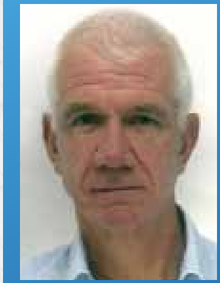
Surplus to requirements

Will passport chips replace security features?

by Tony Dean

The first electronic passports were issued more than eight years ago. Many thought that the introduction of e-Passports would signal the demise of traditional security features, as the RFID chip would contain all the biometric information needed to authenticate the identity of travellers. In this article, Tony Dean discusses whether this has proved to be the case and if not, what has changed.



***Tony Dean** served with the UK Immigration Service for 10 years, five of which were in the National Document Fraud Unit (NDFU) as an advisor to UK Government departments on document security. In 2005 he joined the UK Passport Office to take responsibility for the design and introduction of new identity documents for the United Kingdom. In 2013, he joined De La Rue to work within their identity management business providing technical support to new passport and identity projects.*

Background

Since 2010 it has been a requirement for all ICAO Member States to issue machine readable passports (MRPs) compliant to International Civil Aviation Organization Document 9303, in which the standards for identity documents are defined[1]. Most States have met this requirement, but for the remaining few that have not, ICAO and its working groups are offering every assistance and technical support to remedy this as soon as possible. In addition, more than 100 Member States have already moved on from MRPs to e-Passports and many more are currently in the process of upgrading (figure 1).

The first machine readable passports were introduced in the 1980's and whilst most States have been issuing them for years, many have still yet to introduce the facilities to read them. Some experts see the chip, in some form or other, being the future for passports whilst others see it as just an additional security feature. If history repeats itself it will be many more years before we see readers being employed to read e-Passports at most border posts, so in these circumstances it may not even become a security feature.

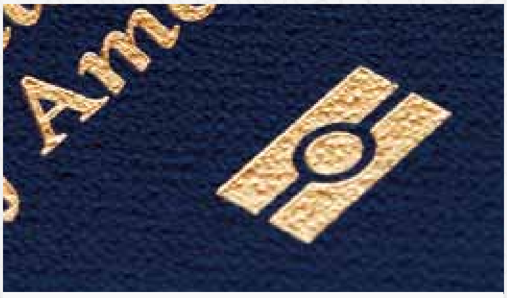


Figure 1
'Chip inside' logo on a passport cover.

Once readers are installed there is a risk that if too many chips fail to read, immigration officers may start to disregard this feature. It is therefore important that States continue to ensure that chips are sufficiently protected and tested, so that they last the life of the passport, just as is done with all other physical and printed security features.

Of those States that have installed e-Passport readers, the majority are not making the most of the security that can be achieved. So long as border control services fail to check the chain of trust, via proper implementation of the ICAO Public Key Directory (PKD), an additional security feature is all that the chip will be. It is vital therefore that States introducing e-Passports join the PKD and make full use of the facilities it offers.

The question is whether the introduction of the chip in e-Passports has signalled the demise of the printed and physical security features. One only has to study some of the most recently introduced passports, particularly those from Belgium, the United Kingdom, New Zealand, Ireland and Sweden to see that this is not the case.

Substrates

Whilst new substrates are undoubtedly being developed for biodata pages, the key forms in use today remain paper and polycarbonate (PC). Polycarbonate data pages are becoming more widely used, and not just for their ability to provide a robust location for the chip, but also as a security enhancement in their own right. This is demonstrated by the Swiss and Hong Kong passports which use a thinner than usual PC data page and house the chip in the cover.

One of the key advantages of PC for a data page is the relative strength of the substrate. This is becoming increasingly important with the proliferation of e-Passport gates that require the passport holder to place the document onto a reader themselves. Whether a passport has a paper or polycarbonate data page, there is an abundance of new security features being introduced.

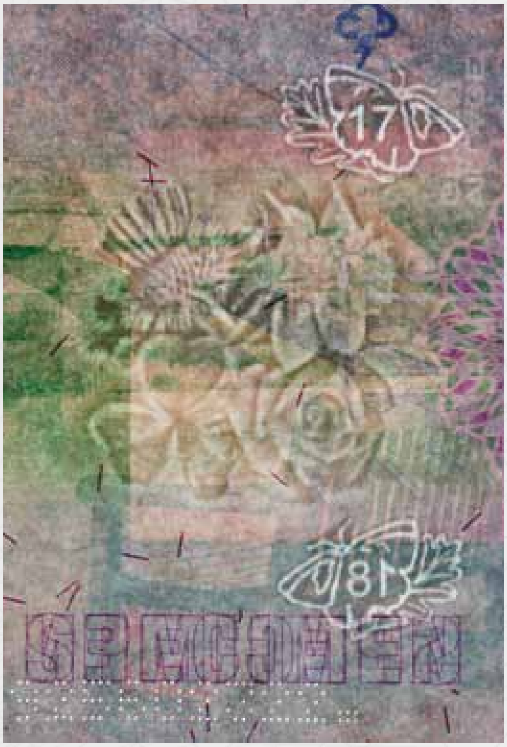


Figure 2 (left)
Mould-made watermark and electrotype page number in UK passport.

Security features

Watermark

A detailed mould-made watermark is still considered by many to be the key security feature for pages made from paper. This is now very often supplemented by the use of an electrotype mark that is different for every page by adding the page number into it (see figure 2).

At one time the detractors of PC claimed that the material would never replace paper, because it lacked the basic substrate features of a watermark. However, this view is now starting to change with the introduction of windows. Several manufacturers are offering this effective level one feature in different formats and it is already seen in a number of passports of countries such as Sweden and New Zealand (see figure 3).

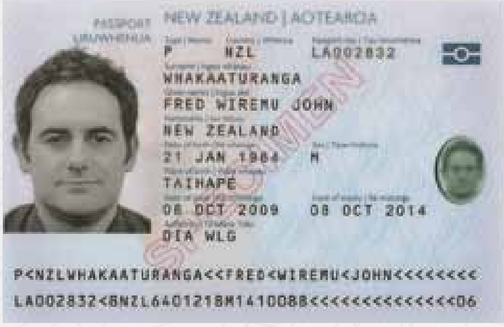

PASSPORT
URUWHENUA
NEW ZEALAND | AOTEAROA
P NZL LA002832
WHAKAATURANGA
FRED WIREMU JOHN
NEW ZEALAND
21 JAN 1964 M
TAIHAPE
08 OCT 2009 08 OCT 2014
DIA WLG
SPECIMEN
P<NZLWHAKAATURANGA<<FRED<WIREMU<JOHN<<<<<<<<<
LA002832<8NZL6401218M1410088<<<<<<<<<<<<<<06

Figure 3 (right)
Window in biodata page of New Zealand passport.

Fibres and threads

Multicoloured fibres were only introduced to the market in 2007 but are now seen in several passports and the EU common format visa. Embedded threads are also used in various forms in paper pages. Together these security features give document examiners a good set of level one features.

Threads are certainly another area in which the industry is moving forward. Windowed threads, common in currency for many years, are now being seen in passports. A recent implementations is the Motion™ thread used in the Swedish passport. Holographic threads are also now being seen in PC ID cards, such as the latest German cards, so it cannot be long before they are introduced into PC passport data pages too.

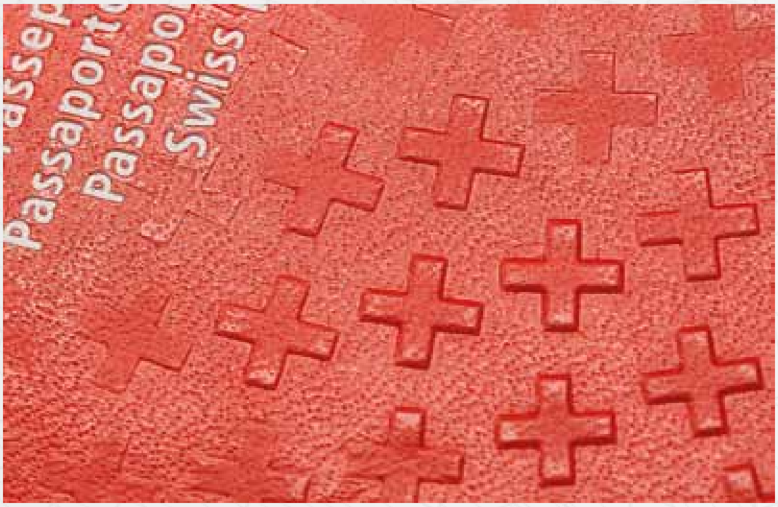
Optically Variable Devices

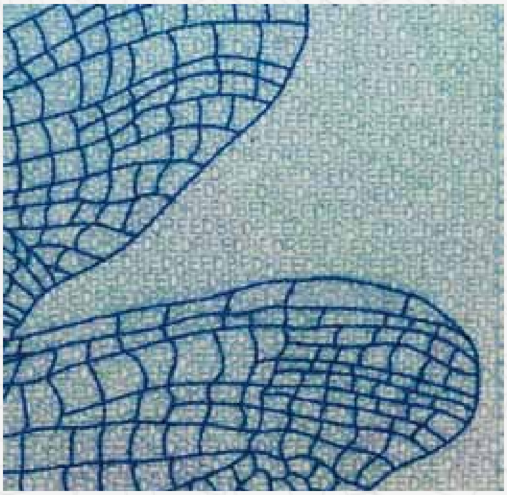
Optically Variable Device features (OVDs) are showing no signs of becoming less popular as a device to protect the personalised data as well as providing anti-copy protection. New level one features are being added by all the major OVD producers with several developing personalised versions.

Tactile features

Tactile security features are being developed that add yet another sense to the document checker's level one armoury. This is particularly the case for PC data pages with tactile elements being added during lamination, but for many years tactility has been incorporated on paper pages by the use of intaglio printing. Another new development in this field is the embossed 'tactile' cover. This was introduced by Switzerland, but others, including the Slovak Republic and New Zealand, have followed suit (see figure 4).

Figure 4
Swiss passport cover.





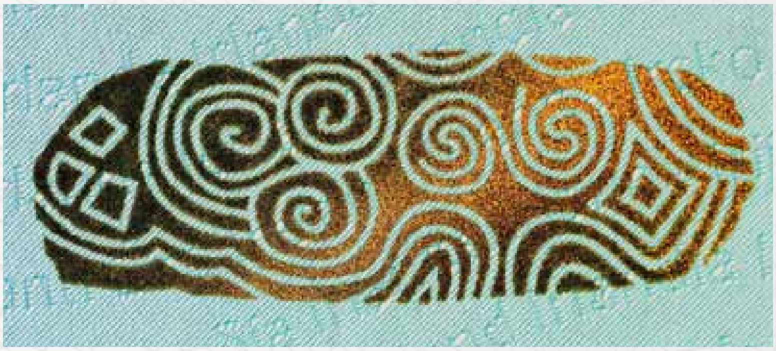


Figure 5 (top left)
User-defined screen in UK passport.

Figure 6 (top right)
SPARK™ feature in Irish passport.

Laminates and patches
Another relatively new development is the combination of different techniques within one laminate/patch. This allows features that can be checked at all four examination levels to be incorporated into one single entity. In some instances these patches are now being given unique serial numbers to increase the security of stock management and provide a tracking number in case of loss or theft.

Print security features
Security printing has also moved on, with key design software suppliers such as Jura and Agfa offering new elements all the time and printing machines offering tighter registration and yet more units. This new technology has allowed for the introduction of user-defined screens containing extra small printing (ESP) or tiny images and the embedding of complex page numbers within a page design (see figure 5).

Tried and tested print security features that can be used for both paper and PC are now being developed further, such as optically variable ink (OVI®) including Charms™ and the new SPARK™ feature (see figure 6). This is a good example of combining different inspection levels in a single feature.

'Invisible' or ultraviolet (UV) printing has been used in passports for many years, but even this has seen advances in recent years. This includes the introduction of rainbow printed UV, true colour UV printing, and the fluorescent feature Gemini™ in the UK passport (see figure 7).

Passport assembly techniques

Passport assembly techniques have advanced too. For passports with PC data pages several new methods for attaching data pages to the booklet have been developed.

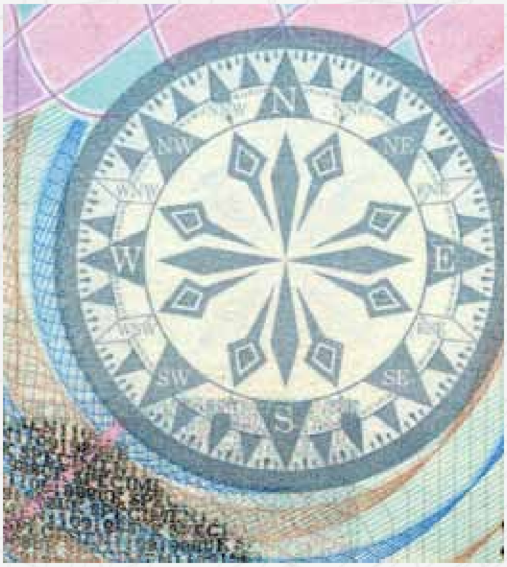
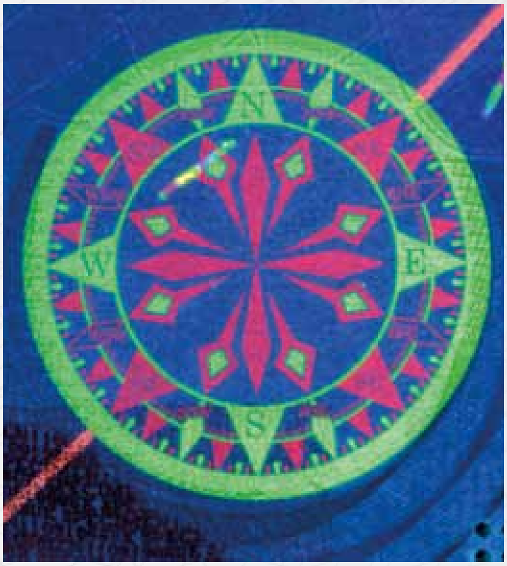
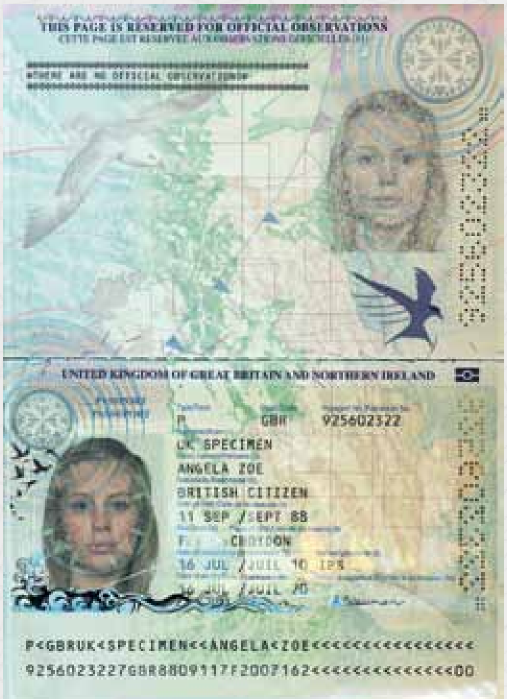


Figure 7
Fluorescent feature Gemini™ in UK passport.



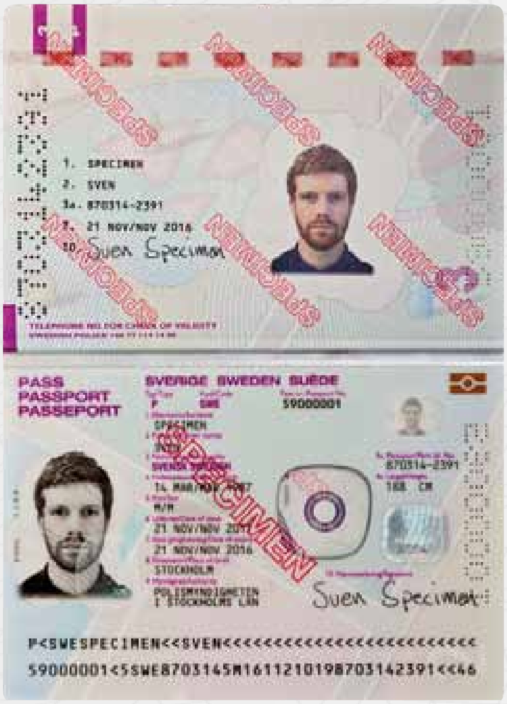


THIS PAGE IS RESERVED FOR OFFICIAL OBSERVATIONS

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND

P GBR 925602322
UK SPECIMEN
ANGELA ZOE
BRITISH CITIZEN
11 SEP /SEPT 88
F CROYDON
16 JUL /JUIL 10 IPS

P<GBRUK<SPECIMEN<<ANGELA<ZOE<<<<<<<<<<<<<<<<<<
9256023227GBR8809117F2007162<<<<<<<<<<<<<<<<00



1. SPECIMEN
2. SVEN
3a. 870314-2391
7. 21 NOV/NOV 2016
10. Sven Specimen

PASS
PASSPORT
PASSEPORT

SVERIGE SWEDEN SUÈDE
P SWE 59000001
SPECIMEN
SVEN
SVENSK
14 MAR/MAR 87
M/M
21 NOV/NOV 2011
21 NOV/NOV 2016
STOCKHOLM
POLISMYNDIGHETEN I STOCKHOLMS LÄN
870314-2391
188 CM
Sven Specimen

P<SWESPECIMEN<<SVEN<<<<<<<<<<<<<<<<<<<<<<<<<<<
59000001<5SWE8703145M1611210198703142391<<46

The limitation of space on a single page has led to secondary (ghost) images being difficult to see because they are underneath the personalisation data or because observations are being added on pages elsewhere in the booklet. At the same time advances in construction have led to the introduction of closely registered cross-page designs. Member States have taken advantage of this by placing the secondary image on the adjacent page, thus forcing forgers to have to deal with the issue of replacing both pages whilst also achieving the complexity of the cross-page alignment (see figure 8).

Personalisation

Passport issuers are calling for more security in the personalisation process and the industry has not been slow to respond. Many passports now feature a secondary image of one type or another and in the case of a couple of recently introduced passports, as many as five images, often produced in different ways, such as laser engraving plus inkjet printing used on adjacent pages as well as the inclusion of a perforated image of the holder (Imageperf^{TM}).

Many issuers have included security within the printed image such as letter screen or embedded invisible information that is viewed via a special decoding lens or software in a passport reader or forensic examination device. Some passport manufacturers have even added the decoding lens into an additional page or a window in a PC page (see figure 9). This moves the checking of this feature from the 'back office' to the border control front desk.

Figure 8 (top left)
Two-page biodata section from UK passport.

Figure 9 (top right)
Pages 2 and 3 of the Swedish passport.

The personal data on paper data pages are no longer protected by thick heat-sealed laminates that can be easily lifted and put back with minimal evidence. The new range of thin films and protective coatings provide a much more secure and tamper-evident barrier.

Conclusion

Although the industry began issuing e-Passports more than 8 years ago, many countries still don't have the infrastructure in place to read the chips. Of those that do, the majority are not making the most of what ePassports can offer by not downloading the root certificates from the ICAO PKD. Until they start using them to properly validate the data on the chip, physical security features will continue to be an essential part of a passport's security. It is therefore vital that we continue to equip our officers with the necessary skills and tools to check the physical security of travel documents, as well as to properly verify the holder's identity, nationality and bona fides against that document.

On this basis, the need for passports to incorporate secure printing and physical security features will be with us for many years to come – the chip has clearly not signalled their demise. What is more, the industry is clearly responding well to this with continued investment into the development of new physical security features.

Reference

1 International Civil Aviation Organization (ICAO), Doc 9303: Machine Readable Travel Documents, Part 1: Machine Readable Passports, current version: sixth Edition 2006; http://www.icao.int/Security/mrtd/Pages/Document9303.aspx.