# ICAO MRTD Report

VOLUME 1 / NUMBER 2

OPTIMIZING SECURITY AND EFFICIENCY
THROUGH ENHANCED ID TECHNOLOGY

## ePassports Have Arrived

## Implementing the New ICAO Standards

MACHINE READABLE TRAVEL DOCUMENTS

PASSPOR

**ICAO MRTD Report**

Vol. 1, No. 2, 2006

**Editor**: Mary McMunn

**Content Coordinator**: Mauricio Siciliano

**Graphic Art Design**: Sylvie Schoufs,
FCM Communications Inc.

**Cover Page Photos**: Jim Jorgenson, Imaging Automation - Viisage and Gilles St-Onge

**Cover Page Graphic Art Design**: Gilles St-Onge, Studio Idées en Page inc.

**Published by**:
International Civil Aviation Organization (ICAO)
999 University Street
Montréal, Québec
Canada H3C 5H7

Telephone: +1 (514) 954-8219 ext. 7068
E-mail: msiciliano@icao.int
Web: www.icao.int/mrtd

The objective of the ICAO MRTD Report is to provide a comprehensive account of new developments, trends, innovations and applications in the field of MRTDs to the Contracting States of ICAO and the international aeronautical and security worlds.

Opinions expressed in signed articles or in advertisements appearing in the ICAO MRTD Report represent the author's or advertiser's opinion and do not necessarily reflect the views of ICAO. The mention of specific companies or products in articles or advertisements does not imply that they are endorsed or recommended by ICAO in preference to others of a similar nature which are not mentioned or advertised.

The publishers extend their thanks to the companies, organizations and photographers who graciously supplied photographs for this issue.

**Advertising Representative**:
Yves Allard
FCM Communications Inc.
835 Montarville Street
Longueuil, Québec
Canada J4H 2M5

Telephone: +1 (450) 677-3535
Fax: +1 (450) 677-4445
E-mail: fcmcommunications@videotron.ca

# Table of contents

# Editor's message

Dear Reader,

In this issue of the *MRTD Report* we celebrate the successful implementation of the ePassport according to the standards developed in ICAO by experts in the TAG/MRTD and ISO. The significance and implications of this achievement cannot be overestimated.

The advent of the ePassport, expected to be deployed by some 40 member States by next year, heralds a global revolution in the issuance of travel documents, inspection of people and identity management. Passport and ID inspection systems used by airlines and border control agencies at airports will be substantially upgraded to enable more precise matching of documents to people, authentication of data in the documents, and more efficient processing of travellers at checkpoints.

Just as important, the ePassport also offers substantial benefits to the rightful holder, by providing a more sophisticated means to confirm that the passport belongs to him or her and that it is authentic, without jeopardizing privacy. A stolen – or cloned – ePassport will be useless as an identity document because the biometric in the chip and the digital photo will not match the person holding it. The chip content mirrors the passport data page, so forgeries will be very difficult. The risk of skimming or eavesdropping has been addressed with Basic Access Control, which in effect requires that the booklet be open and touching an OCR reader before the chip can be read.

Moreover, the validation and authentication of the electronic data with Public Key Infrastructure supports a positive result of passport inspection, so that the traveller with an ePassport can participate in new automated inspection systems and be processed in the shorter lines for airline check-in and border control.

While ICAO encourages its member States to develop the capability to issue ePassports to their citizens, we continue to promote the issuance of conventional machine readable passports (MRPs) by States that are not already doing so. With the digitized photo of the holder printed directly onto the data page and the standard-format machine readable zone with its check digits, MRPs together with machine reading systems are essential components of national measures to deter identity theft, illegal migration and trans-border crime. Travellers carrying them will find it much easier to obtain visas and to pass through formalities at other countries' entry points.

Last year the Organization's 189 member States agreed that all must begin issuing only ICAO-standard MRPs not later than 1 April 2010. Education and assistance efforts are well underway to help States meet that goal.

Mary K. McMunn

PASSPORT
United States
of America

# STOLEN BLANK DOCUMENTS – a target of opportunity for counterfeiters

## Current Situation and Options

by Maria Isabel Baltazar
Serviço de Estrangeiros e Fronteiras, Portugal

## Current Situation

According to recent U.S. statistics on security documents, two thirds of document fraud crime consists of impersonation, i.e., the use of someone else's document. According to the same source, 25 million stolen documents are in circulation worldwide and nearly 80% of all seized documents have been declared stolen, as either pre-issued or post-issued documents.

Techniques to counterfeit and alter documents also apply to stolen pre-issued (blank) documents. The accuracy and the technical quality are often much more complex and ingenious, and the results are frequently far better and the fraud harder to detect.

The user profile for these documents is quite different from the profile of those using *ordinary* forgeries. Stolen blanks are often connected with organized crime and smuggling networks, with highly structured cells working backstage. Therefore, *assessment (profiling) of individuals* is, in most cases, the only way out to disclose cases of identity theft and/ or the use of stolen blanks.

Law enforcement authorities, particularly border control authorities, are continuously seeking timely and accurate information on the validity of identity and travel documents.

## Future Options

**There is no single, foolproof solution!**

The multiplicity and complexity of all the factors entangled in criminality demand a combination of well-targeted and accurate measures. A proactive approach is essential in order to efficiently fight back against document fraud – prevention should be the focus.

It would seem realistic to consider the following three options as promising measures to prevent the theft of stolen blank documents, and to detect or identify invalid/stolen documents.

- A global electronic database focusing on lost and stolen documents;
- A coherent Identity Chain approach, taking extra security measures with breeder documents and aiming at a centralized personalization process (issuance procedures); and
- Harmonized security standards for the storage of (blank) security documents.

### 1. Global Data Interchange

At present, only Interpol furnishes a global system. All over the world there are national and regional databases for stolen documents, but none of them offers the timely global response that Interpol does. The majority of the countries in the world are Interpol members, and the fact that 166 out of the 182 Interpol member States are already entering information on the STD/ Stolen Travel Documents Database presents a promising scenario for globally accessible information, for the sake of all and the security of every individual.

Although participation by States is voluntary, global interchange provides multiple benefits, such as:

- Improved border integrity
- Detection of identity theft cases
- Improved chances for criminal activity detection and identification of criminals
- Recovery of lost and stolen national passports
- Diminution of the value and the usage of lost, stolen or invalid documents for illegal purposes.

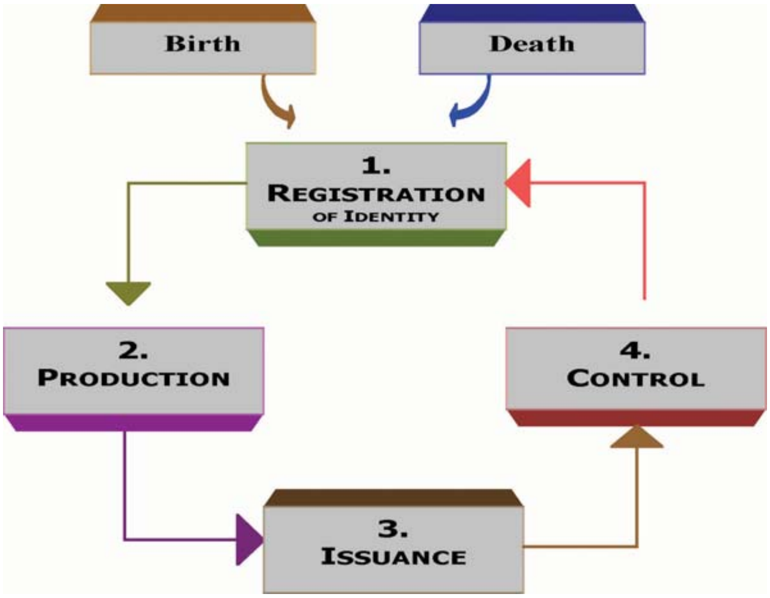
## 2. Coherent Identity Chain and Centralization

### Coherent Policy

In order to improve quality and to achieve according security levels and efficiency, a coherent policy concerning security documentation is required. Hence, basic requirements and access procedures should be shared amongst all concerned agencies and parties along the Identity Chain – Registration/ Production/ Deliverance/ Control – where birth and death records play a crucial part.

By co-ordinating knowledge and investments at each level, synergy can be reached in several areas. At the end this global and integrated approach will assure the best performance possible for each party individually and for the government as a whole.

The figure below illustrates the ID Chain approach.

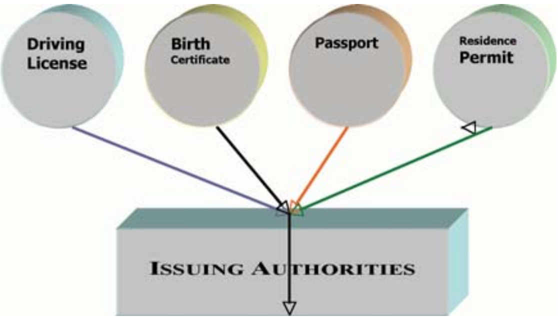


Governments are responsible for the issuance of a number of official documents, which carry individual identity data. Examples of such documents are passports, identity cards, birth certificates and driving licenses, among others. It is often a precondition for the issuance of one of these documents that one of the others (known as "breeder documents") be supplied. Security measures not only focus on the final document but also spotlight the whole chain of documents that supports the issuance/delivery process.

For the issuance of all these documents, different schemes and procedures apply, leading to the conclusion that no systematic or harmonised organisation brings the whole process together. Although the Government is the titular entity, several different agencies are competent to issue security and identity documents. Their requirements and standards have been achieved and improved over time, but usually on a stand-alone basis.

**Centralization**

A thorough assessment and a comprehensive analysis are the working basis to build up a coherent document policy in general and to adjust to a centralized system, as shown in the figure below.



An identity architecture built on a centralized and harmonized solution, assures equal treatment to all documents, consistency over time, best performance in terms of standards, guaranty of security, and bottom line: transparent issuance processes based on standard procedures, circumventing dramatically the risk of stolen blanks.

By contrast, within the framework of machine operated and assisted control, a decentralized issuance system is potentially more subject to nonconformities and inconsistencies for machine-reading functionalities. It requires more resources in the long term. Furthermore, a decentralized approach presents many more challenges to achieving the desirable level of security, especially in terms of biometry and the new-generation ePassport.

Finally, a centralized, transparent and coherent identity system will enhance the reputation of the national government, will boost public confidence and will be viewed with confidence by (inter)national partners as well.

### 3. Storage of blank documents

Even with centralized issuance procedures, there is still room for improvement in the field of theft prevention.

The adoption of security standards for the storage of blank documents, regardless of its security level, together with a procedure-code, seems to be a well-agreed topic. Nomination of access personnel, briefing and debriefing rules, description and listing of materials are a few examples of what should be regarded as much more than best practices.

The EU has already expressed its concern on this matter as well as ICAO and Interpol. The latter organizations have targeted in particular the tracing of blank security components, such as security paper and substrates, amongst other materials and key elements for the assembling of security documents.

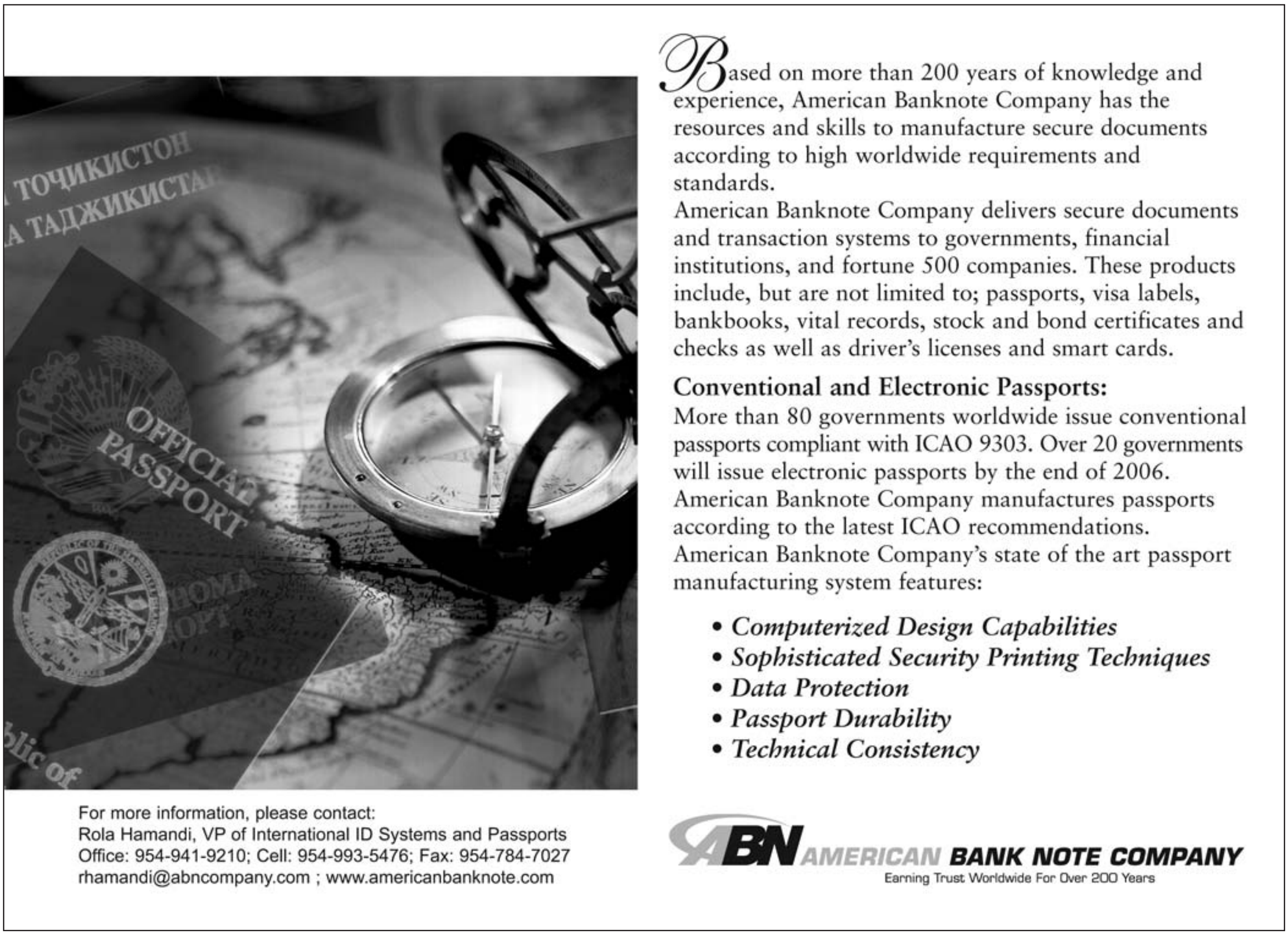
## Conclusion

Due consideration for all issues raised will unquestionably improve efficiency, quality, security and safety, serve to enhance the confidence of all parties involved and boost public awareness and trust.

Processes are, however, dynamic and synergetic, therefore, the latest developments in terms of technology applied to document security, will be presenting new challenges and innovative solutions.

Biometry will add a new dimension to document security by assuring a unique link between the document and its holder.

Finally, interoperability of identification globally and the fine-tuning of processes for enrolment and for checking identities will minimize the value and usage of stolen blank documents, as it will comprise a new generation of e-documents. ◆

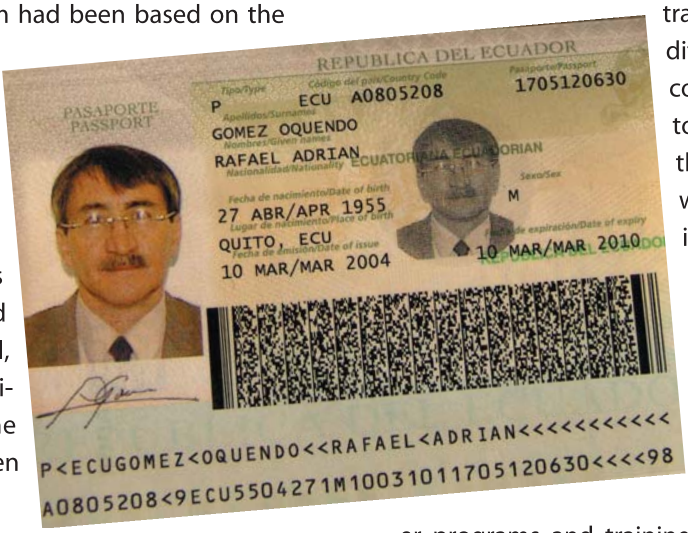


# The New Ecuadorian Passport: A success story

by José Sandoval
Former Director of Ecuador's Passport Office

Almost three years ago, the Ministry of Foreign Affairs decided to launch a comprehensive project to modernize the Ecuadorian passport and create an issuing system connected to a central database. This would allow it to consult in real time aspects related to issuance and validity of passports in the 22 provinces of the country, as well as in more than 60 Ecuadorian consulates abroad.

The situation prior to that was devastating. For many years, the system had been based on the good faith of officials and on the belief that users would make good use of a very rudimentary passport, filled by hand, where the photograph was simply glued and which, on top of it all, allowed the indiscriminate inclusion of the spouse and the children of the passport bearer.



REPUBLICA DEL ECUADOR
PASAPORTE
PASSPORT
Tipo/Type P
Código del país/Country Code ECU A0805208
Pasaporte/Passport 1705120630
Apellidos/Surnames GOMEZ OQUENDO
Nombres/Given names RAFAEL ADRIAN
Nacionalidad/Nationality ECUATORIANA ECUADORIAN
Sexo/Sex M
Fecha de nacimiento/Date of birth 27 ABR/APR 1955
Lugar de nacimiento/Place of birth QUITO, ECU
Fecha de emisión/Date of issue 10 MAR/MAR 2004
Fecha de expiración/Date of expiry 10 MAR/MAR 2010

P<ECUGOMEZ<OQUENDO<<RAFAEL<ADRIAN<<<<<<<<<<<<
A0805208<9ECU5504271M1003101170512063O<<<<98

The first step was to increase the cost of the passport 20%; the additional funds would be used to finance the entire project. The public's reaction was highly positive as, in exchange for a little more money they received a safe, universally accepted document, manufactured according to ICAO standards.

For each passport issued in Ecuador, a certain amount of money is permanently feeding a fund that will allow not only to satisfactorily complete the project, but to guarantee the updating of equipment, training of officials, maintenance of computer programs, and eventually the purchase of facilities to install passport and consular offices, as currently large sums of money are destined to leases.

The next step was designing a new passport book according to ICAO standards, that is, a machine-readable travel document. The design of the new booklet included not only security features, like quality of paper, stitching, etc.; illustrations representing the different regions of the country and promoting tourist attractions and the identity of Ecuador were also incorporated in each page.

The passport issuing system was divided in several successive phases that allowed the provision of equipment, computer programs and training to officials in all the provinces of the country and in the consulates that would be in charge of issuing travel documents.

Twelve provinces were equipped during the first phase. Through an Internet-based system the Foreign Ministry was able to authorize the issuance of passports and control the previous passport history of each user. Once the adequate operation of the system was verified and the required adjustments were made, the system was extended to all 22 provincial government offices. According to the needs of the country, 3 printing centers in Cuenca, Guayaquil and Quito and 19 data-capture centers were opened. In printing centers, the passport is delivered in less than 30 minutes, while in data-capture centers it takes 48 hours.

The following phase included extending the use of the new issuing system to 5 printing consulates and an additional 22 consulates that worked as data capture centers. An intense information campaign was required for the data capture consulates, during this phase to raise the awareness of the public concerning the benefits of a new passport that, precisely because of its new security features, could not be delivered immediately, as had been the case in the past. Passport delivery in printing consulates is immediate, while in data capture consulates it takes approximately 10 days. Once this stage was completed, the new system was extended to more than 60 Ecuadorian consular offices all over the world.

The third phase provides interconnecting the system with Ecuador's international airports, as well as with land border crossings. This phase is expected to be completed in the next few months.

Many national institutions were involved in the project; in fact, the new passport reinforced the idea of having one single national identification number that would be used for the passport, the National ID Card, the driver's license, etc. The Government of Canada[1] and several international organizations also participated in the project, giving it its own dynamics and some legal and financial autonomy, and this also helped reinforce technical and administrative controls. The involvement of the Canadian government ensured the contribution of significant non-refundable financial cooperation.

The experience of the project has been highly positive, because we have not only modernized a key area of public services, but also because we have succeeded in bringing together several State institutions to provide Ecuadorian citizens with a machine-readable travel document manufactured according to ICAO standards.

The authorities of the Ministry of Foreign Affairs of Ecuador have given top priority not only to ensuring a high technical and security level in the process, but also to providing top-quality service. To this end, training courses are given on a regular basis to officials working in the passport service, which is now considered one of the most efficient and customer-friendly public services in the country. ◆

[1] Through the Canadian Commercial Corporation and the Canadian Bank Note Company, which acted as contractor.

# ePassports: Are We There Yet?

by Barry J. Kefauver
Fall Hill Associates, LLC

### The Next Generation of Passports Is Here

With the publication of the Sixth Edition of Document 9303 Part 1, the International Civil Aviation Organization has moved the world's passports to a new level of travel document security, data integrity and identity management. This two-volume set of specifications culminates the work that began with ICAO's first Request for Information (RFI) issued in 1995. This effort reached out to the world's vendors and asked for three areas of focus: physical security features; biometrics; and, data storage media. Emphasis was placed on the latter two, with the connection being that a higher level of storage capacity was required in order to allow for the storage of biometric information on passports. Now, more than eleven years of hard multilateral work later, deployment has begun for what I consider to be the most secure passport the world has ever known. This article discusses a few aspects of policy consideration in implementing biometric enhanced, chip-based passport programs.

### Chips

We have come a long way from that hot February day in Canberra (2004) when none of the 11 readers could read any of the 12 different chips being tested, even though they all puffed out their respective electronic chests proclaiming "14443 compliant", that is, comporting with the ISO standards for contactless chips. Since that time we have seen a huge amount of testing, a great deal of learning, a bit of new science, some good luck and what can only be defined as divine intervention. This all combined has brought us to the point where the June 2006 testing in Berlin and a variety of pilot live-tests all reflect that we do indeed have interoperability; we do indeed have a sound foundation in contactless chips to carry data in passport books. Undoubtedly we have more to learn and discover as passport programs come on stream. Consider these learnings not as warts and flaws in technology, but as simply that which they represent: evolutionary enhancement of our travel document technologies.

### Biometrics

Immediately after the tragedies of September 11, 2001, some astounding claims were made for the virtues of biometrics. A few of these representations were just too good to be true; they weren't. In tempering the unfulfillable hype over the past few years with significant amounts of testing, education and rubber-hitting-the-road applications, we have made much progress to ascribing the proper role of biometrics in border control and identity management as one of the several tools, not THE panacea, that in combination get us closer to that reality of linking a passport to its rightful owner. Remember that it was one-to-one verification that led ICAO toward biometrics as a goal. The ability to effect one-to-few or one-to-many identification is of course desirable and feasible, but the guiding intent was linkage of the document to the individual claiming rightful ownership.

### Enrollment Systems

A tremendous investment in money, time and emotion has gone into the enhancement of the passport, incorporating contactless chips in order to be able to carry more data to accommo-

# ▶ Top of its class in official interoperability tests

**ACG readers feature:**

- ☑ **Easy integration**
- ☑ **Interoperability**
- ☑ **Highest data transmission rates**

***Available now as OEM module, Plug&Play board, desktop reader and plug-in module for mobile devices.***

# Benchmark performance

Making things easy for the integrators and the users of today's advanced border control applications is a complex challenge we are proud to stand up to.

ACG readers offer you:

- ▶ **Upgradeable firmware**
- ▶ **SAM interface for PKI applications**
- ▶ **Customized design-in service**
- ▶ **Highest security**
- ▶ **Anti-collision**

As world class experts in RFID technology and reader R&D, ACG provides you with a key component that represents a make or break factor for the successful deployment of your e-passport and e-visa solution.

**ACG: identification components and know-how for citizen ID programs.**

**www.acg-id.com**
**government@acg-id.com**

ACG id

date the use of biometrics. This investment is now beginning to bear fruit with several countries already issuing chip-based passports and at the time of this writing an estimated 54 countries will have, or be well on the way to having, e-passports within the coming two years. However, it is urgent that the systems and procedures on which these passports rely for entitlement and adjudication judgments are extremely vulnerable to what will undoubtedly be a higher level of attack and threat. I will single out as the two most significant areas of vulnerability: the human resource on which all passport issuers rely; and the "breeder" documents used to validate and verify claims of entitlement. As part of an overall risk assessment-management program, all issuers must devote particular attention and resources to these two highest priority areas of vulnerability.

## Border and Other Inspection Systems

It seems ironic that, while we characterize these travel documents as "machine readable", much remains to be done in the way of gearing up to read the documents. The Berlin testing, while reflecting adequate availability of interoperable readers, made it clear that the development of "documents" is substantially further along than that of readers. I am confident that market forces will prevail in which those readers that are less agile will fall by the wayside just as those that perform well will carry the day and improve over time. We cannot allow ourselves the misguided luxury of the eight years it took to install a meaningful infrastructure to read just the OCR-B in passports. To realize the full potential of today's technological tools such as biometrics, it is critical that border control authorities equip themselves with equally sophisticated inspection capabilities as urgently as possible.

## Privacy, Data Integrity and PKI

Concerns about the protection of individual rights, security and integrity of data and privacy have been focal and pivotal concerns interwoven in all of the deliberations regarding travel document specifications. One of the four prongs of the ICAO biometric blueprint, the foundation for Document 9303, is PKI, the Public Key Infrastructure. These measures, together with the ICAO-recommended best practice of Basic Access Control (BAC), make the e-passport, in this author's opinion, light-years more secure than ANY travel document ever produced. In a presentation at the conference following the Berlin testing, the Dutch delegate systematically analyzed what would be necessary to "crack" the encryption strength offered by BAC. While realistically acknowledging that, of course, humans can break anything that humans create as well, this presentation refreshingly folded in the pragmatic considerations of the real world. To quantify, using BAC entropy as it is now construed, the number of possible keys to open the chip of a ten-year passport is 1.6 X 10 to the 22nd power. So if we take a flight of fancy and assume that sufficiently large number of passports could be skimmed and eavesdropped upon to garner the raw data, there would ensue a challenge for a gaggle of Crays for quite some time at a rather substantial expense to determine the key to unlock a given chip. I submit that this level of protection should reassure the most anxious passport holder that his personal data cannot be read without his knowledge.

To address data security the ICAO-specified PKI itself is designed to provide to the readers of ePassports a means for verifying the origin and authenticity of the data in a chip, and in so doing acts as a powerful deterrent to forgery and counterfeiting. Using the public keys of the respective issuing States, the cryptographic verification function will provide conclusive assurance that the biometric and machine readable zone data were indeed placed in the chip by the issuing authority and that they have not been altered. The public keys of ePassport issuing States will be stored centrally and distributed by the Public Key Directory under the aegis of ICAO, which will in turn assure the users that the public keys are authentic, thus closing the data security loop.

### So, Declare Victory and Fold the Tent?

With the publication of the Sixth Edition of Doc 9303 Part 1, some may feel that the travel document standards work has been completed. I submit that the work has just begun. The rollout of e-passport programs, both issuance as well as inspection, entails an obvious very substantial amount of work and will continue for several years. Additionally, the “next” next generation of technologies must be considered and assessed. I am very bullish on the new work item that the ICAO New Technologies Work Group has recently undertaken. Entitled “Identity Management”, this work will take a holistic approach to the wide range of factors that must be taken into account in properly addressing entitlement judgments, breeder documents, personalization systems, use of commercial and other databases, internal controls, physical and system security, data integrity and privacy and other related matters.

While the travel document community can look back with great pride on the work that has produced Document 9303, we must look forward to that “next” generation of technologies and systems that will be required to keep pace with tomorrow’s security and facilitation requirements. Now is the time to prepare for the inevitability of that tomorrow. ◆

DO YOU KNOW
WHO'S TRAVELING?
iA-thenticate® Smartchip
A full page document authentication
scanner with RFID contactless chip
reader for ePassports and government
issued identification cards. It includes
Basic Access Control (BAC) and 1 pass
read with automatic authentication.
Massachusetts 978.932.2200
Washington D.C. 703.414.5800
EMEA +49 234.9787.0
www.viisage.com
email: info@viisage.com
ViiSAGE

# ePassports and the Implications of ICAO Standards

by Simon Lofthouse,
Temporal S. Limited.

As the visa-waiver deadline approaches, an increasing number of Countries are either now issuing new ePassports or are soon to do so. These Countries have made tremendous progress in a short period of time and they have demonstrated how this major challenge can be addressed. However, in reality, such progress is limited to a relatively small number of Countries leaving the vast majority still in the very early stages of ePassport development.

In an attempt to assist those those early-stage Countries, this article examines the International Civil Aviation Organisation (ICAO) requirements for the PKI component of an ePassport production system. Specifically, this article looks at the architecture implications, PKI component functionality and PKI interfaces. The operational environment issues are not covered within this article, but these can be found in the complete white paper from which this article is summarised http://www.temporals.co.uk/tss/pages/ts_dl_request.php

For passport production, States around the world operate their own facility or use facilities operated by a service provider. With the introduction of the new International Civil Aviation Organisation (ICAO) specifications for Machine Readable Travel Documents, States and service providers need to enhance their facilities in order to issue compliant ePassports. The use of a contact-less IC chip in the ePassport means that the production process must incorporate elements of a Public Key Infrastructure (PKI) to generate, digitally sign and subsequently verify the embedded data, as well as the facility to write the data to the chip. The implementers and operators of the existing facilities are addressing many of the changes to existing processes needed to support these new requirements. However, new components are required which are outside their experience and expertise. These include devices to interface with the contact-less chips and the PKI that needs to be put in place.

ICAO has specified some aspects of the implementation of a PKI to support the production of standard, inter-operable ePassports. However, some features are optional and many processes and procedures are not detailed but left for subsequent specification by implementing States. This will inevitably lead to inter-operability issues especially where components are being specified, implemented and/or operated by different bodies or organisations.

## Architecture

In its [PKITR] technical report http://www.icao.int, ICAO has specified some aspects of the implementation of a PKI to support the production of standard, inter-operable ePassports. However, some features are optional and many processes and procedures are not detailed but left for subsequent specification by implementing States. This may lead to inter-operability issues especially where components are being specified, implemented and/or operated by different bodies or organisations.

At its most basic, [PKITR] is intended to enable receiving States to verify the authenticity and integrity of the data stored in the MRTD in the form specified in [LDSTR] using Contactless Integrated Circuits as specified in [BIOTRI]. The use of Public Key Cryptographic techniques ensure that signed data can be verified using a certificated public key. ICAO does not specify the CA hierarchy within a State any further than identifying that there must be a Country Signing CA (CSCA) which signs Document Signer (DS) certificates. There are, however, some requirements imposed on the operation of these facilities which need to be implemented and documented in the Certification Practice Statement (CPS).

**Passport Production Systems**

Any existing passport production system must already perform a number of significant steps in the process of producing a passport. This is illustrated in Figure 2.1. With the introduction of the requirement for an MRTD offering access for Receiving States to the Logical Data Structure (LDS) on a contact-less IC chip, the production process must incorporate elements of a PKI to generate the SOD and subsequently verify it, as well as the facility to populate the LDS and to write data to the chip. This is illustrated in Figure 2-2.

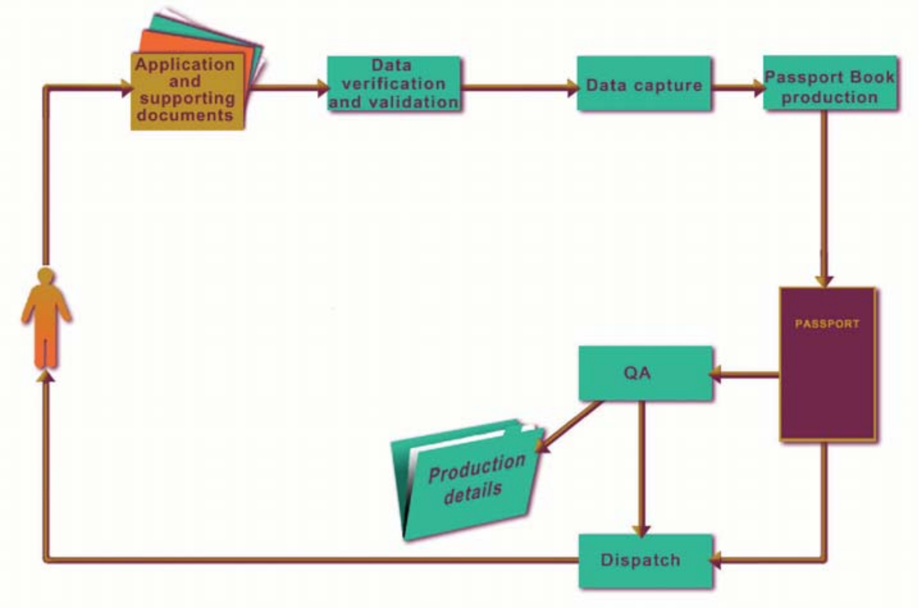


Figure 2.1: Passport Production System

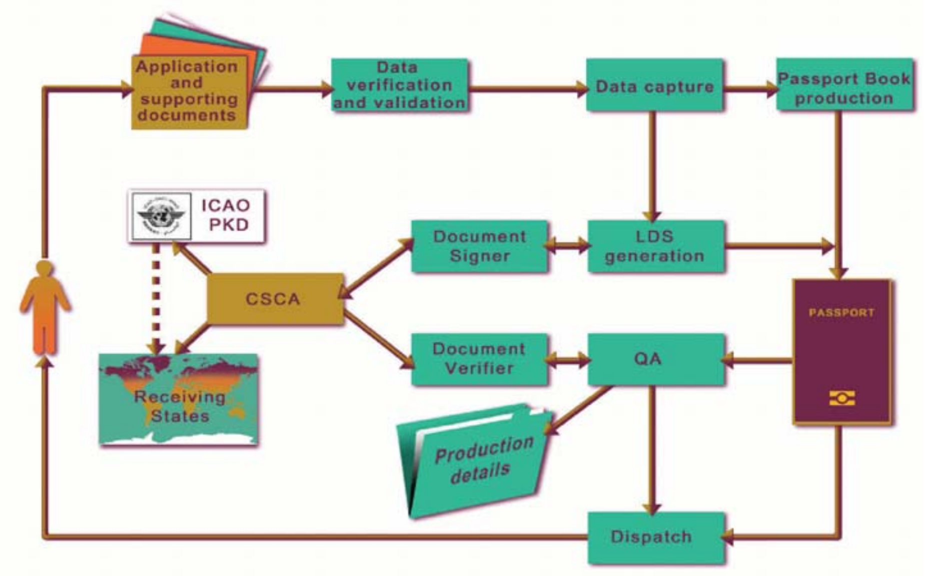


Figure 2-2: ePassport Production System

## PKI Component Functionality

From Figure 2-2 it is clear that there are a number of components to the PKI that provide the required functionality. These are further identified in Figure 3-1 below and subsequently specified in the subsections that follow. References to the summarised requirements are shown as [*n*] as they appear in the [PKITR].

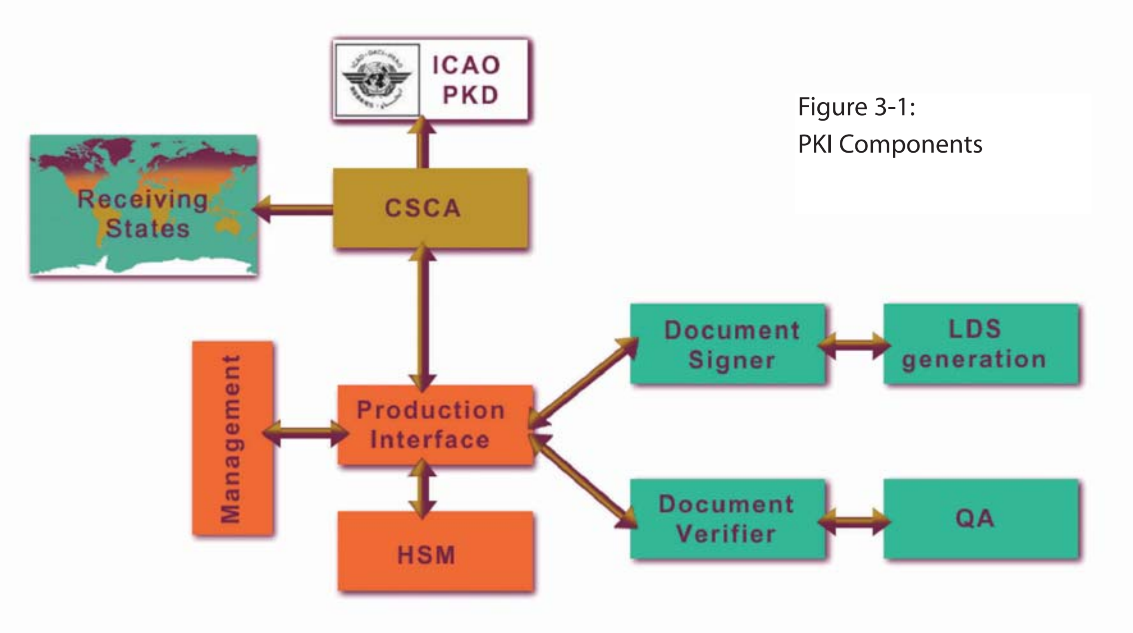


Figure 3-1:
PKI Components

## Country Signing CA (CSCA)

The CSCA is operated by (or on behalf of) the Issuing State and must be a secure installation with offline key generation and storage facilities using a CC certified HSM [*1,4,26*]. It is used to generate a key pair every 3 to 5 years; it is used to generate the resulting self-signed CCSCA, which is distributed by bilaterally agreed diplomatic means to each Receiving State, as well as electronically to the ICAO PKD using LDAP protected by SSL [*2,3,5,6,22,23,24*]. It is also used to generate the CDS to certificate the signing keys used in the DS at least every three months (or more frequently, especially if multiple DS keys are in use concurrently) [*7,10,11*]. The $C_{DS}$ must also be delivered electronically to the ICAO PKD using LDAP protected by SSL [*9,22,23,24*]. The CSCA must also generate a CRL at least every 90 days, and within 48 hours of a certificate being revoked. CRLs are to be distributed by multiple bilaterally agreed diplomatic means to each Receiving State, as well as electronically to the ICAO PKD using LDAP protected by SSL [*14,15,22,23,24,25*].

## Production Interface

The Production Interface provides the means to enable communication and interaction between the CSCA and the MRTD production facility. There may be multiple MRTD production facilities communicating with the State's CSCA. The Production Interface also ensures appropriate, timely and correct communication with the HSM. The Production Interface will not only provide the interface between the MRTD production facility and the HSM/CSCA, it will also provide the interface to the management facility.

## Hardware Security Module (HSM)

The HSM is a secure device that is designed to protect cryptographic keying material in use and in storage and should be Common Criteria (CC) certified. The HSM is used to securely generate key pairs, store them and use them to perform signing operations for the Document Signer and verification operations for the Document Verifier [*8,26*]. It may also act as a repository of the appropriate certificates from the CSCA.

### Management

Management will enable the MRTD production facility's requirements on the CSCA to be managed effectively. Thus it will provide the means to ensure the timely generation of new key pairs for the DS, certificate requests for the resulting public keys to be sent to the CSCA and revocation requests of compromised certificates to be sent to the CSCA [*8,10,11,14*].

### Document Signer (DS)

The DS is operated as a part of the MRTD production facility. It is passed the LDS Data Groups by the production facility and, through the Management Interface uses the HSM to perform the signing operation, generates and returns the $SO_D$ including the $C_{DS}$ for the production system to store in the MRTD IC chip [*8,12,13,27*].

### Document Verifier (DV)

The DV is operated as a part of the MRTD production facility. It is passed the LDS Data Groups and the SOD read from an MRTD IC chip by the production QA facility and, through the Management Interface uses the HSM to perform the signature verification operation, generates and returns a response to the QA system to verify the data in the MRTD IC chip [*8*].

### PKI Interfaces

An Issuing State's PKI will be required to interface with a number of external points.The interface to the ICAO PKD is specified in [PKITR] as LDAP on communications channels protected by server side authenticated SSL.

The interface to receiving states is specified in [PKITR] as existing bilateral diplomatic agreements between States, or newly established agreements where they don't currently exist. It is recommended that multiple channels be established to protect against Denial of Service attacks.

The production interface will be dependent on the passport production system.

The interface between the CSCA and the DS is not specified in the [PKITR] except in so far as the keys and certificates are identified and defined. In some environments the CSCA may be implemented as an integral part of the system and the interface can be chosen to be the most appropriate means of moving cryptographic material between the CSCA and the HSMs, probably using PKCS#11 [PKCS]. More usually, however, the CSCA will be a separate, externally operated facility. In that case, if it is a pre-existing facility, the interface is likely to be defined and enforced by the operating body. If not the same mechanism can be specified as would be used internally. ◆

**References**

**[BIOTR]** *Technical Report, Biometrics Deployment of Machine Readable Travel Documents*, Version 2.0, 21 May 2004, ICAO TAG MRTD/NTWG

**[BIOTRI]** *ANNEX I, Use of Contactless Integrated Circuits In Machine Readable Travel Documents*, Version 4.0, 5 May 2004, ICAO TAG MRTD/NTWG

**[BIOTRK]** *ANNEX K, ICAO Requirements for ePassports Interoperability*, Version 2, 6 July 2004, ICAO-NTWG ePassports Task Force

**[LDSTR]** *Technical Report, Development of a Logical data Structure – LDS for optional Capacity Expansion Technologies*, Revision 1.7, 18 May 2004, ICAO

**[PKITR]** *Technical Report, PKI for Machine Readable Travel Documents offering ICC read-Only Access*, Version 1.1, 01 October 2004, ICAO-NTWG, PKI Task Force

**[PKCS]** *Public Key Cryptography Standards*, RSA Labs, 1991+, http://www.rsasecurity.com/rsalabs/pkcs/

**[RFC3369]** *RFC 3369, Cryptographic Message Syntax*, August 2003

# Machine Readable Zone: 25 Years of Efficiency and Security

by ICAO Secretariat

**Reading the information in the Machine Readable Zone (MRZ)**

The MRTD follows a standardized layout to facilitate reading of data on a global basis by both eyes readable and machine readable means (global interoperability).

MRTDs produced in accordance with Doc 9303, incorporate an MRZ to facilitate inspection of travel documents. In addition, the MRZ provides verification of the information in the Visual Zone (VIZ) and may be used to provide search characters for a database inquiry. As well, it may be used to capture data for registration of arrival and departure or simply to point to an existing record in a database.

The MRZ provides a set of essential data elements in a standardized format that can be used by all receiving States regardless of their national script, language, or naming convention.

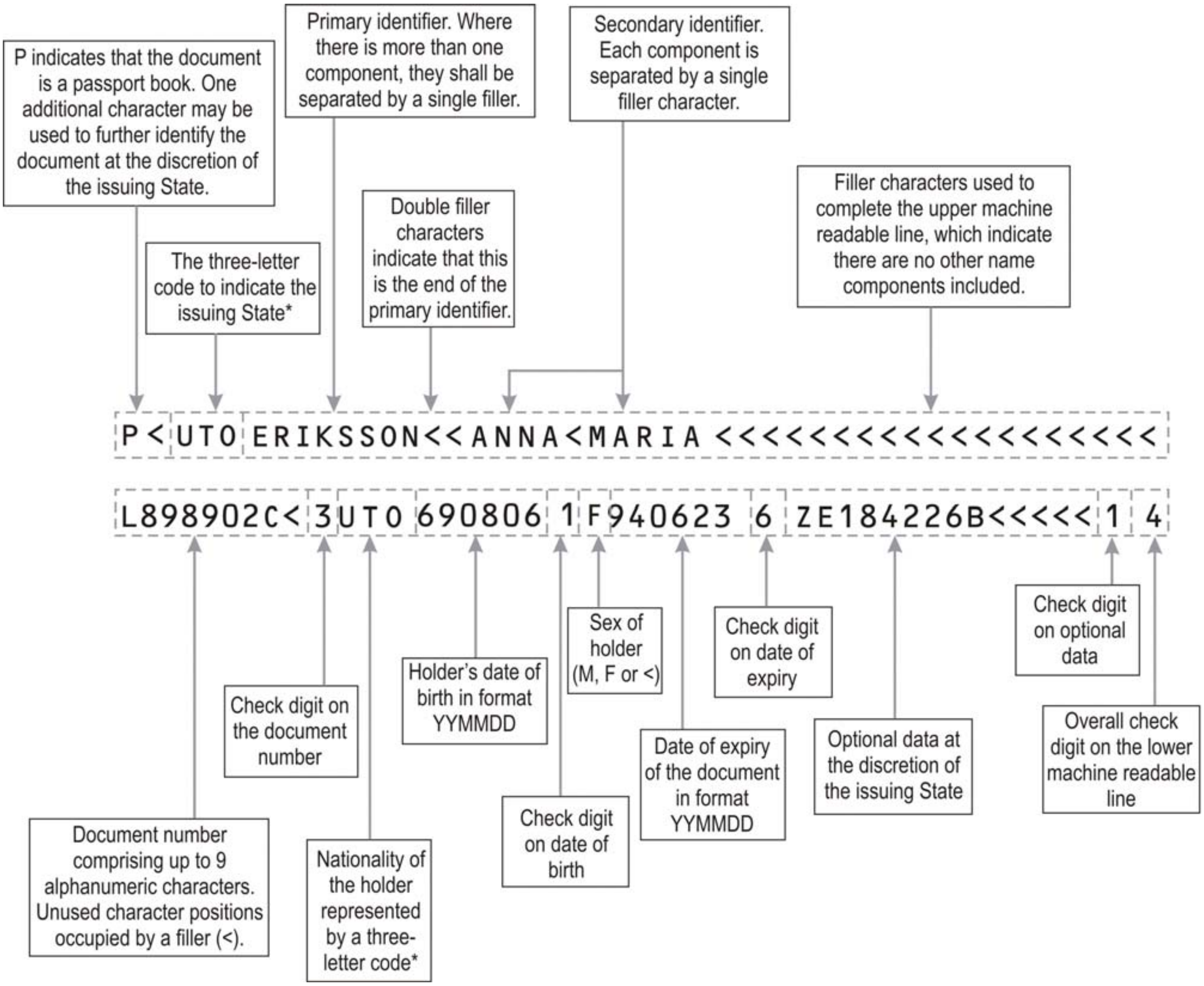
The data in the MRZ are formatted in such a way as to be readable by machines with standard capability worldwide. It must be stressed that the MRZ is reserved for data intended for international use in conformance with international Standards for MRPs.

In the interest of transparency, the data in the MRZ must be visually readable as well as machine readable. Data presentation must conform to a common standard such that all machine readers configured in conformance with Doc 9303 can recognize each character and communicate in a standard protocol (e.g. ASCII) that is compatible with the technology infrastructure and the processing requirements defined by the receiving State. National characters and diacritical marks cannot be used.

To meet these requirements, OCR-B typeface is specified in Doc 9303 as the medium for storage of data in the MRZ. The specified size is ten characters per inch (25.4 cm.)The MRZ as defined herein is recognized as the machine reading technology essential for global interchange and is therefore mandatory in all types of MRPs, whether conventional or ePassport.

**Security Features in the MRZ:**

When the MRZ is read by a machine, a series of calculations is done to verify the integrity of the data contained in the MRZ. For this, the data structure of the lower machine readable line provides for the inclusion of five check digits. Four check digits are calculated using a specific methodology with the alpha numeric characters contained in each field, while the fifth is a composite check digit calculated from all four fields and their check digits. When the machine reads the MRZ, it performs the respective calculations and compares the results with each check digit printed in the lower machine readable line, which should be the same. Any discrepancy would indicate that the passport is suspect – a possible forgery. ◆

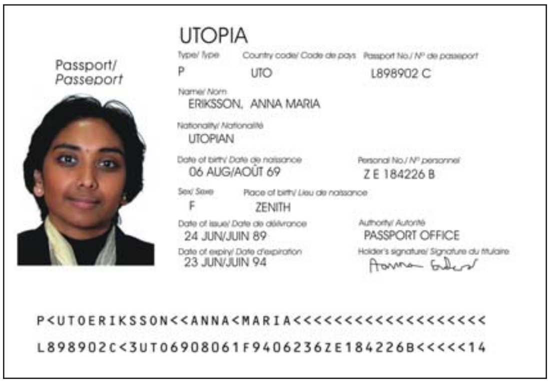

P indicates that the document is a passport book. One additional character may be used to further identify the document at the discretion of the issuing State.
The three-letter code to indicate the issuing State*
Primary identifier. Where there is more than one component, they shall be separated by a single filler.
Double filler characters indicate that this is the end of the primary identifier.
Secondary identifier. Each component is separated by a single filler character.
Filler characters used to complete the upper machine readable line, which indicate there are no other name components included.
P< UTO ERIKSSON<<ANNA<MARIA <<<<<<<<<<<<<<<<<<<
L898902C< 3 UTO 690806 1 F 940623 6 ZE184226B<<<<< 1 4
Document number comprising up to 9 alphanumeric characters. Unused character positions occupied by a filler (<).
Check digit on the document number
Nationality of the holder represented by a three-letter code*
Holder's date of birth in format YYMMDD
Check digit on date of birth
Sex of holder (M, F or <)
Date of expiry of the document in format YYMMDD
Check digit on date of expiry
Optional data at the discretion of the issuing State
Check digit on optional data
Overall check digit on the lower machine readable line

Source: ICAO Doc 9303, Part 1 Machine Readable Passports Volume 1 - Passports with Machine Readable Data Stored in Optical Character Recognition Format, 6th Edition - 2006.

# Examples of a Personalized Machine Readable Passport Data Page

(not to scale)

Example 1



UTOPIA

Passport/
Passeport

Type/ Type
P

Country code/ Code de pays
UTO

Passport No./ N° de passeport
L898902 C

Name/ Nom
ERIKSSON, ANNA MARIA

Nationality/ Nationalité
UTOPIAN

Date of birth/ Date de naissance
06 AUG/AOÛT 69

Personal No./ N° personnel
Z E 184226 B

Sex/ Sexe
F

Place of birth/ Lieu de naissance
ZENITH

Date of issue/ Date de délivrance
24 JUN/JUIN 89

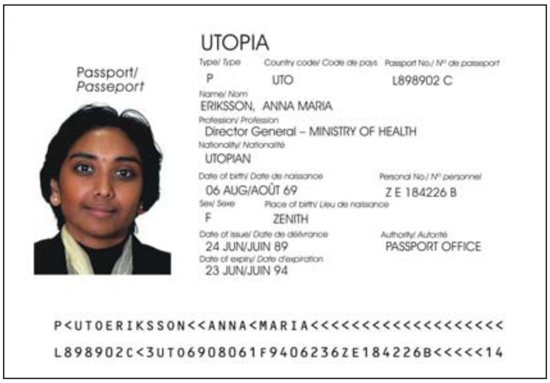
Authority/ Autorité
PASSPORT OFFICE

Date of expiry/ Date d'expiration
23 JUN/JUIN 94

Holder's signature/ Signature du titulaire
Anna Eriksson

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Example 2



UTOPIA

Passport/
Passeport

Type/ Type
P

Country code/ Code de pays
UTO

Passport No./ N° de passeport
L898902 C

Name/ Nom
ERIKSSON, ANNA MARIA

Profession/ Profession
Director General – MINISTRY OF HEALTH

Nationality/ Nationalité
UTOPIAN

Date of birth/ Date de naissance
06 AUG/AOÛT 69

Personal No./ N° personnel
Z E 184226 B

Sex/ Sexe
F

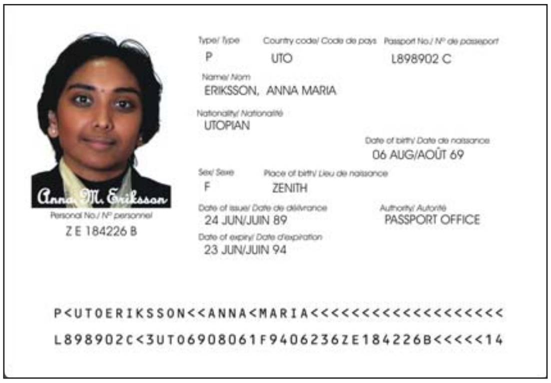
Place of birth/ Lieu de naissance
ZENITH

Date of issue/ Date de délivrance
24 JUN/JUIN 89

Authority/ Autorité
PASSPORT OFFICE

Date of expiry/ Date d'expiration
23 JUN/JUIN 94

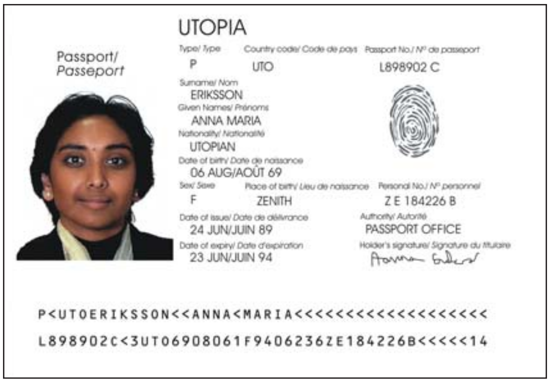
```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```



Type/ Type P
Country code/ Code de pays UTO
Passport No./ N° de passeport L898902 C
Name/ Nom ERIKSSON, ANNA MARIA
Nationality/ Nationalité UTOPIAN
Date of birth/ Date de naissance 06 AUG/AOÛT 69
Sex/ Sexe F
Place of birth/ Lieu de naissance ZENITH
Date of issue/ Date de délivrance 24 JUN/JUIN 89
Authority/ Autorité PASSPORT OFFICE
Date of expiry/ Date d'expiration 23 JUN/JUIN 94
Anna M. Eriksson
Personal No./ N° personnel Z E 184226 B

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Example 3



UTOPIA
Passport/ Passeport
Type/ Type P
Country code/ Code de pays UTO
Passport No./ N° de passeport L898902 C
Surname/ Nom ERIKSSON
Given Names/ Prénoms ANNA MARIA
Nationality/ Nationalité UTOPIAN
Date of birth/ Date de naissance 06 AUG/AOÛT 69
Sex/ Sexe F
Place of birth/ Lieu de naissance ZENITH
Personal No./ N° personnel Z E 184226 B
Date of issue/ Date de délivrance 24 JUN/JUIN 89
Authority/ Autorité PASSPORT OFFICE
Date of expiry/ Date d'expiration 23 JUN/JUIN 94
Holder's signature/ Signature du titulaire

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14
```

Example 4

For the correct measures of the passport data pages, please see, Appendix 2 and 3 to Section IV of the ICAO Doc 9303, Part 1 Machine Readable Passports Volume 1 - Passports with Machine Readable Data Stored in Optical Character Recognition Format, 6th Edition - 2006.

EDAPS
CONSORTIUM

ЕДАПС
КОНСОРЦІУМ
ПАСПОРТ
PASSPORT
PASSEPORT
PASSAPORT
PASSAPORTO
UTO01234567
01 DEC 1994
EDAPS CONSORTIUM
01 DEC 2014
PRESENT<UTOPIA<IVANOVA<IVANNA<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
AA12345678PRS<123456789TOPIA<0000012345678<<<<<<<<<<<<048

## PASSPORT

Passport documents are booklets with a polycarbonate page containing personal data of the document holder.

A combination of state-of-the-art materials and advanced technologies utilized for blank form manufacturing as well as personal data page shall provide a higher level of anti-fraud protection.

Availability of a personal data page as well as utilizing laser-engraving and laser perforation for data entering shall be an effective tool for meeting all the requirements imposed for passport documents manufacturing

## DRIVING LICENSE

Driving license is a plastic card type document on multilayer polymer base with both sides protected by the film containing holographic security elements as well as by transparent film which adds to its higher durability.

Driving license being manufactured in conformity with the International Standards includes a set of state-of-the-art security features, namely: anti-scanner grids, micrographics and printing elements implemented with special inks.

Driving Licenses contain the holder's personal information written in Latin letters that meets the requirements of the UN Road Traffic Convention.

**EDAPS CONSORTIUM** BEING A SYSTEM INTEGRATOR, DEVELOPS AND IMPLEMENTS COMPUTER-CONTROL RECORDING AND INFORMATION MANAGEMENT SYSTEMS IN ALL SPHERES OF GOVERNMENT AND PRODUCTION ACTIVITIES THAT ALLOWS US TO OFFER "TURN-KEY" SOLUTIONS UTILIZING STATE OF THE ART INTEGRATED PRODUCTS.

# The EDAPS Consortium: Development and manufacturing of passport and other identity documents utilizing the most advanced technologies.

## VEHICLE REGISTRATION CERTIFICATE

The EDAPS Consortium is now producing Vehicle Registration Certificates as plastic cards in accordance with international standards.

These cards have eight security levels. Except for the microtext, printed in the smallest font, the document blanks have inscriptions executed using daylight invisible ink, visible only under ultra-violet radiation.

An optical security element is also embedded into every blank. There are special antiscanner background grids plotted into the document in order to prevent their replication.

## CREW MEMBER IDENTITY DOCUMENT

Crew member identity document is a machine-readable travel document manufactured as a passport card of standard size developed in conformity with ICAO requirements.

Both document covers contain background graphics including all the security elements specific for high security documents.

Special security inks as well as special holographic security element contribute to higher document protection.

WE CAN PROVIDE THESE SOLUTIONS AND PRODUCTS IN A VERY COST EFFECTIVE WAY FOR YOUR GOVERNMENT OR PRIVATE SECTOR PROJECT.

CONTACT US TO LEARN MORE!

| Address: | Telephones: | Fax: | E-Mail: | WWW: |
|---|---|---|---|---|
| 64, Lenina Str.<br>Kiev, Ukraine, 02088 | +38 (044) 561-25-90<br>+38 (044) 561-25-89 | +38 (044) 561-25-85 | edaps@edaps.biz | http://www.edaps.biz |

# An innovative new website INTERNATIONAL FORUM FOR TRAVEL DOCUMENTS, the IF4TD.

by Sjef Broekhaar
Ministry of Interior and Kingdom Relations, The Netherlands

Issuers of travel documents and identity cards now have a new vehicle for exchanging technical information and development news with their peers in other governments worldwide. Called the IF4TD, the International Forum for Travel Documents is an online discussion forum for issuing authorities across all regions of the world, and is accessible only to members. The website is secured by the use of usernames and passwords, and only government officials and members of the advisory board can gain access.

The objectives of the IF4TD are:

- To be a single point of contact/reference for technical information on all passport/travel documents and identity card related issues as well as issuing systems of participating member countries/territories.
- To share documents, experience etc. via the website.
- To use the website to conduct online surveys.

The IF4TD comprises four regions - Europe, America, Africa and Asia Pacific. Each region will have a regional representative and a deputy regional representative. These representatives form a Standing Committee to manage the operation of the IF4TD.

The membership of the IF4TD is on country/territory basis. Admission is voluntary. No admission fee is required. Members are free to join and leave. To become a member of the IF4TD, the relevant issuing authorities need only to complete the following formalities:

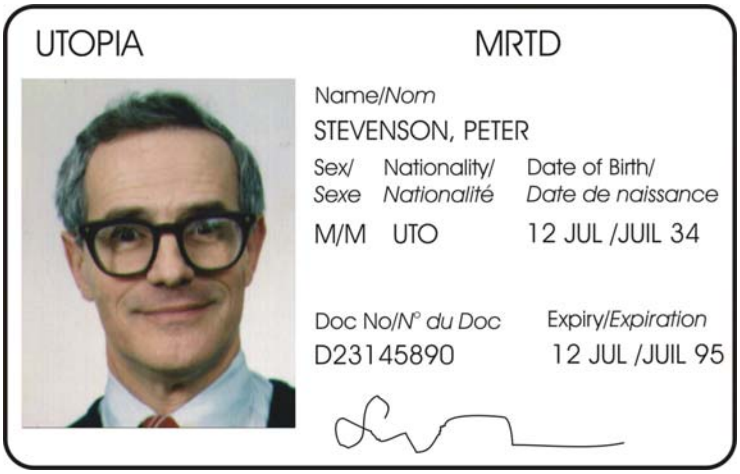
1. To appoint one or more officials who will become a contact person for other members worldwide.
2. To complete the 'Members Profile Form'. The Members Profile is an overview how the issuing process in the particular country/territory is organized.
3. To keep this information up to date.

In an era in which the processes around the production, personalization and issuance of those documents are becoming more and more complex, the IF4TD provides a worldwide network facilitating efficient and effective communication among members. Information gathered is valuable for research and planning purposes. Currently, 42 ministries/ organizations from 37 countries/ territories have become members of the IF4TD, and the Forum is still expanding. Applications for new memberships are welcome.

For more information please contact Sjef Broekhaar, Regional Representative for Europe at the following e-mail address: sjef.broekhaar@bprbzk.nl ◆

# The ICAO machine readable official travel document/ID card: keeping it simple and globally interoperable

by ICAO Secretariat

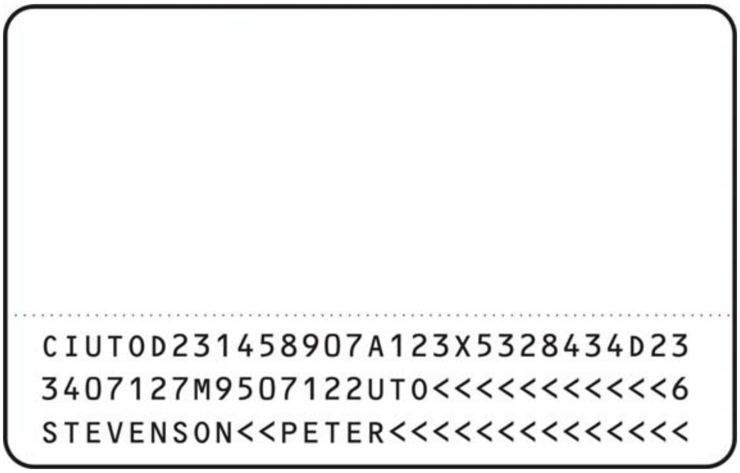


UTOPIA MRTD

Name/Nom
STEVENSON, PETER

| Sex/<br>Sexe | Nationality/<br>Nationalité | Date of Birth/<br>Date de naissance |
|---|---|---|
| M/M | UTO | 12 JUL /JUIL 34 |

| Doc No/N° du Doc | Expiry/Expiration |
|---|---|
| D23145890 | 12 JUL /JUIL 95 |



```
CIUTOD231458907A123X5328434D23
3407127M9507122UTO<<<<<<<<<<<6
STEVENSON<<PETER<<<<<<<<<<<<<<
```

Having published the new ePassport specifications in the Sixth Edition of Doc 9303, Part 1, ICAO and its ISO partners now turn their attntion to finalizing the new specifications for biometrically enhanced eMRTDs. Known as "machine readable official travel documents" these are the size-1 and size-2 cards issued by States as official documents of identity and with the intent that they may be used as international travel documents. The updated specifications have been under development by experts in the TAG/MRTD and, when finished, will be published as the Third Edition of Doc 9303, Part 3.

Readers of the new Part 3 can expect to find the extensive specifications for implementing the ICAO Blueprint for incorporating biometric identification in travel documents, similar to those detailed Volume 2 of Part 1. On the other hand readers may be surprised to find that the discussions of options for deploying biometrics and choices of data storage technologies have been substantially simplified, particularly with respect to the size-1 ("wallet size") plastic card.

**Doc 9303, Part 3, current edition (2002)**

The current edition includes "specifications" (maximum dimensions and locations) for several optional technologies for data storage that might "coexist" on a wallet-size card, including magnetic stripe, 2-dimensional barcodes, optical memory, integrated circuit chip with contacts, and contactless chip. The dimensions and locations for all of these technologies were specified, not only to allow for more than one to be carried on the same card, but also to ensure that they did not interfere with or displace the machine readable zone (MRZ) and other mandatory data. No expectation of global interoperability of these technologies was given and none was intended. Rather, what was contemplated and explained in the specifications was that they might be used to store data for the State's own use or for a bilateral travel arrangement, e.g. between or among States sharing a common land border.

### Doc 9303, Part 3, next edition (2007)

Nevertheless the presence of these "specifications" conveyed the erroneous impression that the use of these optional data storage technologies was part of the ICAO standard. In order to reduce confusion and to update the published specifications in keeping with the evolution of thinking in ICAO, the next edition of Doc 9303, Part 3 will specify only the MRZ and the contactless chip. Why? Because these two technologies are all that is required for an ICAO-standard, globally interoperable ID/travel card.

### Options still available to States

An issuing State may continue to exercise its discretion and decide to place an additional, optional data storage technology on the Size-1 card for the purpose of storing additional data deemed necessary by that State. However, the following cautionary notes are offered to a State making such a decision:

1. The issuing authority needs to understand that such additional stored data can be for home use or bilateral use only. High-capacity technologies other than the chip, encoding devices such as templates, and/or reading systems for other than the contactless chip are not globally interoperable.

2. Since the number of other countries reading the stored data would be limited, consider the added expense against the value of storing additional data on the card as opposed to keeping it in a data base that can be accessed. The amount of storage space needed should also be considered; a technology that offers excessive space may not be cost-effective.

3. If a technology in addition to the contactless chip is elected, such technology shall be located so as not to interfere with or cause displacement of any of the mandatory data on the card, including the MRZ. Otherwise the result would be a non-compliant card and the information presented in the visual zone would be compressed to a size difficult to read.

4. A possible, partial exception could be made for the chip with contacts, the correct placement of which would require the photo to be placed on the right-hand side of the card, while the MRZ remained in its mandatory location on the back of the card.

In any of the above cases, in order for the biometrically enhanced card to qualify as an ICAO-compliant, globally interoperable eMRTD both the contactless chip and the MRZ are required. ◆

# DATACARD GROUP

SECURITY, EXPERTISE AND EXPERIENCE

## END-TO-END SOLUTIONS FOR GOVERNMENT IDENTIFICATION PROGRAMS

To issue secure travel documents and ID cards, you need a solutions provider that understands government identification. You need a provider with expertise in every phase of data capture, entitlement and production. And you need a provider with a complete portfolio of software, systems, supplies and services.

That solutions provider is Datacard Group. We have more than 30 years of experience with secure ID programs, and we have deployed solutions in more than 65 countries. In other words, Datacard Group knows what it takes to issue secure documents. Whether you are integrating biometrics with contactless technology, formatting data to the ICAO standards, providing a secure framework to manage data or personalizing documents with secure technology, our solutions can help you enhance security.

In fact, our new Datacard® PB6500™ passport issuance system is highly flexible, so you can easily integrate the latest technologies. It offers color printing, laser engraving, number perforation, security laminates, secure verification and much more.

Talk to Datacard Group today to find out how we can help you protect your program, your documents and your investment.

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

| | |
|---|---|
| PHONE (U.S): | +1 952 933 1223 |
| PHONE (UK): | +44 (0) 1489 555 600 |
| E-MAIL: | INFO@DATACARD.COM |
| WEB: | WWW.DATACARD.COM |

# International Cooperation Keeps Brazil Passport Project on Track

by Mauricio Siciliano and Isabel Baltazar

The worldwide harmonization of standards, specifications and practices related to MRTDs can best be achieved through global cooperation and dialogue among States. This premise was again validated with an ICAO mission to Brazil in December 2005, under the auspices of the Organization's Universal Implementation of MRTD (UIMRTD) Programme.

The Programme is aimed at States that have not yet implemented and/or issued MRTDs. It consists of an in-depth situation analysis, including the identification of needs and resources or assistance required, as well as recommendations for increasing MRTD security in the issuance and control processes, all according to ICAO standards.

The specific objective of the Brazil mission was to assist Government authorities meet Standard 3.10 of Annex 9 – Facilitation, by which "Contracting States shall begin issuing only Machine Readable Passports in accordance with specifications of Doc 9303, Part 1, no later than April 2010".

The two-member mission team consisted of Mauricio Siciliano, from the Security and Facilitation Branch of ICAO and Isabel Baltazar, on loan from the Portuguese Immigration Service for this project. Together, in consultation with Brazilian officials, they were able to assess the preparedness of Brazil to launch a new passport in 2006 and make practical suggestions for adjusting their passport programme. Characteristically, the exercise comprised five elements:

1. Explain ICAO's requirements and specifications regarding the issuance and use of travel documents;

2. Become acquainted with reports from each entity involved in the issuance process of the new Brazilian Passport;

3. Determine basic areas where Brazil required assistance;

4. Accordingly, help identify States and organizations that could cooperate with the issuance and proper use of the machine readable zone (MRZ), in conformity with ICAO requirements, and also identify potential international partnerships in the field of security ID and Travel documents, namely capacity building, expertise, training and equipment needs, amongst others;

5. Propose general recommendations concerning issuance, personalization and passport use procedures, as required by ICAO.

The scope and comprehensiveness of the mission was made possible by the excellent cooperation of local Brazilian officials: Carlos Roberto, Casa da Moeda du Brazil – the Brazilian Mint and organizers of the mission; Rogério Galloro, from the Federal Police Department, who helped coordinate the mission; Wilton Motta, from SERPRO; Pedro Bittencourt de Almeida, the Representative of Brazil to ICAO; and Fernando Cerdeira, Brazilian Civil Aviation Authority.

From left to right Wilton Mota , Manager of Strategic Businesses (SERPRO); Mauricio Siciliano from ICAO; Isabel Baltazar from the Portuguese Immigration Service; Rogério Augusto Galloro, from the Federal Police Department and Executive Coordinator of the Passport Project; Marcos Vinicius, Manager of Marketing (SERPRO); Carlos Roberto, Director of Technology from Casa da Moeda do Brasil (Brazilian Mint); Raimundo Nonato from the Federal Police and Chief of the Center of Information Technology.

The willingness of Brazil to take full advantage of the UIMRTD Programme led to strategic visits to the passport assembly and personalization facilities located in the Casa da Moeda, in Rio de Janeiro, and the Federal Police facilities and SERPRO offices, both located in Brasilia. Meetings there proved essential to providing high-level recommendations.

Based on the successful outcome of the ICAO mission, and taking into account the assessment contained in the mission report and to further assist the State, the Government of Portugal, through the Portuguese Immigration Service, offered Brazil considerable tangible support in three fundamental areas:

- *E*-Documents - **To share** its know-how, expertise and experience relating to the Portuguese Electronic Passport project (image acquisition, data processing, passport production and e-readers), to be implemented this summer;

- Biometry – **To extend** this assistance to various applications of biometrics such as those being undertaken in Portugal, namely Passports, ID Cards, Residence Permits for foreigners and visas;

- Training – **To cooperate** in terms of technical training. Portugal has been promoting different training events, nationally and within the European Union training structure. Two-week Seminars on Security Documentation and on Polymer Substrates are examples that could be duplicated or adapted to Brazil.

Missions such as this one to Brazil under the UIMRTD Programme are yet another example of the role of ICAO in enhancing intergovernmental cooperation, in this case for the implementation of a global system aimed at facilitating the movement of passengers at airports and enhancing security through the reduction of document fraud.

For more information on the UIMRTD and ICAO assistance to States on MRTD, please visit our web site at www.icao.int/mrtd. ◆

# ICAO Contracting States

## NORTH AMERICA
Canada
United States

## CENTRAL AMERICA
Belize
Costa Rica
El Salvador
Guatemala
Honduras
Mexico
Nicaragua

## CARIBBEAN
Antigua and Barbuda
Bahamas
Barbados
Cuba
Dominican Republic
Grenada
Haïti
Jamaica
St. Kitts and Nevis
St. Lucia
St. Vincent and the Grenadines
Trinidad and Tobago

## SOUTH AMERICA
Argentina
Bolivia
Brazil
Chile
Colombia
Ecuador
Guyana
Panama
Paraguay
Peru
Suriname
Uruguay
Venezuela

## EUROPE
Albania
Andorra
Armenia
Austria
Azerbaijan
Belarus
Belgium
Bosnia and Herzegovina
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Hungary
Iceland
Ireland
Italy
Kazakhstan
Kyrgyzstan
Latvia
Lithuania
Luxembourg
Malta
Monaco
Netherlands
Norway
Poland
Portugal
Republic of Moldova
Romania
Russian Federation
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Tajikistan
The former Yugoslav Republic of Macedonia
Turkey
Turkmenistan
Ukraine
United Kingdom
Uzbekistan

## MIDDLE EAST
Afghanistan
Bahrain
Iran, Islamic Republic of
Iraq
Israel
Jordan
Kuwait
Lebanon
Oman
Qatar
Saudi Arabia
Syrian Arab Republic
United Arab Emirates
Yemen

## AFRICA
Algeria
Angola
Benin
Botswana
Burkina Faso
Burundi
Cameroon
Cape Verde
Central African Republic
Chad
Congo
Côte d'Ivoire
Democratic Republic of the Congo
Djibouti
Egypt
Equatorial Guinea
Eritrea
Ethiopia
Gabon
Gambia
Ghana
Guinea
Guinea-Bissau
Kenya
Lesotho
Liberia
Libyan Arab Jamahiriya
Madagascar
Malawi
Mali
Mauritania
Mauritius
Morocco
Mozambique
Namibia
Niger
Nigeria
Rwanda
Sao Tome and Principe
Senegal
Seychelles
Sierra Leone
Somalia
South Africa
Sudan
Swaziland
Tanzania, United Republic of
Togo
Tunisia
Uganda
Zambia
Zimbabwe

## ASIA/PACIFIC
Australia
Bangladesh
Bhutan
Brunei Darussalam
Cambodia
China
Comoros
Cook Islands
Fiji
India
Indonesia
Japan
Kiribati
Korea, Democratic People's Republic
Lao People's Democratic Republic
Malaysia
Maldives
Marshall Islands
Micronesia, Fed. States of
Mongolia
Myanmar
Nauru
Nepal
New Zealand
Pakistan
Palau
Papua New Guinea
Philippines
Republic of Korea
Samoa
Singapore
Solomon Island
Sri Lanka
Thailand
Timor-Leste
Tonga
Vanuatu
Viet Nam

# Behind the scenes in ICAO – NTWG wins award for designing the ePassport

## How Smart Card Chips Found Their Way Into Passports

by Kevin Woodward, associate editor
Card Technology magazine

*Reprinted with permission from Card Technology.*

In the mid-1990s, when the International Civil Aviation Organization set out to survey various technologies for possible use in the next generation of passports, there were no assurances smart card chips would make the list. The odds were even greater against contactless smart card technology, which was still in its infancy.

But that was 1997, when ICAO's New Technologies Working Group, made up of representatives of passport-issuing government agencies, was just beginning its work. By 2003, ICAO had come to the conclusion the best technology available to better verify the identity of travellers was contactless smart card chips that could carry biometric data on the passport-holder.

Contactless technology had come a long way, but there was still much to do. The New Technologies Working Group has spent the past three years feverishly resolving all the issues involved in creating a secure document that could potentially be used by 500 million travellers worldwide.

That work has paid off with some 40 nations preparing to issue electronic passports that conform to an ICAO-developed specification. The result is to introduce smart card technology into an arena - passports - in which it has never been used before.

It comes as little surprise then that ICAO's New Technologies Working Group has won this year's *Card Technology* New Markets Breakthrough Award for opening up a new market for smart card technology with its passport specification. Two other smart card initiatives were finalists in the category.

Gary McDonald, chairman of the working group, says the award should be shared with an International Organization for Standardization committee that has worked closely with the ICAO group on the technical elements for epassports.

McDonald's group is primarily comprised of government officials, and he says they recognized early on the need to work with ISO, along with other technologists, airport officials and law enforcement agencies.

"Our job was to develop some of the technology solutions," says Joel Shaw, convener of ISO Working Group 3, which aided McDonald's group." (ICAO/NTWG) established a suite of specifications that were acceptable worldwide. And that was no small feat. What ISO did was try to contribute in some of these difficult areas, like PKI and contactless chips." PKI, or public key infrastructure, is used in passports to verify that an authorized national agency produced the passport.

"The goal we set for ourselves in 1997 was very broad," McDonald recalls. "We were tasked by ICAO to explore the incorporation of advanced technologies into travel documents to improve security. When we started this in work in 1997 we had a blank page in front of us."

The underlying idea was that somehow advances in card technology and in the printing and securing of documents would lead to more secure passports that did a better job of verifying identity without impeding the movement of people, McDonald says.

The strategy that eventually surfaced had four elements, he says. First, the working group needed to determine what data to collect. Second, how would this data be stored in a new travel document? Third, some biometric was needed to link the document to the traveller, McDonald says, but which one? And, last, how would all this information be secured?

With that framework in place, the working group set out, beginning in 1999, to define how the data would be structured, McDonald says. "In parallel with that, we were dealing with the whole issue of data storage." he says.

Smart cards were considered, as were optical media and two-dimensional bar codes, among others, he adds.

Fingerprints were considered and initially dismissed because each vendor had its own technology for analyzing and comparing fingerprints. ICAO wasn't going to choose just one vendor's biometric technology for use on passports.

Instead, a facial image was chosen as the mandatory identifier because it is a biometric that can be read by a variety of readers and software, McDonald says. It was also considered the least-intrusive biometric since passport-holders already submit photos for conventional passports. But ICAO permitted fingerprints to be used as an optional biometric identifier.

The solution was to store the entire facial image on the chip, so any vendor's software could work with the image. But that meant storing relatively large amounts of data. Facial images range from 8 kilobytes to 32K, according to an interoperability test conducted in Singapore in November.

"The next issue was how do you secure chips in paper," McDonald says. While there were contact smart cards that could hold a chip in plastic, passport agencies were not willing to abandon the booklet format they had been using for many years in favour of a plastic passport card. Contactless chips, which were just emerging were picked, McDonald says, because they could work with paper or plastic documents.

"We had to take leaps of faith," he says. "We knew, for example, that 32K contactless chips did not exist. We knew the industry was coming out with 8K chips at that time."

"Fundamental to these choices was the working group's perspective." We weren't writing a specification for 2002,"" McDonald recalls." We knew we were writing a specification for 2004 to 2005."

And in doing so, it was breaking ground by combining contactless chips and travel documents.

"We knew we were proposing something different," McDonald says. ◆

# Preparing for ePassports

## - laying the foundations for implementing secure, trustworthy and cost-efficient ePassport programmes

by Paul Wilson,
Managing Director, De La Rue Identity Systems

In the last 25 years, the passport has evolved in line with the growth in global travel, with the result that the machine-readable passport (MRP), first introduced in 1981, has become the familiar standard now issued by approximately 140 countries.

Now the 21st century challenges of migration, identity theft, cross-border crime and terrorism are instigating a period of much more rapid change to which governments and international organisations are already responding. This has brought us to a point where, by the end of this year, some 40 countries will have implemented an ePassport programme that is compliant with new international standards.

### International standards for ePassports

On 28th May 2003, ICAO adopted a global, harmonised blueprint for the integration of biometric identification into passports and other MRTDs. The blueprint consists of four parts: the facial image, the contactless proximity chip, the logical data structure, and the PKI. ICAO details its requirements for ePassports in its Doc9303-part 1 and supporting documents.

The EU Council Regulation adopted on 13th December 2004 mandates the inclusion of a digital facial image in all EU passports by 28th August 2006. It supplements the ICAO standard by also requiring the inclusion of fingerprints in EU passports by 28th February 2008.

Since 26th October 2005, U.S. Visa Waiver Programme members have had to include digital photographs in their MRPs and have an "acceptable plan" to issue ePassports within one year.

Adopting an ePassport not only improves security, but can also facilitate passenger processing and provide better services to passport holders. There can also be indirect economic benefits. An ePassport can provide:

- more precise matching of documents to people and better authentication of document data
- heightened international travel security, particularly aviation security
- greater protection against identity theft, fraud and counterfeit
- easier inspection by government and airline officials
- more efficient processing of travellers at check points
- improved customer service through integration with eGovernment
- easier access to visas and even visa-free travel programmes

Nevertheless, the majority of ICAO's 189 Contracting States are still using conventional passports and many may wish to do so for some time to come. As ePassports become a de-facto standard, how will the governments of these countries prevent their citizens facing increasing challenges to immigration and travel?

**Building on solid foundations**

The answer is to lay the foundations for a successful future ePassport programme now when specifying, developing and implementing conventional MRP documents and systems. And to do so in accordance with the guidelines of the ICAO blueprint. Ultimately, this will ensure that, when the government decides the time is right, its ePassport upgrade path will be fast, smooth and cost-efficient.

### A systematic approach

Of course, the components of an ePassport programme are no panacea, merely useful technologies that enhance passport and passport issuing procedures. Therefore, as with any government document issuing programme, when putting the building blocks of an ePassport programme in place it is essential to address every stage of the passport lifecycle to ensure that the whole system is efficient, robust and secure.

### Application Process

A large part of the change to the application process, both for first issuance and renewal, is accommodating biometric data capture and verification. Governments will benefit from capturing biometric data as early as possible even if it is not used immediately on the passport. Biometrics can be used to enhance the background checks made during the application process and to reduce the opportunities for fraudulent applications by freezing the link between the biometric and one identity.

As the only globally-interoperable biometric, facial recognition should be addressed as the priority. This is the time to review existing image databases to normalise quality. Similarly, data capture technology should be reviewed and, if necessary, upgraded to ensure all new images captured are compliant with ICAO's photograph guidelines and compatible with facial recognition technology once it is implemented[1].

States can also consider whether to deploy a second biometric for their own or bilateral use. This is particularly relevant if the State has an existing fingerprint or iris database from another government programme, for example its national identity card, against which it can verify biometrics submitted with passport applications.

To ensure that the identity of the applicant is properly established at this crucial stage and that ePassports are not being issued to people who are not entitled to them or in false identities, this is also the opportunity to audit the current system to identify weak points and to determine where to employ new technologies and processes to improve system reliability and security. Considerations might include:

- A review of breeder documents: are sufficient checks made to confirm the legitimacy of breeder documents submitted with passport applications? More fundamentally, are accepted breeder documents secure and securely issued? If not, they may be used all too easily to support fraudulent passport applications.
- The introduction of a face-to-face interview process as in, for example, the UK where the Identity and Passport Service is establishing a network of 69 new interview offices for first-time applicants. Face-to face interviews are an excellent way to establish identity and nationality and act as a deterrent to fraudulent applicants.
- Any necessary changes to the legal framework.

**Document Production, Personalisation and Issuance**

Moving towards an ePassport programme allows States to reengineer passport production, personalisation and issuance for greater security and better service to citizens. This is the opportunity to consider:

- Ensuring the physical security of passport production and issuing sites up to the levels required to hold a PKI signer[2].
- Ensuring the physical security of all materials against theft through a secure audit trail of all non-commercially available materials and security accounting procedures that control passport blanks and consumables.
- Putting in place procedures to secure the issuing process against fraud.
- Testing to ensure passport book durability exceeds the required standards and can easily include a chip at a later stage[3]. Governments could also consider reducing passport validity from ten to five years to allow faster adoption of more sophisticated security print, biometric, chip and chip security technologies and more regular rechecking of passport applications with new technologies and techniques.
- Trialling the PKI first on a small scale, for example with diplomatic ePassports.
- Installing document issuing software that is ICAO-compliant and has an easy ePassport upgrade path.

ICAO publishes further recommendations on securing document production and issuance in its Doc 9303 standard.

### Document verification and usage

Biometrics in ePassports will help to confirm identity at border control, bringing benefits for immigration officials and travellers alike. However, in order to reap maximum benefit, here again preparation is essential before implementation.

To aid inspection at its own borders, a State needs to put robust infrastructure and procedures in place:

- to verify the identity of citizens and visitors, perhaps using new, automated systems
- to handle exceptions and process secondary inspection
- to ensure officials can inspect an ePassport and its bearer by means of machine-assisted or visual inspection.

To aid inspection of its citizens at foreign borders, a State needs:

- to ensure its ePassport complies with ICAO's interoperability standards so that it can be validated and authenticated by the receiving state[4]
- to ensure that the ePassport and its bearer can be inspected by means of machine-assisted or visual inspection.

To achieve both, we recommend that the State work with a supplier which scored highly in recent global interoperability tests and initially trial its ePassport alongside its current passport to identify and resolve any issues.

### Communication

While laying the foundations of an ePassport programme, it is important to maintain positive and proactive communication with stakeholders: citizens, passport service staff, parliament, media, etc. Good communication is critical to success because it will ensure that the reasons for and nature of the move to an ePassport are understood and accepted rather than criticised and rejected.

Messages should be kept simple and targeted at the right audience at the right time using the most appropriate method of communication. States can learn from previous examples of successful communications in similar fields, including the introduction of the euro and the forthcoming launch on U.S. driver's licences of a new common holographic security feature which will be supported by a high profile public education campaign.

### Securing ePassport success

Putting ePassport procedures and technologies in place early so that the move to an ePassport programme can take place easily once the decision is taken to do so will bring numerous and significant benefits to a State's government and

citizens. The government will benefit from a swift, straight-forward upgrade path, implementation timing to suit its programme, managed costs, tried and tested systems, proven security, improved identity confirmation at application, and better facilitation and enforcement at border control. Meanwhile, its citizens will clear border controls faster and find it easier to obtain visas and make travel arrangements.

Therefore, all governments should now carefully consider an ePassport upgrade path when specifying a new passport document and/or system and ensure that their chosen supplier has the breadth and depth of expertise, understanding and experience to support this. This way, governments will achieve a secure, trustworthy and cost-efficient conventional passport programme now and a secure, trustworthy and cost-efficient ePassport programme in the future. ◆

[1] Reference: ICAO Biometrics Deployment Technical Report, Annexes A-D

[2] Reference: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, v1.1; Development of a Logical Data Structure – LDS For Optional Capacity Expansion Technologies, revision 1.7

[3] Reference: ICAO Biometrics Deployment Technical Report, Annex I – Contactless IC's Supplementary Information, v4.0

[4] Reference: ICAO Biometrics Deployment Technical Report, Annex K – ICAO Requirements for ePassports Interoperability, v2.6

# Staying on top of new technology

## NTWG to issue new RFI in 2007

by Gary McDonald, Passport Canada
Chairman, New Technologies Working Group

The New Technologies Working Group (NTWG) of the ICAO TAG/MRTD plans to publish its fifth Request for Information (RFI) in the second quarter of 2007. Suppliers of relevant products and services will be invited to make presentations on new and emerging technologies that could support the NTWG's developmental work on international standards related to the issuance and use of machine readable travel documents (MRTDs). For more information on the RFI, please visit our web site: www.icao.int/mrtd.

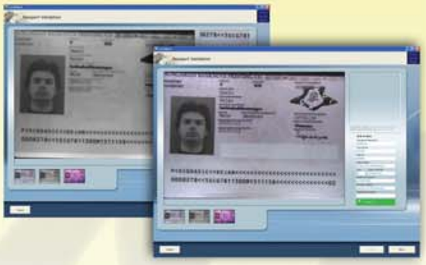
The NTWG, comprised of government officials in passport issuance and border control and supported by technical experts from the International Organization for Standardization (ISO), has been responsible for studying new technology applications and generating the technical work on which ICAO standards on ePassports, identity verification and document authentication have been based. To equip itself for its continuing work NTWG issues an RFI every three years in order to keep itself abreast of new developments and improvements in technology.

The RFI published in 2004 attracted 97 proposals for presentations in the following categories: biometrics, data storage media, e-commerce, RF technologies, self-service facilitation, travel document printers, readers and security concepts. From these, 28 firms were selected and invited to make oral presentations. It was evident that many vendors had participated with member States in refining the emerging interoperability standards, and although several products were suitable for implementation then, many more would be available in the near future. That time is now.

In September 2006 the NTWG will determine the categories and requirements for new technologies to be sought via the 2007 RFI. Key to all submissions from vendors is that the technology applications must be presented in the context of ICAO Doc 9303, which defines specifications for machine-readable passports, visas, and other official travel documents. Orders to purchase Doc 9303, Parts 1, 2, and 3 should be directed to sales@icao.int or on line through the ICAO web site, www.icao.int. ◆

# VLATACOM

## ICAO e-Passport Compliant
## **Document Reader**



**Full page, one step optical and chip reading of:**

- *ICAO Doc. 9303 compliant documents (ID1, ID2, ID3)*
- *national documents (ID cards, driving licenses, working permits,...)*

**Features:**

- ***Optical Reading***

- high resolution (400 dpi) images in visible, IR and UV illumination
- UV and IR security features
- MRZ OCR-B decoding and verification
- 2D barcode decoding PDF 417
- verification of 3M confirm passport security foil using coaxial light (optional)

- ***Chip Reading***

- contactless ISO/IEC 14443A&B
- ICAO e-Passport LDS1.7 and PKI1.1 compliant
- contact ISO/IEC 7816 (national ID, working permits...)
- two SAMs (Security Access Modules)
- advanced digital security features

- ***Software***

- SDK with OCR-B and image processing library, e-Passport contactless chip reading and cryptosecurity checks
- BAC (Basic Access Control), Passive authentication, Active authentication
- fully functional application for border control

## Vlatacom Biometric Identity Enrolment and Verification Systems

**Solutions that include all necessary hardware and software for instant travel document authentication and rapid biometric identity verification**

- optically scans and displays all machine readable data from the passport's data page
- reads and displays all digitally stored data from the contactless chip
- acquisition of signature, fingerprints, 2D face image (options: iris, 3D face image)
- automatically verifies document holder identity against the biometric data stored on the e-Passport: fingerprints and face image
- operator-free, unmanned, crewless operation (option: e-gate)
- visual and audio guidance assists user throughout highly intuitive user interface
- convenient, reliable, efficient, high service level

VLATACOM d.o.o.
7, Dunavska St.
11080 Belgrade – Zemun, Serbia
tel: +381 (0)11 377 11 00, fax: +381 (0)11 377 11 99
www.vlatacom.com info@vlatacom.com