

SECURITY DOCUMENT WORLD & IDENTITY LOOP 2008 DOCUMENT **SECURITY FEATURES: THE FRAUD BUSTERS' PERSPECTIVE**

Charlie Stevens UK Border Agency
National Document Fraud Unit

Introduction:

Good afternoon ladies and gentlemen. I would like to thank the organisers for inviting me to speak to you today on the continuing importance of robust physical security features for passports and other travel' and identity documentation in this new world of, eDocuments and smart cards using stored biometric identifiers. My background is a career of more than 39 years working operationally in all areas of the UK immigration and border control and for the last 15 years managing the UK Border Agency's National Document Fraud Unit (NDFU), the UK's centre of expertise in all areas of travel and identity document security and for detecting and combating document abuse. My responsibilities have also involved my participation for the last ten years in ICAO, the International Civil Aviation Organization's, New Technologies Working Group (the NTWG) which develops global specifications for machine readable travel documentation (including passports and identity documents) including the international standards and specifications for the latest eDocuments utilising stored biometrics identifiers as well as minimum specifications for document issuing and physical security standards

***Aims of the presentation:**

- The role of ICAO in developing new ePassports and Travel Documents
- The challenge of achieving global uptake of ICAO specification ePassports and Travel Documents
- The need for backward compatibility
- The continuing value of robust physical document security features into the future.

*The role of ICAO in developing new ePassports and Travel Documents ICAO has for decades held the leadership role for development of standard specifications for passports and travel documents 'having been set up in 1947 as an outcome of the 1944 Convention on Civil Aviation, commonly called the Chicago Convention. The first manual of guidance material for states was published in 1980 by ICAG as the first edition of Document 9303. This document has now progressed over the years into three parts covering specifications and standards for machine readable passports, visas and other travel documents, including card formats.

The aim of ICAO in developing these specifications was to facilitate international border crossing for increasing numbers of travellers by creating standardised layouts for machine readable travel documents to enable the nearly 200 member states of ICAO to have their passports and documents recognised and verified by border control official. the same time ICAO reorganised the security and criminal threats posed by abuse of travel documents and built in minimum standards for the physical security of travel documents. This involved incorporation of a minimum set of high security features that could be checked and tested by properly trained border control officials and which would frustrate forgers or counterfeiters attempting to compromise the documents. ICAO also provided advice and minimum standards for travel document issuing authorities in order to secure and maintain the integrity of the application and issuing processes for travel and identity documents.

The measure .of success of ICAO's work was its target for global interoperability, that is the ability for all countries' passports and travel documents to be recognised and their integrity established by both visual examination and machine reading along with verification of the identity and nationality of the person presenting the document.

ICAO recognised that there would always be a risk of forgery or counterfeiting of travel documents and, in particular, it was concerned that genuine documents presented by imposters or look-alikes or fraudulently completed stolen blank documents might deceive border control officials and conventional machine readers that simply verified the contents of a documents machine readable zone. It was natural, therefore, for ICAO, as its work progressed, to look to new and developing technologies to assist in providing additional layers to- the document security and verification process and in the 1990's the ICAO NTWG started to consider the technical feasibility of the introduction of biometrics technology into travel documents. This work was well underway at the time of the 9/11 attacks in New York in 2001 which led to political and legislative demands in the USA and the EU for the introduction and issuance of biometrics ePassports and travel documents, that finally came into effect in 2006. I must emphasise, however, that it was never the intention by ICAO for biometrics identifiers to become the sole panacea for determining the identity of document holders'. Biometrics were, and still are considered by ICAO as being one more extremely useful and additional security safeguard to the existing range of document security safeguc;1rds and features employed in Machine Readable Travel Documents.

***The challenge of achieving global uptake of ICAO specification ePassports and Travel Documents**

The work of ICAO in setting international standards and specifications for machine readable travel documents has been universally applauded. With more than 200 countries in the world each issuing a range of passports and travel and identity documents there are, as a result, literally thousands of different valid travel documents in existence worldwide. The problem faced by border control, other enforcement authorities and carriers in identifying and verifying all these documents would be overwhelming without common standards for format, machine readability and physical document security features.

The question that might be asked then is why are all countries not currently issuing ICAO specification passports and travel and identity documents or the new specification eTravel Documents? The fact is that the majority of international travellers nowadays do hold documents issued by states that do issue ICAO specification machine readable travel documents (MRTDs). There are still a large number of countries, however, that have not yet introduced ICAO MRTDs. These countries are generally from the developing world where the costs of introducing new technologies to passport issuing are often considered disproportionately high or from states that have not yet developed to machine readable travel document technology.

ICAO introduced the specification for globally interoperable machine readable travel documents as far back as 1980 (28 years ago). It has been a long and often tortuous process in encouraging states worldwide to introduce ICAO specification documents. Whilst ICAO sets the global standards and specifications it has no legal mandate over states and ICAO standards only become mandatory when certain states or groups of states such as the EU pass their own legislation requiring their introduction by law. It has not only been developing countries that have been slow to accept ICAO standards for their documents. Even the UK did not introduce ICAO compliant documents until 1988 and it was not until 1995 that we had full machine reading capability of the documents at our border controls. Indeed, ICAO has been so concerned about global uptake of machine readable travel documents (let alone eTravel Documents) that in 2005 it sought and achieved agreement to a resolution by its then 188 Contracting States for them all to be issuing ICAO compliant machine readable passports by 1 April 2010.

Encouragement of all states to meet this target is now being worked towards by ICAO and numerous government bodies such as the G8 group of states in an ICAO programme called Universal Implementation of Machine Readable Travel Documents (UIMRTD). This programme aims to offer technical advice and assistance to non-compliant states to meet the 2010 deadline. Whilst the aim is to achieve global interoperability of machine reading for passports it is acknowledged that even if the 2010 deadline is met then there will be a further period of up to 10 years when non-compliant legacy documents might be remaining in circulation before global interoperability of all passports by machine reading will be

achievable. UIMRTD is focusing on standard MRTDs and ICAO will, come 2010, be looking to encourage in a similar way uptake of new eTravel Document biometrics enabled passports.

Given the timescales I have described to achieve global interoperability for standard, non-biometric MRTDs it will clearly be many years into the future before full global uptake is achieved of new ePassports and Travel Documents. The problems with uptake of these documents are, in many respects, greater for a number of reasons:

- The costs of producing new ePassports with the associated chip technology is greater than for non-chip passports
- The costs of installing and using machine readers for ePassports and Travel Documents at all immigration and enforcement control points and training staff in their use is substantial, particularly if verification of the chip data and one to one biometric comparison of document holders with chip data is to be achieved.
- Given the logistics of installing ePassports readers it will be many years before all remote border crossing and other check points globally are provided with Passport, biometrics verification readers and in the interim these control points require manual checking of documents.
- Security and verification of chip data depends upon a sophisticated public key infrastructure (PKI) which requires exchanges of vital key information between all states globally on a regular basis, which is proving slow to achieve at present.
- Chip technology in travel documents with validity periods of up to 10 years is new and cutting edge and yet to be proven in terms of reliability and durability.
- If a chip fails to read in an ePassport other than through malicious damage then the passport will still remain a valid passport certifying the identity and nationality of the holder and it will be relying on manual inspection of conventional physical document security safeguards to confirm the veracity of the personal data contained in it.
- Whilst legislative requirements for states to issue ePassports is growing it is still a long way short of achieving a global requirement on all states to move

to ePassports.

***The need for backward compatibility**

Given all these problems it is unlikely that global interoperability of both document issuance: and machine reading and verification of documents with their holders using stored biometrics will be achieved for many year ICAO has been aware of this and so it has always emphasised the need for backward compatibility in its document development processes. This means that traditional standards for document layout and format are carried forward into new, higher technology documents. As a result the latest ePassport readers will also be able to read older style MRTDs and the layout and physical security features built into documents will be of the same robust standards in new ePassports as in previous model documents. ICAO recognises this need and is keen to ensure that states do not let traditional physical security safeguards and features decline because of the introduction of ePassports.

***The continuing value of robust physical document security features into the future**

I hope that my presentation has explained why, despite the excitement felt in border control and enforcement circles about the value of new biometrics, ePassports and Travel and Identity Documents, there is still a *very* firm requirement among control authority practitioners for the maintenance of high quality robust physical security features into the future. I considered that a most fitting conclusion to this address would be to provide some illustrations of a few of the types of document security feature that have proved themselves robust and valuable for control authority inspections.

***Quality passport covers with detailed embossing**

(image)

***Front endpaper with high quality printing such as intaglio print.**

(image)

***Biodata page or insert in accordance with ICAD specifications with image and personal data properly protected**

(images of biodata page and polycarbonate insert in white light and UV)

***Secure laminate with appropriate safeguards**

(images showing holographic safeguards and UV safeguards)

*** Watermarks**

(image)

***Quality fine line offset printing and rainbow printing**

(image)

***High quality security paper with low base fluorescence and security fibres or
planchettes**

(image)

Laser security features.

(images of laser numbering/perforation/changeable laser image) ,

Thank you for your attention.