hard numbers, the size of the problem appears more significant. In the United

Camouflage Name	Real Name
British Guiana	Guyana
British Honduras	Belize
British Hong Kong	Hong Kong
British West Indies	Does not exist
Burma	Myanma
Dutch Guiana	Surinam
Eastern Samoa	American Samoa
Netherlands East Indies	Indonesia
New Grenada	Does not exist, although Grenada does
New Hebrides	Vanuatu
Rhodesia	(Republic of) Zimbabwe
South Vietnam	Vietnam
Spanish Guinea	Equatorial Guinea
U.S.S.R.	Now known as the SNG countries
Zanzibar	Amalgamated with Tanganyika to become Tanzania. Exists but does not issue passports

## Passport and travel document readers

Automatically verify the visual and MRZ zones whilst also checking the authenticity of a travel document.

- Reveals features with UV, IR, white & coaxial light
- Identifies and compares MRZ, RFID & visual zones
- Portable or desktop authentication
- Library of passports and travel documents
- Details of 1400 International travel documents
- SDK available for integration with third party systems



tssi

Tel: +44 1793 747 700  
 Fax: +44 1793 747 701  
 Email: sales@tssi.co.uk  
 Web: www.tssi.co.uk

Kingdom, where some 6.6 millions passports are issued every year, the estimated number of passports fraudulently obtained ranges between 10,000 and 33,000 depending on who one asks. In 2006, the British Home Office admitted that they are only able to catch about half of the falsified applications during the screening process. To help combat this, they introduced face-to-face interviews for first-time applicants in May 2007. Applicants are expected to know the answers to a pool of nearly 200 personal questions about their previous addresses, financial history and ancestry.

## Who Uses Forged Passports?

Those prone to conclusion jumping would say that there may now be 33,000 additional terrorists in possession of newly minted UK passports. While this alarmist attitude is clearly ridiculous, it does illustrate one of the central problems of airport security and personal identity, namely the imperfect relationship between false documents and illegal activity.

The following two statements are reminiscent of high school logic problems but sum up the difficulties facing security personnel and policy makers.

- Not all travellers using false documents are criminals.
- Not all criminals use false documents.

While it is certainly true that those involved in drug smuggling, money laundering, social security fraud and terrorism use forged passports regularly, it is also common for those claiming asylum to resort to false documents as well. Customs and

immigration officials in major migration centres such as New York and London are quite used to seeing forged passports in these cases. There have been cases where criminals have taken advantage of the asylum system to take up residence in a Western country under false pretences, particularly in Canada where immigration laws are more lax than in the UK or America.

Ahmed Rasan's Millennium Plot to bomb Los Angeles International Airport in December of 1999 is a classic case. The Algerian entered Canada in 1994 with a false French passport and declared political asylum. He supported himself over the next four years by drawing benefits from the Canadian government and stealing documents, credit cards and cash from tourists. During this time, he became an expert in forging identity documents and provided them to fellow Algerians involved in al Qaeda terrorist activities. He travelled to Afghanistan in 1998 to receive training from the Taliban and returned to Canada early in 1999 with supplies, money and instructions. Rasan was arrested on 12th December 1999 in Port Angeles, Washington when customs officers found explosives in the trunk of his car. He was on his way to Los Angeles from Canada to carry out the airport mission.

Even the tragic events of 11th September 2001 illustrate the need for effective immigration controls by Western governments and, indeed, those elsewhere. Of the 19 hijackers, six were using false names and false Saudi Arabian passports, three had overstayed their visas, two had entered on student visas and had not turned up to class and two were already on existing FBI terrorist watch

lists but not discovered in time.

Saudi Arabian passports were chosen on purpose because, although a visa was required for entry, the country's friendly relationship with America means that very little suspicion would have been roused.

Those who deal in false documents are extraordinarily clever and know exactly how to work the system. Overstaying a business or tourism visa is also a common occurrence. The United States Citizenship and Immigration Service estimates that nearly 2 million people are in the country on overstayed visas. Again, most of these people are not criminals or planning terrorist activity but, invariably, some are. The sheer number means it is impossible to locate and deport each person. Student visas are problematic in the same way. A staggering number are issued each year and once a person enters a country, it is very difficult for the government to keep track of them. Immigration departments simply don't have the resources to find people and put them on planes.

Ultimate security means that every passport is checked by a forgery expert to ensure that each one is legitimate and every passenger is thoroughly searched. This scenario, of course, does not take into account legitimate passports acquired with false documents, which are nearly impossible to detect. Ultimate expediency means there are no restricted areas of the airport or security checkpoints. Neither goal is practical and finding an acceptable meeting point between the two is one of the great security dilemmas. With 30 million overseas visitors entering the United States every year and nearly 20 million passengers going through London Heathrow alone, it is a case of balancing risk with convenience. Biometric passports do help and can be made better if the inadequacies of facial recognition software and personal privacy are addressed. The overwhelming majority of people are who they say they are but it is those few that aren't that keep security businesses and governments searching for the next solution.



A passport reader

*The author is a freelance journalist.*