MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

The New 9303

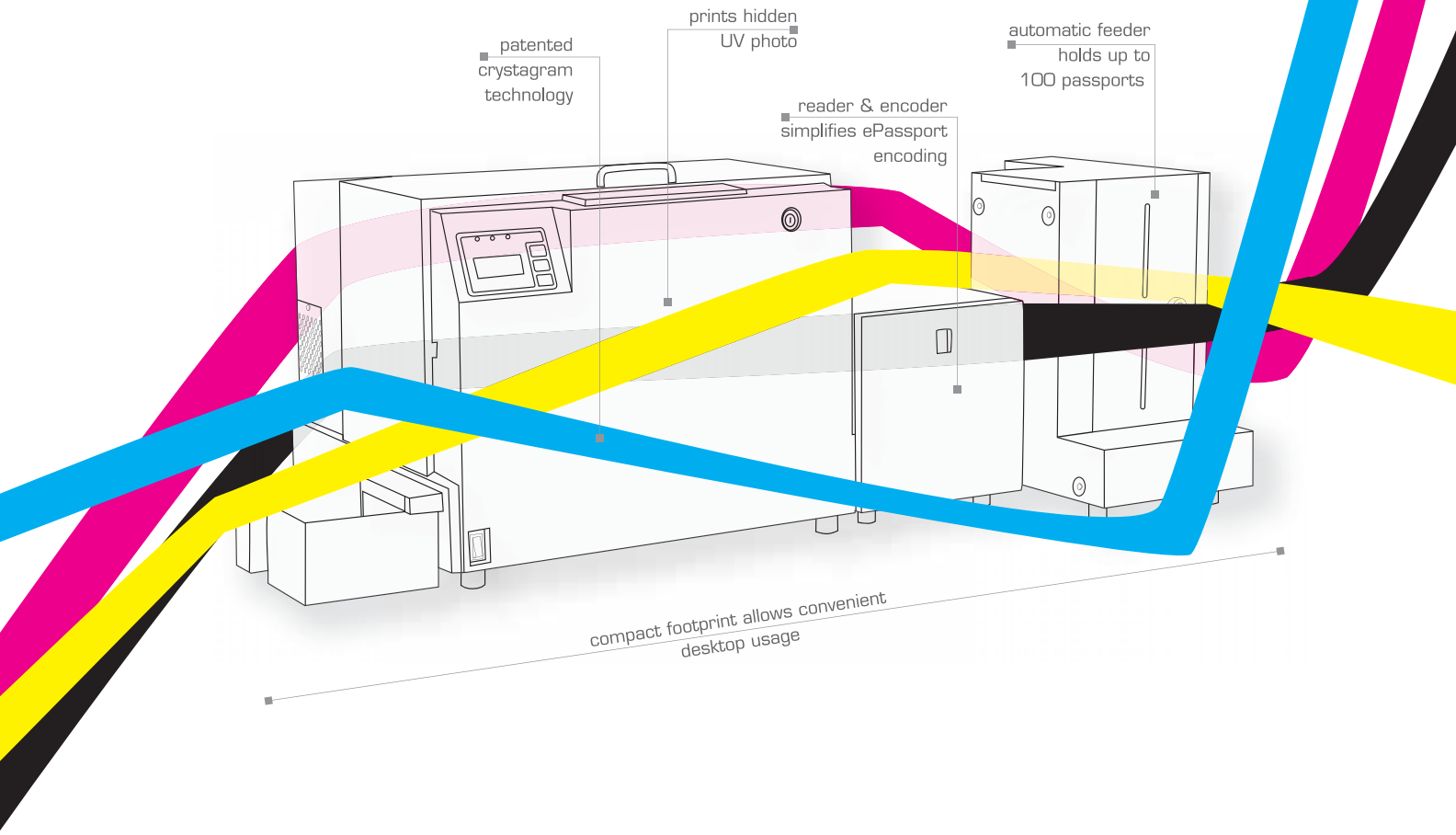
The addition of a globally interoperable biometric standard to Part 3 of ICAO Doc 9303 expands and enhances the world's guiding MRTD document to help States develop a new generation of ID card implementations

Also in this issue:
Rethinking identity in the digital age • Before and after ePassports
Operating systems for ID documents • Automated border control
State feedback: The Portuguese viewpoint

Vol. 3, N° 3

Global Enterprise Technologies Corp.
230 Third Ave. ▪ Waltham, MA 02451 ▪ USA
T: +1 (781) 890 - 6700
F: +1 (781) 890 - 6320
www.getgroup.com

Secure your passport...



...with our E2000 passport printer.

GET Group is the world leader in state-of-the-art passport solutions. With references around the world, more than 20 years of experience, and as exclusive distributor of Toppan digital passport printers, GET Group is uniquely positioned to provide passport solutions that meet your highest security needs.

Toppan passport printers employ proprietary digital pigment ink printing and lamination technologies to produce one of the most secure passports in the world. Our latest TOPPAN E2000 passport printer fully meets the requirements for ICAO/ISO ePassports and features on-line chip encoding, automatic book feeding as well as user-friendly operation.

TOPPAN
E2000
Passport Printer

ICAO MRTD REPORT
VOLUME 3, NUMBER 3, 2008

Editorial
Managing Editor: Mauricio Siciliano
MRTD Programme—Aviation Security
and Facilitation Policy Section
Tel: +1 (514) 954-8219 ext. 7068
E-mail : msiciliano@icao.int

Anthony Philbin Communications
Senior Editor: Anthony Philbin
Tel: +01 (514) 886-7746
E-mail: info@philbin.ca
Web Site: www.philbin.ca

Production and Design
Bang Marketing
Stéphanie Kennan
Tel: +01 (514) 849-2264
E-mail: info@bang-marketing.com
Web Site: www.bang-marketing.com

Advertising
FCM Communications Inc.
Yves Allard
Tel: +01 (450) 677-3535
Fax: +01 (450) 677-4445
E-mail: fcmcommunications@videotron.ca

Submissions
The *MRTD Report* encourages submissions from interested individuals, organizations and States wishing to share updates, perspectives or analysis related to global civil aviation. For further information on submission deadlines and planned issue topics for future editions of the *MRTD Report*, please contact Mauricio Siciliano, managing editor at: msiciliano@icao.int

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.

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

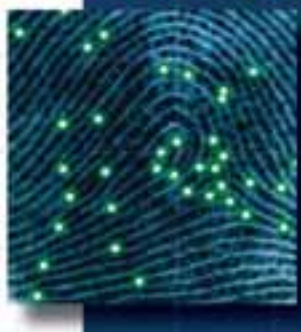
The objective of the ICAO *MRTD Report* is to provide a comprehensive account of new developments, trends, innovations and applications in the field of MRTDs to the Contracting States of ICAO and the international aeronautical and security communities.

PRINTED BY ICAO

Contents

Helping Solve the Global Challenges in Managing Identity






Verifying an identity and proving the legitimacy of ID credentials is no longer an issue of national concern. It is a matter of global security. Governments and agencies around the world depend on L-1 Identity Solutions to help them protect citizens against crime perpetrated by fraudulent identities. Our solutions scale from simple digitizing of paper records to state-of-the-art self-service border crossing solutions using advanced multi-biometric recognition technologies.

Built on a flexible and scalable platform, our solutions serve a trusted role within the world's most important identity management programs. They also form the foundation behind the most secure credentials used today including National IDs, Voter Registration Cards, Passports and Alien Resident Cards. In fact, L-1 Identity Solutions produces millions of secure government-issued IDs each year, including ID solutions for more than 25 countries.

Count on L-1 Identity Solutions to protect and secure personal identities and assets.

L-1 solutions are modular and can be used alone or together to form a complete identity management system

- Digitization & scanning of paper records
- Identity database management
- Multi-biometric enrollment and verification - face, finger and iris
- Document authentication
- Identity verification
- Integration of automated testing & scheduling
- Identity management workflow
- International credential design & production
- Proximity ID cards with RFID

L-1 IDENTITY SOLUTIONS™

SECURE CREDENTIALING DIVISION

www.L1id.com

296 Concord Road
Billerica, MA 01821 USA
Telephone +1 978-932-2200
Facsimile +1 978-932-2225

Bringing States the globally-interoperable tools they require

Dear readers,

With this issue of the *MRTD Report*, we are proud to announce the publication of the third edition of Doc 9303, Part 3, Machine Readable Official Travel Documents. We have included an overview of this document in this issue.

The specifications in this document are not intended to be a standard for national identity documents; however any State which participates in bilateral agreement(s) with one or more additional States, and which allows its identity document to be used to cross the border(s) between them, should design its identity document to conform to the specifications of Doc 9303, Part 3.

As with Doc 9303, Part 1, this third edition consists of two volumes: Volume 1, which is an updated version of the second edition containing all the specifications required for a State wishing to issue a machine readable official travel document without the incorporation of machine-assisted biometric identification. The second volume contains the specifications for enhancing the machine- readable official travel document with the globally interoperable system of biometric identification and its associated data storage utilizing a contactless integrated circuit.

With the publication of this document any additional biometric identification methods and data storage media, as included and described in the second edition (e.g. bar codes), are no longer to be regarded as ICAO-endorsed options within the new globally interoperable standard. However, States may use the non-standardized identification methods and media as they deem appropriate for their exclusive or agreed bilateral purposes.

One concept highlighted by the ICAO MRTD Programme is that of **'global interoperability.'** In this context, the term is understood as the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States.

Global interoperability is a major objective of the standardized specifications for placement of both human readable and machine readable data in all Machine Readable Travel Documents (MRTDs). Therefore, it is important to highlight that any international organization promoting the issuance of official documents of identity, or States wishing to issue such official document of identity designed to facilitate cross-border travel with enhanced security by incorporating the globally interoperable, machine assisted biometric identification/data storage system, should comply with both Volumes of Doc 9303 Part 3.

Enjoy your reading. ■

Mauricio Siciliano
Editor

Doc 9303, Part 3:
An essential global standard

The third edition of ICAO Doc 9303, Part 3, updates and replaces the specifications for machine readable official documents of identity published in the second edition (2002) and represents a substantial modernization of the material contained in previous editions. As with all improvements to this essential global standard, this new round of improvements and enhancements is the result of an extensive and very cooperative process participated in by the world's foremost experts in this area, most notably from the ISO and the various Member States that have played instrumental roles as this process has continued.

The specifications in Doc 9303 are not intended to be a standard for national identity documents; however any State which participates in bilateral agreement(s) with one or more additional States, and which allows its identity document to be used to cross the border(s) between them, should design its identity document to conform to the specifications of Doc 9303, Part 3.

This third edition incorporates the new globally interoperable optional standard covering biometric identification of the holder and storage of the associated data on a contactless integrated circuit. Consequently, additional biometric identification methods and data storage media, as included and described in the second edition, are no longer to be regarded as ICAO-endorsed options within the new globally interoperable standard. States may, however, use the non-standardized identification methods and media as they deem appropriate for their exclusive or agreed bilateral purposes.

"For those States either planning to introduce an identity card or upgrade an existing document the new ICAO Doc 9303, Part 3 standards provide a proven foundation for this work with the added benefit of a card that can be used for international travel on a bilateral or multilateral basis," commented Annette Offenberger, General Manager, Identity Services, New Zealand Department of Internal Affairs, and Chair of the ICAO TAG MRTD.

"While New Zealand has no current plans to introduce an identity card, I appreciate that a form of identity document is commonplace in many ICAO member States. The fact that the data storage medium together with the associated PKI security infrastructure has been proven operationally in ePassports will give States confidence that the standard can be applied in both national and international settings."

The magnitude of the specification for the new globally interoperable biometric identification system and the data storage using a contactless integrated circuit is such that Doc 9303, Part 3, is now divided into two volumes. The first volume is an updated version of the second edition—containing all the specifications required for a State to issue a machine readable official document of identity where said State does **not** wish to incorporate the global facilitation option for its citizens that will be available with machine assisted biometric identification.

The second volume contains the additional specifications for the globally interoperable system of biometric identification and associated data storage utilising a contactless, integrated circuit.

It is important to note that any State, when wishing to issue an official document of identity designed to facilitate cross-border travel with enhanced security by incorporating the globally interoperable, machine assisted biometric identification/data storage system, will therefore need to comply with both Volumes of Part 3.

"Part 3 now benefits from the comprehensive experience that has been developed based on implementations of the ePassport," began Eckart Brauer, TAG MRTD member and specialist in this area from Germany's Federal Ministry of the Interior.

"In Germany, the development of an electronic national ID card is now underway with issuance currently planned for the end of 2010," Brauer continued, "however, the new German ID card is more than a travel document—it also comprises e-government as well as e-business functionality. These modern concepts needed to be reflected in appropriate standards to safely secure identity and other personal information stored on the card, and Doc 9303, Part 3 will prove invaluable in helping States to manage and take advantage of this ever-widening distribution of biometrically-secured identity cards that are now being used more and more worldwide for simplified border crossing. Germany is therefore very supportive of every effort extended to keep Part 3 updated and a living, evolving document."

Certain specifications within Volume 1, particularly in relation to the portrait and other identification features, have been amended to ensure that when a State decides to upgrade to a globally interoperable biometric document only a minimum amount of change to the document will be required.

Who's behind?

Gemalto: the fastest* ePassport

Gemalto's new Common Criteria certified Sealys eTravel operating system:

- **Speeds up border control** with a reading time of less than 3 seconds* in Extended Access Control (EAC) mode
- **Increases ePassport personalization** throughput by leveraging record writing performance

Available on multiple interchangeable microprocessor platforms, the new Sealys eTravel operating system secures your supply chain management.

Gemalto's Sealys eTravel operating systems are used in more than 18 national ePassport programs worldwide including Côte d'Ivoire, the Czech Republic, Estonia, Denmark, France, Norway, Poland, Portugal, Qatar, Singapore, Slovenia, Sweden and the United States of America.

Now you know who's behind.

* 2,8 seconds for a full EAC transaction with 48 KB of data, RSA 1024 and extended length (EAC test in June 2008)

www.gemalto.com

gemalto
security to be free

The expanded specifications and guidance material on matters such as naming conventions, transliteration of national characters in the machine readable zone, as well as the calculation of check digits, have been retained in this first volume of Part 3. The options for the inclusion and placement of an integrated circuit with contacts, a bar code, a magnetic or an optical memory stripe on the document remain, as does the option to use biometric identifiers other than facial recognition supported by fingerprint and/or iris data. It is to be emphasized, however, that the inclusion of these storage media and the data thereon is solely for use by the issuing State or by other States by bilateral agreement—they are not globally interoperable.

The emphasis on the security of the document against fraud by alteration or counterfeit is given greater prominence in this third edition, as is the need for security of the premises in which a travel document is made, personalised and issued. New emphasis has also been added on the need for carefully vetting staff employed in these activities.

One concept highlighted in the second edition was that of 'global interoperability.' In this context, the term is understood as the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both human readable and machine readable data in all Machine Readable Travel Documents (MRTDs).

In our increasingly security-conscious world, the need for machine assisted global interoperability has become a pressing concern. This has necessitated the standardisation of one primary biometric identification method and of one method of data storage.

The New Technologies Working Group (NTWG), established by the ICAO TAG in the mid-1990s, commenced an evaluation in 1998 of the various options and, in early 2001, selected and recommended facial recognition as the primary biometric to be employed along with a contactless, integrated circuit as the approved data storage technology. The recommendation was made specifically in response to the needs of passport issuing and immigration authorities to ensure accurate identification of a travel document applicant or holder—while minimising facilitation problems for the traveller. This recommendation was endorsed by the ICAO TAG and by the ICAO Air Transport Committee in 2003.

As before, provision has been made for issuing a passport as a wallet-size card in accordance with the specifications for the Size-1 machine readable official travel document as set forth herein, provided that the issuing State makes appropriate provision for other States to associate visas with it. ■

Automated Border Control

By Sjef Broekhaar, International Organization for Migration, and Julian Ashbourn, International Biometric Forum

Among the many potential benefits of the eMRTD is the promise of automation and the possibility of either fully- or semi-automated border control points. Such a model might serve to relieve the ever-increasing burden of manual border checks, allowing immigration and border control personnel to be more effectively deployed in handling exceptions and further refining their own internal processes. Sjef Broekhaar and Julian Ashborn explain.

The introduction of eMRTDs represents a significant change in the quality of travel-related documentation. We now have a document which is not only considerably enhanced with respect to the physical security features of the document itself, but which also introduces valuable operational features in the form of the integral electronic chip and the provision of biometric identity verification.

Considering the relatively short gestation period of the new documents, the emergence of the eMRTD represents a solid achievement of international collaboration, spearheaded by the New Technologies Working Group (NTWG) of ICAO. Furthermore, an associated NTWG working group has produced a comprehensive set of guidelines regarding "eMRTDs & Passenger Facilitation," that offers advice and best practices with respect to maximizing the potential of the eMRTD in passenger processing systems.

The combination of coordinated processes and the eMRTD itself provide an interesting framework for future border control operations. Legitimate travellers would also benefit from such automated processes, providing the physical implementation is thoughtfully considered and properly scaled in relation to the wider operations of the port or entry point in question.

FIGURE 1: PASSENGER THROUGHPUT INCREASE AT MAJOR HUBS: 2002-2007				
Airport	**2002**	**2007**	**Growth**	**%**
London Heathrow	63,338,641	68,068,554	4,729,913	7.47
Tokyo Narita	61,079,478	66,671,435	5,591,957	9.16
New York JFK	29,943,084	47,810,630	17,867,546	59.67
Amsterdam Schiphol	40,736,009	47,793,602	7,057,593	17.33

Since the mid-80s, immigration services worldwide have been looking for new solutions to process the ever increasing number of travellers. As an illustration of this fact, Airports Council International (ACI) reports that, in 2006, 1,100 airports processed approximately 4.4 billion passengers. Not all of these passengers were processed by immigration or border control authorities, since this number also contains passengers on domestic flights. However, this figure places the sheer scale of travel transactions in context and the information in Figure 1 *(above)* provides a further illustration of the volume and growth in passenger movements using four large international airports as a test sample.

The processes and metrics used by immigration services and border control authorities have also progressed in recent decades. In the 80s the Immigration and Naturalization Service of the United States developed a system whereby passports of incoming passengers were scanned by Airlines at check in and details of the Passenger Name Record (PNR) were transferred to the US immigration authorities in order to execute an initial name check within their databases. The aim was to accelerate the border control process for those who had been pre-checked. Other processes were subsequently introduced, like Advance Passenger Information, APP and Pre-Clearance programmes in several countries.

Currently, passengers departing for the United States from a number of airports are cleared for entrance into the US by immigration officials and, upon arrival, can go straight to the baggage area to clear customs. Other countries have followed suit, some with more comprehensive entry systems like that introduced in Australia, in order to reduce the process time at the border.

Today, at many airports, seaports and border crossing points at train stations, automated border control systems are used in order to process large numbers of passengers. These systems have earned their place within the broader border control environment. Increasingly,

countries, airport authorities and border control authorities are considering the use of such systems as part of their passenger handling process.

One variation, which was first implemented at Schiphol Airport in Amsterdam, was an automated border control system. Frequent travellers had the opportunity to enroll into a voluntary registration system and were provided with a separate token containing an electronic chip. On this contact chip, the traveller's fingerprint was stored in addition to applicable biographical data. The token could be used by the traveller to cross the border by verifying the live fingerprint against the stored fingerprint, and the transaction was always undertaken under the surveillance of an immigration officer.

For these authorities the aforementioned guidelines on "eMRTDs & Passenger Facilitation" provide a better understanding of the how to implement such systems successfully.

A limitation with this idea at the time was that the token could only be used at one port. However, with the introduction of the ePassport, similar (automated identity verification) benefits may be realised at all ports due to the universality of the document. The "eMRTDs & Passenger Facilitation" guidelines promote the use of the eMRTD as a possible token for this process. However it must be remembered that the document is simply the physical result of a much wider process that includes issuance, renewal, revocation, as well as identity verification from a security perspective. The combination of the eMRTD and these wider processes together provide an operational framework for ethical, responsible and sustainable border control. The framework, however, is only as strong as its weakest link and, with the introduction of a properly implemented eMRTD, the weakest link is now unlikely to be the travel document itself.

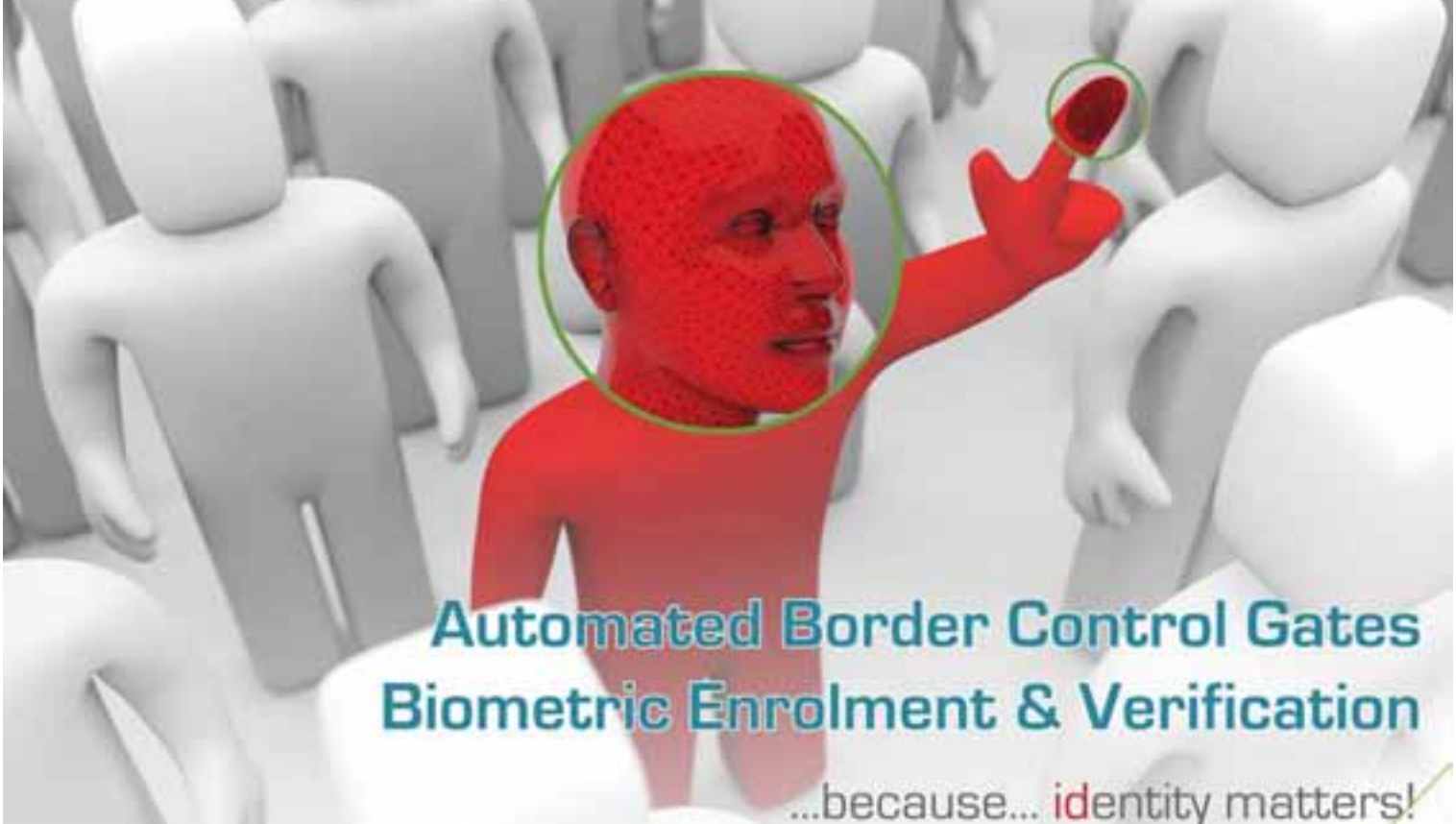
We must also turn our attention to the systems and processes which operate in tandem with the eMRTD in order to provide the broader operational framework, while respecting the individual and, especially, those with special requirements, such as the disabled and elderly.

Given the extra confidence that eMRTDs are likely to inspire, it is especially important to review our issuance processes, including the use of breeder documents and mechanisms for initial identity verification. The supporting systems are equally important because, if these are compromised, data associated with a legitimate eMRTD may easily be falsified, leading to inappropriate actions including admissions and denials of service.

The security of every link in the system must receive attention, including root-level access control, administrator rights, activity logs, data encryption, secure communications, the proper use of firewalls and regular audits. We must also respect privacy and ensure that personal data is not misused. In addition, contemporary compliance issues, including PCI DSS (Payment Card Industry Data Security Standard) must be observed. The whole area of systems security and associated responsibilities may be further complicated if government agencies elect to outsource the provision and maintenance of such systems. This is an area for careful consideration.

In conclusion, the design and introduction of the eMRTD has undoubtedly been a notable success story for ICAO and its Member States. We might now consider this achievement as a distinguished first step towards a broader accomplishment: a harmonised and globally interoperable immigration and border control framework which may be operated fairly and efficiently for the common good. ■

The guidelines discussed in this article are published on the ICAO website and may be accessed via: http://www.icao.int/mrtd.



Automated Border Control Gates
Biometric Enrolment & Verification

...because... identity matters!

VB-eGate

VB-ePass

VB-mPass

Identity recognition and passport verifications with Automated Border Control Gates, it's all about speed and security. Vision-Box's high-tech borders comply with the e-Border strategy of any nation, supporting the tight security rings, while performing the toughest checks ever, without grinding the borders to halt. The VB-eGates have been designed with the user in mind, providing passengers with a positive user experience and allowing those who have the right to pass, to get through rapidly, while freeing the Border Guard to concentrate on high risk flights and passengers.

Portugal
Rua Casal do Canas, Nº 2, Zona Industrial do Alto Lagoa
2730-204 Carnaxide, Portugal
t: +351 96 253 3679

Germany
Berlin Checkpoint Charlie, Friedrichstrasse 50
10117 Berlin, Germany
t: +49 3020059475 f: +49 3020059200

For more information, please contact info@vision-box.com or visit our sales team.

www.vision-box.com

vision-box

Before and after ePassports

By John Mercer, Senior Associate, Kelly-Anderson & Associates

The discipline required to operate a MRP issuance system is good training for the much higher level of technical performance that is possible with the ePassport. John Mercer provides background and insight into the steps that States must take in order to create sound systems of issuance, production and distribution.

States that have long issued machine readable passports are upgrading their production to ePassports to provide better identification for their citizens, to react to security concerns because of perceived threats to national and international security, to meet requirements of regional associations of States, most notably the European Union, and in the hopes that having an ePassport will be the ticket to getting Visa Waiver status.

States that do not yet issue machine readable passports share the same concerns as the present MRP-issuing States, but they have the added challenges of establishing a basic passport issuance system built on good citizenship data and accurate national records. In some cases, States may go directly from a non-MRP status to the ePassport.

The purpose of this article is to describe the process of transitioning from the present passport to an ePassport. Regardless of what the present national conditions are, major changes have to be made in how the passport is issued.

Background

A passport is a government document that identifies the holder and facilitates travel by providing bearer information in a uniform way, and a place for visas and other entrance and exit records. ICAO Document 9303, Part 1, describes the structural and security features of the modern Machine Readable Passport (MRP). In 2006, ICAO issued a revised version of Doc 9303, Part 1, in two volumes, one describing the traditional passport with machine readable data stored in optical Character reading (OCR) format, and the second volume describing the procedures for the electronic storage of data.

Being a government document, there are laws, regulations and procedures that are established by each issuing State or Organization that describe how their passports are to be issued, and used. Not surprisingly, these various issuance and usage laws differ between the States. In some cases, a passport is a right of citizens, and other cases, citizens must justify their need to travel in order to be issued a passport.

ICAO provides standards and recommended procedures for passport and visa issuance in Facilitation Annex 9 to the Convention on International Civil Aviation. However, this guidance consists of only 25 points, and is less than two pages. Consequently there is much room for different interpretation and practice. There's an old saying that applies here: "In theory, there is no difference between theory and reality, but in reality, there is."

Nonetheless, there are a number of steps to the issuance of a passport through which all passports are issued. This paper is to provide an overview of these common steps, and the ways in which the addition of the biometric information, stored in an Integrated Circuit (IC) chip contained in the passport, has changed the procedures. In many cases, collateral advantages may be realized in the automation of the application process.

In speaking about upgrading passports to the ePassport standard, there are several initial points that should be considered.

States should ensure that they have adequate funding for the development and systems cost for the ePassport programme. This funding may be self-funded by user fees, or from government appropriated funds, or there may be donor nations or organizations involved. In any event, funding is first.

States should consider the reasons for introducing the ePassport. Visa Waiver States have dates certain for compliance. Members of international communities, such as the European Union, have deadlines for ePassport introduction.

While non-MRP States may wish to proceed directly to the electronic passport, there is value in ensuring that their passport is first brought up to the MRP standard in Doc 9303, Part 1. The passport should be correctly formatted, contain the recommended security features as cited in the Security Annex to Section 3 of any Doc 9303 MRTD standard, and must have a data page in compliance with Doc 9303 Part 1 on MRPs, including a fully readable, correctly formatted, and properly printed machine readable zone.

Not only is this the operating norm for international travel, but for States

contemplating use of the Basic Access Control feature in their MRPs, having a correct MRZ is mandatory for allowing electronic access to the data stored on the ePassport. In many cases, the ePassport will be inspected visually, and it is important to maintain the traditional physical security features, so that in the case of electronic compromise or broken electronics, the passport can still serve as a trusted credential for border crossing. An ePassport with a broken or malfunctioning chip is still a valid passport.

Steps to passport issuance

Application

The person decides to apply for a passport. This usually requires filling out a form, either in paper or online. In addition to personal information, the applicant has to provide photos and the proper fees. All first-time applicants require a personal appearance before an authorized government official to check the veracity and completeness of information provided.

ePassports require biometric information to be captured for inclusion in the electronic chip contained in each passport. The mandatory biometric is the face image. This image must meet uniform standards for clarity and size, as defined in ISO/IEC 19794-5. Illustrative guidelines for portrait quality, style and lighting, glasses and head covers, and expressions are included in Doc 9303, Part 1, Appendix 11.

In moving to electronic scanning of forms, considerable efficiencies can be obtained by having a scannable-friendly form: all data on one side of the page, clear layout of data fields that may be machine scanned, and print fonts that are easy for the applicant to read, and to fill-in correctly.

Optional biometric measures are the fingerprint and iris. The quality of the biometric images is critical to the success of the identity comparison process. While 10 print cards have often been used for fingerprints, the quality of the images varies, so electronic live-capture and quality assessment is becoming more prevalent. Certainly live capture assures that the fingerprints belong to the applicant, and electronic image quality checks ensure that the fingerprint is clear enough to store and obtain minutia required to do machine comparison of fingerprints.

Application review and processing

The application file is established, and information on the application is used to determine the eligibility of the applicant to receive a passport. Is the person a citizen? Are there any reasons why the person should be denied a passport or have limited validity? Checks may be made against any pertinent private or governmental record that bears on the applicant's eligibility. Fees must be tracked and deposited.

Existing passport systems records must be modified to accommodate the additional biometric information associated with each applicant, and in a way that is retrievable for use by the government. Pertinent information may be stored in a variety of branches of government, and problems of interoperability have to be resolved in order for thorough and timely checks to be made. These interoperability problems are often significant, difficult to resolve, and expensive to fix. Ideally, improvements in passport data could be used to leverage improvements throughout the national data storage systems.

ePassports require the biometric characterization of the applicant. This adds complexity to the process because there is more applicant data to be checked. However, the addition of fingerprint data allows checking against existing national fingerprint databases, and thus a better chance of detecting an imposter or fraudulent applicant prior to document issuance.

Decision to issue

With all available data at hand, the passport adjudicator or examiner will make the decision to issue the passport. The only thing different between present practice for a State that already issues a MRP and issuance of an ePassport is that there is more data to be evaluated and more certainty of the identity of the applicant.

Data capture for passport printing

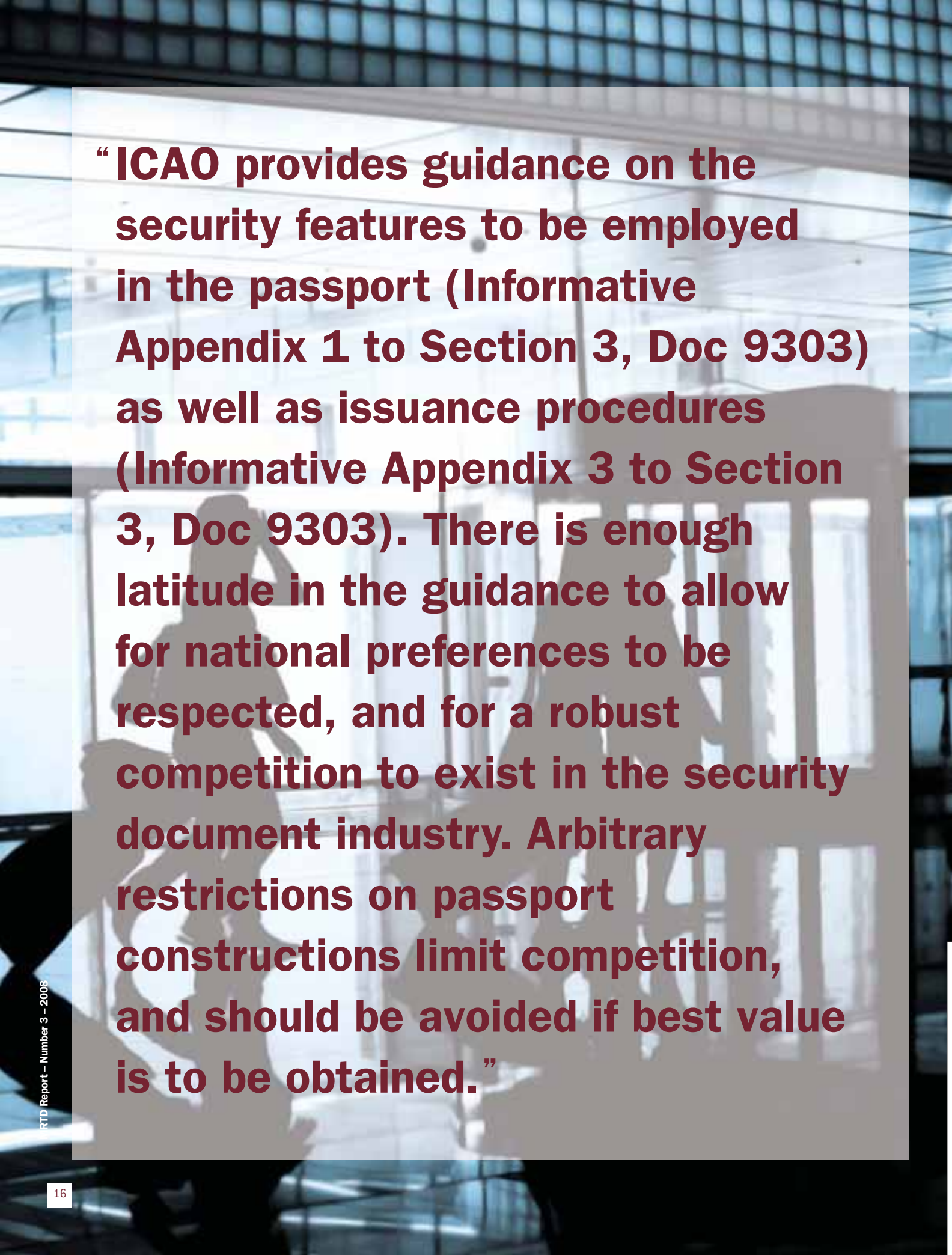
In present operations, data may be entered into the system early in the application review and receipt process or later, after the decision to issue has been made. In either method, it is important to ensure that the images are reproduced with the highest fidelity. Assuming digital printing of the portrait, the resolution of the scan should be as high as the resolution of the printer, otherwise the printed image may be degraded by pixilation or other print-related problems.

Typing the data from the application is the most common method of data acquisition. This has to be double checked for accuracy, and often double entry of data is the best method. Electronic scanning of data is difficult, given the differences in the handwriting of people.

States whose primary language uses a non-Latin script will face the problem of transliteration of their data in the Visual Inspection Zone as well as the MRZ. This is a basic requirement and applies to both MRP and ePassports.

It is important that there be a method of correction of errors, so that only correct data is used to print a passport. If caught internally, then book spoilage is reduced, and the system corrects itself. If a bad book enters circulation then the traveler will be inconvenienced or prevented from traveling. Error correction methods are vital in increasingly automated systems, where the system is the arbiter, and if the system is wrong, then there is no recourse for the citizen to make corrections or seek relief.

Electronic passports add the need to match the electronic data with the visual data on the passport. Facial biometrics at least allow the border officer to make a visual comparison between the holder and the book as well as the electronically stored image. Fingerprint readers are common enough that a similar comparison could be made, but given the time involved, such a comparison will most often be made in a secondary examination, where time of examination is less of an issue. Getting the stored fingerprints right is especially important, since a difference in prints between the holder



"ICAO provides guidance on the security features to be employed in the passport (Informative Appendix 1 to Section 3, Doc 9303) as well as issuance procedures (Informative Appendix 3 to Section 3, Doc 9303). There is enough latitude in the guidance to allow for national preferences to be respected, and for a robust competition to exist in the security document industry. Arbitrary restrictions on passport constructions limit competition, and should be avoided if best value is to be obtained."

and the book will automatically be considered fraud, and the holder will be guilty until proven innocent.

Book printing

ICAO has mandated (Annex 9, paragraph 3.10) that all passports issued on or after April 1, 2010, to be machine readable. This refers to the presence of the two lines of machine readable code on the bottom of the data page. Printers and systems must be in place to accomplish compliance by that date. A further policy compliance requirement is that member States shall have only MRP books in circulation after November 24, 2015. This has the practical effect that a State with a 10-year validity document is required to either plan on replacing such non-MRP books issued before November 24, 2005, or shorten the validity term of their non-MRPs so that they expire in 2015.

Of course books must be made with the printer in mind. All ICAO compliant passports should be formatted and constructed according to the Doc. 9303 Standard. But there are a myriad of methods of making ICAO-compliant data pages and passport books, and the books have to possess the physical structure to accept, retain and protect the entered data.

Some States find it appropriate to move to a centralized issuance system with the advent of the ePassport. Other States may continue with a distributed application and biometric live capture system, and centralized production.

Fingerprint and iris biometrics are particularly suited to live capture.

ICAO provides guidance on the security features to be employed in the passport (Informative Appendix 1 to Section 3, Doc 9303) as well as issuance procedures (Informative Appendix 3 to Section 3, Doc 9303). There is enough latitude in the guidance to allow for national preferences to be respected, and for a robust competition to exist in the security document industry. Arbitrary restrictions on passport constructions limit competition, and should be avoided if best value is to be obtained.

Some security features are substrate based, others ink based, while some are related to the personalization process. An often repeated request from border inspectors is for more features that can help the first line inspector. Features added in personalization, such as steganographic features offer such help, especially if the country is using a full-page reader that has been electronically programmed to look for the steganography present in the facial image. Such features can usually also be worked into the image stored on the IC chip, if desired by the State in question.

Conversion to an electronic passport requires significant changes to the book structure, accountability and security. The passport must contain the electronic IC chip and associated antenna in order to store the biometric information in a standard way so that the passport may be interrogated by authorized readers. This latter is accomplished by conformance to both volumes of Doc 9303. The data must be stored in its proper data groups within the electronic record, so that it can be read. This electronic writing and reading is a significant change as none of that has existed before.

ePassport books are required to have the ePassport logo appear on the front cover of the book.

The chips are numbered so an additional accountable item is added. The structure of the book must be modified to protect the chip. Presently there are three

EDAPS

CONSORTIUM

The new passport that Ukraine started issuing to its citizens in July 2007 combines multiple features – not only does it have an interesting graphic background design, but its production employs state-of-the-art digital technologies.

The new document has a high level of security and it fully complies with the international civil aviation organization (ICAO) specifications for machine readable travel documents.

The main feature of the passport is its personal data page made of multilayer polycarbonate and located inside the passport booklet pursuant to Doc 9303 guidelines. The advantage to using a new material is that, in addition to the traditional methods of document protection (background interlace patterns, guilloche micrographics, secure ink), one can use brand-new methods of recording the owner's data. This primarily affects the main biometric identifier – the owner's facial image, which is recorded onto the page by laser engraving and is then duplicated by laser perforation. The resulting black-and-white image has a high resolution, which provides a clear view of all facial features and makes the image easy to perceive. In the process of engraving the polymer structure undergoes irreversible changes, which makes the data impossible to counterfeit. This is the primary security measure undertaken by the government to prevent counterfeiting.

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

The Consortium EDAPS is ready to issue e-Passport containing a contactless chip integrated in the cover developed in compliance with the ICAO specifications.
The electronic chip can store any additional biometric information about the document holder adopted by the state and specified by international requirements. The new e-Passport is planned to be introduced after adoption of appropriate government regulations.
Both the passport documents and the system solutions developed and implemented by the EDAPS Consortium are in full compliance with the international requirements.

Crew member identification 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:
64 Lenin St.
Kiev, 02094, Ukraine

Telephones:
+38 (044) 561 2590
+38 (044) 561 2589

Fax:
+38 (044) 561 2585

E-Mail:
edaps@edaps.biz

WWW:
https://www.edaps.biz

locations for IC chips in ePassports: in a hard thick plastic card, usually the data page; in between the center pages of the book, or in the cover, usually the non-foil-stamped cover. Protection against unauthorized electronic access may also be included. This may take the form of a metallic foil or screen which disrupts electronic access to the IC chip.

The process control of ePassports involves reading the IC chip for viability during and after the production at the book printer, and also reading on receipt by the government prior to personalization. This is especially important since the addition of the IC chip usually adds a significant increase to the price of the base passport. Thus in-process monitoring and reduction of spoilage attains an importance that may have previously been overlooked. Spoiling a $3 book is different than spoiling a book costing $30 or more.

To insure data integrity, ICAO has chosen to use a Public Key/Private Key system, in which the data is written with a Private Key and read using a Public Key. In order to use the Public Key Infrastructure (PKI, it is necessary to establish Country Signing and Document Signing Certificate Authority (CA) and Document Object Security (SOD). This issue is very complex, and must be done exactly right in order to have international interoperability of the electronic data. ICAO is the nexus for this authority.

The data has to be written to the IC chip in a way that fits within the Data Groups prescribed by ICAO in Volume 2 of Doc 9303, Part 1. Furthermore, legitimate access to the IC chip can be controlled by several levels of electronic security, starting with Passive Authentication, Basic Access Control and Active Access control. These possibilities were first explained in ICAO Technical Reports and then later added to the Doc 9303 in Volume 2 of Part 1, MRPs.

But there is more, in that the physical structure, and particularly the thickness of an ePassport is different and often personalization printers have to be changed to adapt to the new thickness. Thicker books also may mean changes in shipping boxes, as fewer ePassport books will fit into a given box, compared to non-ePassports. Vault space may also have to be increased. In many cases, multiple changes are made to the passport, with new designs, changes in numbering schemes and location of the data page within the book, so that these physical changes are not trivial, and once made, are not readily adjustable back to the original settings. Going to the ePassport is a one-way commitment.

Quality check and return to holder

Once printed, the modern MRP passport is usually visually inspected for obvious defects, and the MRZ is read to ensure that it is correctly printed. After that, the book is returned by whatever means is customary in the particular State.

The electronic passport has more information to check and has to be read electronically as well as by MRZ readers. This is not only to assure viability of the IC chip, but to ensure that data has been entered correctly into the various Data Groups.

Summary

In summary, this article is a fast and relatively high-level comparison of passport issuance before and after the advent of ePassports. It is not intended as definitive, as each point in the process requires great attention to detail in order to get it right.

States need to communicate to their citizens about the advantages of the ePassport, enable citizens to check the operation and content of their ePassport (to eliminate surprise malfunctions on departure, and for privacy reasons), and communicate information about their new passport to neighboring States, other States in the world in illustrated brochures or other communications tools appropriate to the audience (i.e. border control agencies or the general public).

There are significant reasons to make the transition to ePassports as soon as possible, but the success of any ePassport system is based on the proper functioning of the basic MRP platform. The readers of these words will have to judge where their States are in relation to a strong and secure system of identity management. Suffice it to say that experience with the discipline required to operate a MRP passport issuance system is good training for the much higher level of technical performance that is possible with the ePassport. ■

Operating systems for secure ID documents

A G&D White Paper comparative analysis of the Native, Java and Multos options

The chip in modern electronic identification documents consists of the microprocessor (hardware), the Chip Operating System (COS) and the card applications (software). ICAO specifications define the software (Logical Data Structure) for e-passports, and while some recommendations exist for the memory of the microprocessor there is presently no specification for the COS.

The result is that State officials have a choice between several chip operating system options and the following paper seeks to explain these in more detail.

Currently, three different types of smart card operating systems are being employed in the segment of national high-security documents:

- Native COS (also called file-based or ISO cards)
- Java Cards
- MULTOS cards

Unlike a PC operating system, chip operating systems are restricted in size and processing capabilities but need to be highly optimized for security. Because the security of any smart card is defined by the interaction of its hardware, COS, and LDS, COS evaluations need to consider interrelated factors relating to performance, security, interoperability, reliability, cost, etc.

States may wish to note that Native COS implementations currently dominate in ePassports worldwide, possibly due to performance requirements for the reading process. There is no clear trend as concerns national ID cards, with most current systems being based either on Java or on Native, depending on the geographic region (Europe is primarily Native-oriented while Asia and the Middle East have seen a number of Java implementations). Only a very small number of MULTOS projects have been deployed internationally.

Native systems

In the early days of smart card technology, Native operating systems didn't follow any common standards and the functionality supported was mainly proprietary. Modern Native systems support file systems based on the ISO-7816 smart card standards although they may still contain vendor-specific commands as well as proprietary functions. The reason for

this is that while Native systems overcome memory and performance constraints, they also provides additional functions beyond the standard—which is a benefit.

Native cards have a pre-defined command set which allows developers to dynamically create their own applications based on the pre-established card functionality. The pre-defined command set is the interface to the outside world. The application and its data are completely separate, although they use the same basic card functions. The functions are executed directly by the microprocessor and there is no interpretation of byte code as is the case in a Java Card.

Java systems

Java Card technology adapts the Java platform for use in smart cards and other devices whose environments are highly specialized, and whose memory and processing constraints are typically stricter than those of a regular PC.

A Java Card implementation is supposed to follow two sets of specifications:

- The Java Card specifications initially defined by SUN Microsystems, and now by the Java Card Forum.
- The GlobalPlatform specifications defined by the GlobalPlatform organization.

Sun Microsystems realized the potential of smart cards and similar resource-constrained devices many years ago. It defined a set of specifications for a subset of Java technology and proceeded to create applications for them—the so-called Java Card applets. A device that supports these specifications is referred to as a Java Card platform.

The *Java Card technology specification* is in three parts:

- The Java Card Virtual Machine (VM) specification, which defines a subset of the Java programming language.
- The Java Card Runtime Environment (JCRE) specification, which further defines the runtime behavior of Java-based smart cards.
- The Java Card API specification.

The Java Card platform is a secure multi-application environment—many different applets from different vendors can safely coexist in the same card. Each applet is assigned to an execution context—the security area assigned to the applet. The boundary between one execution context and another is often called an applet firewall. This firewall ensures that one applet cannot access the code and data objects of another applet. If necessary, the Java Card platform can support mechanisms for secure data sharing across firewalls, although for security reasons this is not recommended in routine use.

The Java Card specifications define the general behavior and architecture of a Java Card, but they do not describe a specific solution for the card or the application lifecycle management in detail. By contrast, the GlobalPlatform card specification defines a concrete implementation of card components, command sets, transaction sequences and interfaces that are hardware-neutral, operating system-neutral, vendor-neutral and application-independent.

One of the main differences between Java Cards and Native and MULTOS operating systems is the organization of the "file system structure." Java Cards do not have any similar ISO7816-4 compliant file-system structure, nor do they support the ISO7816 commands and their security mechanisms. It is therefore up to the applet developer to define their own file system organization and supported commands that can be either compliant or non-compliant with ISO specifications.

MULTOS systems

MULTOS is a smart card operating system that provides the underlying communications, the memory management, and an Application Abstract Machine (AAM) for multi-application smart cards. Operating system or platform services are available to application programmes in the form of an AAM.

The MULTOS COS handles the loading and deleting of applications and the sending/receiving and dispatching of commands to (and responses from) the card. Like Java Cards, the core of the MULTOS operating system is an interpreterthat allows the applications to be developed independently of the underlying card hardware. Applications written with the MULTOS API could be run anywhere on any MULTOS platform.

The MULTOS AAM provides every application stored on the card with its own memory space. Each application resides in a rigorously enforced application space, which consists of the application code and data segments. The memory and file system is organized as an ISO7816-4 compliant file system structure.

Application loading and deletion is done using certificates. While an application is being loaded onto the smart card, MULTOS checks its validity and allocates a memory area protected by a firewall. Each application is stored strictly separated from the other applications and it is not possible for them to interfere with each other. This means that an application has full access rights to its own code and data, but cannot directly access the code of another application. Like Java Cards, MULTOS allows applications to be loaded onto the smart card even when it is already in the cardholder's possession.

Choosing a Chip Operating System (COS)

Dynamic Application Management and Flexibility

MULTOS and Java Cards have always been considered highly flexible operating systems. This is due to the option of adding post-issuance functionality to issued cards through highly standardized, secure processes. But modern Native cards are now also capable of adding new functions and applications to cards in the field. Their processes and mechanisms are also based on standards (ISO7816), although they can include some vendor-specific features.

Native and Java Cards offer dynamic memory management, whereas MULTOS offers static memory management only, which can lead to memory fragmentation. In the latter case this is caused by the static memory allocation for applications residing in their own, dedicated physical area.

Another aspect is the flexibility for adding new functionality and applications to the card quickly and cost-efficiently before issuance. On a Native operating system, the functionality required for this could exceed the existing core operating system functionality (e.g. security protocols) and might require the basic functionality to be extended. It is likely that new functionality could be integrated in the existing card (as a so-called patch in EEPROM). If not, a new COS development resulting in higher costs and longer lead-times will be required.

Security

Any smart card platform used for identification purposes needs to meet very high security standards. In many cases the issuer

of an identification document will ask for certifications from an independent and accredited evaluation authority. In most cases, the certification of a Native card consists of composite certification of the operating system and one or more dedicated applications. The certification of Java Card and MULTOS platforms can be done for the operating system alone, or as a composite evaluation for both the operating system and the card applications. In terms of genuine security, only the latter certification guarantees a highly secure end-product that is comparable to a Native composite end-product. This should be the certification to aim for.

Each platform has its own security-related benefits and drawbacks: the fact that a Java Card applet can be developed by the governmental agency itself could be seen as a benefit. However, this could also be a big security risk, since applications should always be designed by experienced architects and there are complex security guidelines that must be considered.

The mechanisms implemented for MULTOS—the necessary application load and delete certificates and dedicated memory addressing is a benefit, but this comes at a high administrative cost. This type of security is important if a single smart card offers services from more than one organization. However, the vast majority of smart cards today offer a single application from a single issuer.

In general, all three COS architectures can be judged as secure, but the security of a concrete implementation needs to be verified by undergoing rigid tests and evaluations.

Performance

It has already been mentioned above that MULTOS and Java Cards are operating systems in which the functions are interpreted and not directly executed by the microprocessor. This is the crucial argument in favor of Native platforms when it comes to performance. Java Card performance has always been a contentious issue. The topic is sensitive, because it is a commercial argument, which has been used (and misused) over the years.

Generally, COS implementers have to make trade-offs between some important parameters:

- **Speed:** Many factors influence the speed of the platform, which can be an important differentiation factor.
- **Security**: Security often implies redundancy (e.g. double-checks), which in many cases contradicts performance.
- **Compliance:** Compliance with all specifications and recommendations can be costly, and little “cheats” can ease both speed and security. This can be tempting, especially in niche cases, although it does create problems for application portability.
- **Flexibility:** Flexibility means supporting a wide range of functionalities in order to cover use cases in the future. In doing so it may result in more overheads while executing functions.

Any platform can be optimized in any way and, as stated above, it is a trade-off between certain parameters. However, in the case of MULTOS and Java Cards you are tied to standardized processes, especially during the production phase—the initialization and personalization of the card.

If you have a highly stable and properly defined use case supporting specific mechanisms—for example the electronic passport—then Native platforms will always be a very good choice.

Implementation levels

ISO standards as well as MULTOS and Java Card/GlobalPlatform specifications are mainly driven by the industry, although the number of bodies involved in the definition and implementation of these specifications varies.

Java Card platforms are more widespread on the market than MULTOS platforms—there are also many more vendors who have implemented and/or who offer Java Card rather than MULTOS platforms. However, the majority of smart cards used for identification purposes are still Native. In the case of single-purpose cards with no post-issuance intention, open systems like Java Card and MULTOS are not necessary.

Application development toolkits

As a rule, all card vendors offer an accompanying software toolkit that allows skilled software programmers to develop their own applications for the specific card. All these development kits are vendor-proprietary and naturally vary considerably in terms of functionality and user-friendliness. They range from provision of the basic core functionality, such as definition of the ISO7816-compliant file system structures (for Native and MULTOS), through support for whole sets of cryptographic functionality, to debugging at byte-code level and support for TCP/IP interfaces for direct connections between the simulation or debugger with external (third party) programmes or live environments.

Whereas toolkits for Native operating systems may be used only in conjunction with the corresponding Native platform of the particular supplier, the toolkits for MULTOS and Java Cards can in theory be used with the platform of a third-party vendor, thanks to the write-once-run-anywhere principle of these platforms. In reality, this is not the case, since those platforms have their own specific characteristics due to their different interpretation of the MULTOS and Java Card specifications. Thus it could, though is not guaranteed, to be the case that an application which has been developed with a specific development kit from vendor A will run on a platform of vendor B.

As mentioned above, toolkits for Native platforms cannot be used by third parties to develop applications for any other platform than the given COS, since the implementations are always vendor-specific.

Comparison summary

From a functional point of view, all the operating systems described offer the full spectrum of functionality and security for the implementation of secure ID documents.

In summarizing the various aspects speaking for or against a dedicated smart card operating system, we can say that in general all have some strengths in certain areas, and none has any major weakness. States will have to consider all of the factors noted above in the context of their particular need in order to ascertain which COS will be right for their electronic document. ■

Identity fraud and digital capability

Identity fraud is a worldwide problem, with criminals and terrorists currently traveling between States using non existent, fabricated identities or identities that have been stolen from a legitimate citizen. Government and law enforcement personnel tend to this problem through a wide range of measures—including improvements in the security of the travel document itself—but Clemens Willemsen of the Dutch Department of Justice argues that in the digital age we may wish to begin considering eliminating ID documents altogether.

Though some of the solutions being presented in the following article may appear straightforward, they also require that those of us involved in the areas of passport issuance and border control may need to change our way of thinking about the very nature of identity documents. The three basic steps that I propose are required for States to diminish identity fraud are:

1. Using identity documents published by official authorities only.
2. Distinguishing between establishing identification with a document and granting rights to the owner of a document.
3. Replacing the physical document by a virtual document.

---

1. Using identity documents published by official authorities only

Identity documents can be categorized as:

- Primary *(published by an official authority).*
- Secondary *(published by a public or private organization such as a hospital, public transportation service, company, etc).*

A Primary ID document (PID) is handed over by an official authority, such as a State passport office or a regional license bureau branch, after a thorough check on a citizen's administrative and/or biometric identity—making use of, for example, a birth certificate or an expired passport. There are strict procedures surrounding identity establishment and document issuance that are employed by PID sources *(editor's note: see the 'Issuance and Identity' section in MRTD Report Issue 01 2008 for more on this topic).*

A Secondary ID document (SID) is based upon the PID. A hospital for example will admit you as a patient and requires you to show a PID. After verifying it is you, you will be registered and handed a hospital card to serve as a SID. This card identifies you only for hospital purposes and grants you certain rights to specific hospital procedures. This type of SID document is generally significantly less secure than a PID and therefore easier to copy or forge.

It is more recommendable then to use the PID for each visit to organizations that currently distribute SIDs for their own use. In the past, this might have been a problem, but in more and more countries citizens are required now both to carry and to show their PID for official purposes. Therefore they are much more likely today to have it with them at all times.

Under this type of regulated PID environment States and other organizations or more localized government entities would no longer need to concern themselves with the infrastructure, staffing and costs inherent in their SID programmes. Overall citizen privacy would furthermore be augmented by the fact that there would be fewer cards in circulation containing private information that could possibly be lost or stolen.

2. Distinguishing between establishing identification with a document and granting rights to the owner of a document

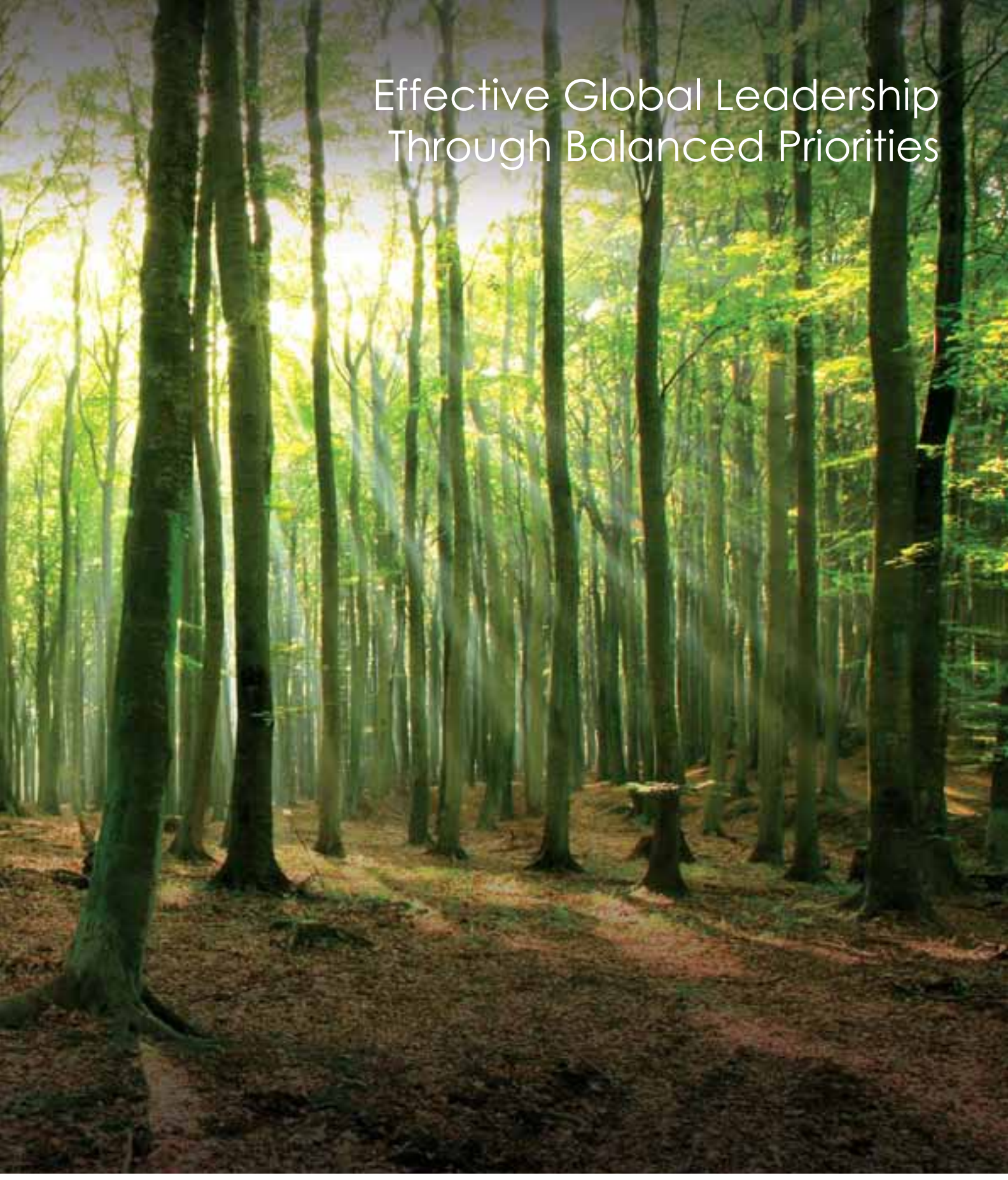
Traditionally, PIDs not only identify the bearer and authenticate him or her for national or international authorities, but also grants certain rights to the bearer, such as:

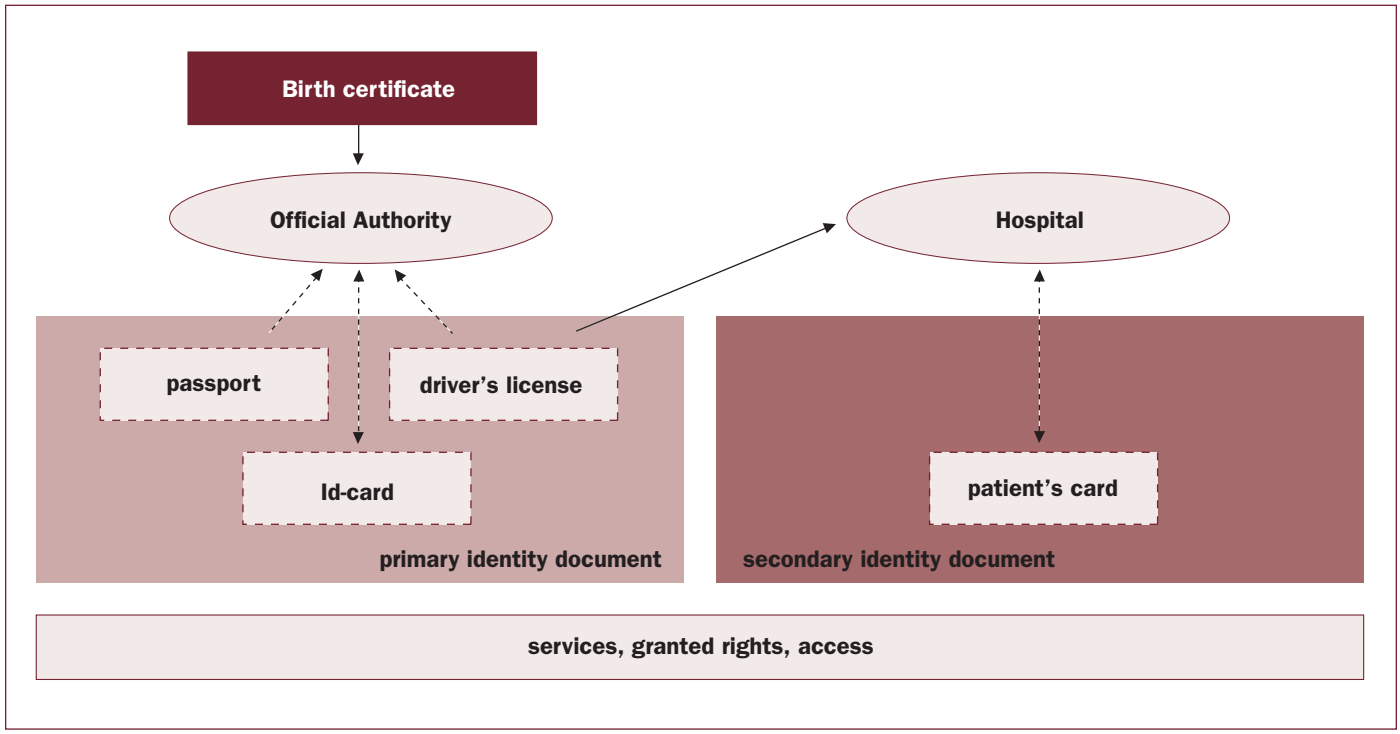
1. *Passport*—identifies and grants the bearer the right to cross certain borders.
2. *Driver's license*—identifies and grants the bearer the right to drive a motor vehicle.
3. *Social security card*—identifies and grants the bearer the right to use social services.

In other words, identity establishment and user rights are combined in the current PIDs. Many SIDs operate in the same fashion:

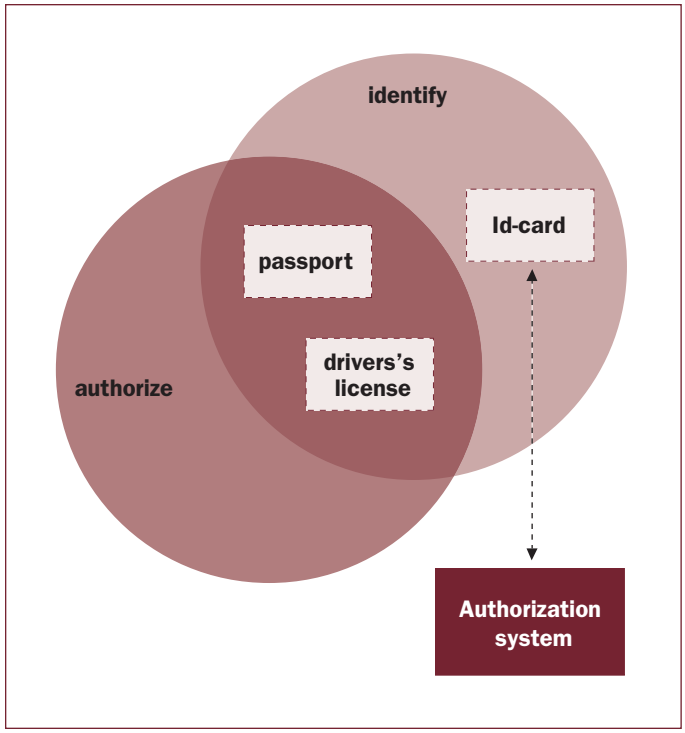
1. *Library card*—identifies and grants the bearer the right to borrow books.
2. *Credit card*—identifies and grants the bearer the right to spend money.

Effective Global Leadership Through Balanced Priorities





This combining of ID establishment with bearer rights and permissions was required in the past when physical ID tools and systems (cards and/or other documents) were distinct and separate from the administrative systems that tracked and recorded the bearer's associated permissions. It obviously wasn't practical using paper-based systems to re-verify the bearer's rights at each presenting of their ID and so the ID itself needed to clearly indicate what rights the bearer was entitled to and when these could be exercised, but when viewed in light of current digital capabilities this requirement is no longer necessary.



When all State infrastructures become more developed in this regard it would be advantageous to move away from the current requirements (even with the newer ePassports bearer rights are still reflected on the ID itself as per the needs of older administrative structures) and instead simply use the PID to enable border and customs officials to access real-time indications of the bearer's completely up-to-date rights and permissions.

The advantages of separating identity establishment from rights establishment with PIDs are numerous therefore:

1. Your specific identity card can be stolen but not your granted rights.
2. Granted rights can be checked online and are no longer restrained to the time of issue and the expiration date of the card. It is always up to date.
3. A bearer would only require one PID.
4. There would no longer be a need for SIDs that are less secure then PIDs.
5. When stolen, you only need to report/reapply for one card instead of numerous cards.
6. The real-time and continuous verification of bearer rights would facilitate the identification and removal from circulation of stolen or fraudulent PIDs

One of the few disadvantages would be that digital systems would need to be available and accessible to officials at all times. System down-time could result in significant impacts to travel and other activities that will always require PID verification. These disadvantages could be dealt with, however, through established procedures now in place to create independent power back ups, information redundancy and mirrored access for essential digital networks—such as those that currently exist in defense and banking systems or other properly secured corporate networks.

An additional hesitancy could also be envisaged by those who might be reluctant to have all their ID establishment reflected in just a single card (especially for suppliers who currently furnish the global population with multiple PIDs and SIDs). For the bearer, however, the separation of rights from ID establishment would minimize the implications of a lost or stolen PID, which brings to mind how a bearer's ID could be established if they were no longer in possession of their only form of physical ID, and where this line of thought would take us if carried to its logical conclusion.

3. Replacing the physical document by a virtual document

The ultimate step in this process would be to eliminate the physical document altogether and replace it with a 'virtual document' (basically the rights information alone that would be displayed electronically when an official queried an individual's rights). Biometric information is currently being employed in the newest ePassports and visas to assist officials in establishing a PID bearer's identity, but why not simply have the traveler submit to biometric scans at point of entry and forego the need for a physical document completely? This

would be the next step in the evolution of our ability to ascertain the identification and rights of all citizens in a fully digital age.

Clemens Willemsen works for the Dutch Department of Justice where he is involved in identity management and biometrics. This article is his personal view only and does not necessarily reflect the point of view of his government or its respective departments. ■

Portugal: capitalising on the full ePassport potential

With over 50 percent of the world's annual total of new passports now conforming to ICAO's ePassport specifications, and with the number of countries still using non-Machine Readable Travel Documents (non-MRTDs) growing smaller year by year toward ICAO's 2010 MRTD implementation deadline, the *MRTD Report* will be devoting its attention in coming issues to highlighting the work of specific countries in the efforts they've extended in adapting to and implementing new MRTD standards.

In this second instalment of the Report's national profiles, Dr. José Magalhães, Secretary of State for Portugal, provides a testament to the importance of the new ICAO standards in the development of his country's impressive ePassport and passenger facilitation systems.

***ICAO MRTD Report:* How did ICAO's work in developing MRTD standards and specifications assist Portugal in its own efforts to modernize its passport?**

Dr. José Magalhães: Working closely with ICAO has played a decisive role in our efforts to fight against time constraints and limit the huge risks in project management that can detrimentally affect this type of large-scale infrastructure effort. As we were latecomers at the time (our project was launched in April 2005), not only did we carefully consider ICAO standards and documents as we finalized our planning, but we also requested to participate in the related MRTD working groups.

Portugal wanted to benefit from the knowledge of a worldwide network of experts who were capable of helpings us solve concrete problems. That very practical support was provided in a very timely manner with the assistance of ICAO and we learned the lessons we needed to very quickly. We could, of course, be proud of the fact that we were such fast learners, but the excellent assistance and guidance we received was probably what really made the difference.

Has Portugal also developed new visas or ID cards as part of its recent work in this area and, if so, have ICAO specifications been helpful in this regard as well?

The new single European residence permit model takes ICAO's standards and specifications strictly into consideration. Before the end of this year these new biometric cards will begin to be issued by our Border Control Service in association with the Portuguese Government Printing House (IN-CM). With respect to ID cards, as of yet no mandatory standards have been established at the European Union level, but despite this an effort has been made by Portugal to incorporate ICAO's standards into our Citizen Card project, which is now being gradually expanded.

Lessons will be learned during the first months of service for the new card, which is presently replacing four separate low-security cards that had been previously issued (ID cards, health cards, social security cards and taxpayer's cards).

To get back to travel-related matters for a moment, Portugal's passenger facilitation system (RAPID) is now one of the most advanced in the world. Could this type of system have been developed without the hard work that has been done to make the new generation of MRTDs as globally interoperable as they are?

Definitely not. The key point that led to RAPID was this basic question: now that more and more electronic passports are being issued, how can we make passengers feel that besides being secure the new documents can make travelling easier and faster? The answer to this question always came back to the manned checkpoints and whether or not we could devise a system to replace them. Obviously, security was one of our primary considerations as we considered the various options before us. We concluded that if we could compare the picture inside the passport chip with an image obtained in real-time at the checkpoint, and then augment that verification with as many queries as possible in the available security databases, then we just might be able to achieve the desired result.

The first feedback generated by our original pilot project in Algarve was overwhelmingly positive in every regard. The final result is that RAPID is now fully installed in most of our airports and on certain days some machines are processing up to 3,000 passengers!

What countries' travel documents are currently capable of being read with the RAPID system?

Any holders of the 27 ePassports compliant with the EU regulations are capable of taking advantage of the RAPID system. Norwegian and Icelandic ePassports are also now compliant.

What is the scope of Portugal's current MRTD program? In other words, how many passports does your country have in circulation, what percentage now conforms to MRTD or ePassport (biometric) specifications, and how many documents are issued on an annual basis?

Of the 3 million passports currently in circulation approximately 670,000 of these are now ePassports (we began to issue our electronic document as of August 28, 2006). I should note that the Portuguese ePassport has become very popular. Citizens admire the fact that no paper forms or photographs are used. We established rigorous processes as concerned issuance and delivery, but, in all, Portugal's citizens enjoy almost zero bureaucracy, zero narrow-mindedness and very short delays in delivery.

Moreover, facts have confirmed that by decentralizing the enrolment of data and centralizing the issuance of passports (delivered to any part of the world by a leading distribution network) we can achieve a win-win solution. Once and for all Portugal has said adieu to stolen or lost blank booklets. ■

This glossary is included to assist the reader with terms that may appear within articles in the *ICAO MRTD Report*. This glossary is not intended to be authoritative or definitive.

Anti-scan pattern An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print, but when the original is scanned or photocopied the embedded image becomes visible.

Biographical data (biodata) The personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the biographical data page of a passport book, or on a travel card or visa.

Biometric A measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrollee.

Biometric data The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).

Biometric sample Raw data captured as a discrete unambiguous, unique and linguistically neutral value representing a biometric characteristic of an enrollee as captured by a biometric system (for example, biometric samples can include the image of a fingerprint as well as its derivative for authentication purposes).

Biometric system An automated system capable of:

1. capturing a biometric sample from an end user for a MRP;
2. extracting biometric data from that biometric sample;
3. comparing that specific biometric data value(s) with that contained in one or more reference templates;
4. deciding how well the data match, i.e. executing a rule-based matching process specific to the requirements of the unambiguous identification and person authentication of the enrollee with respect to the transaction involved; and
5. indicating whether or not an identification or verification of identity has been achieved.

Black-line/white-line design A design made up of fine lines often in the form of a guilloche pattern and sometimes used as a border to a security document. The pattern migrates from a positive to a negative image as it progresses across the page.

Capture The method of taking a biometric sample from the end user.

Certificating authority A body that issues a biometric document and certifies that the data stored on the document are genuine in a way which will enable detection of fraudulent alteration.

Chemical sensitizers Security reagents to guard against attempts at tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.

Comparison The process of comparing a biometric sample with a previously stored reference template or templates. See also “One-to-many” and “One-to-one."

Contactless integrated circuit An electronic microchip coupled to an aerial (antenna) which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.

Counterfeit An unauthorized copy or reproduction of a genuine security document made by whatever means.

Database Any storage of biometric templates and related end user information.

Data storage (Storage) A means of storing data on a document such as a MRP. Doc. 9303, Part 1, Volume 2 specifies that the data storage on an ePassport will be on a contactless integrated circuit.

Digital signature A method of securing and validating information by electronic means.

Document blanks A document blank is a travel document that does not contain the biographical data and personalized details of a document holder. Typically, document blanks are the base stock from which personalized travel documents are created.

Duplex design A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.

Embedded image An image or information encoded or concealed within a primary visual image.

End user A person who interacts with a biometric system to enroll or have their identity checked.

Enrollment The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Enrollee A human being, i.e. natural person, assigned an MRTD by an issuing State or organization.

ePassport A Machine Readable Passport (MRP) containing a contactless integrated circuit (IC) chip within which is stored data from the MRP data page, a biometric measure of the passport holder and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology, and which conforms to the specifications of Doc. 9303, Part 1.

Extraction The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

Failure to acquire The failure of a biometric system to obtain the necessary biometric to enroll a person.

Failure to enroll The failure of a biometric system to enroll a person.

False acceptance When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

False Acceptance Rate (FAR) The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The false acceptance rate may be estimated as FAR = NFA / NIIA or FAR = NFA / NIVA where FAR is the false acceptance rate, NFA is the number of false acceptances, NIIA is the number of impostor identification attempts, and NIVA is the number of impostor verification attempts.

False match rate Alternative to "false acceptance rate;" used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection."

False non-match rate Alternative to "false rejection rate;" used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of "false acceptance" and "false rejection."

False rejection When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate (FRR) The probability that a biometric system will fail to identify an enrollee or verify the legitimate claimed identity of an enrollee. The false rejection rate may be estimated as follows: FRR = NFR / NEIA or FRR = NFR / NEVA where FRR is the false rejection rate, NFR is the number of false rejections, NEIA is the number of enrollee identification attempts, and NEVA is the number of enrollee verification attempts. This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of enrollees. The false rejection rate normally excludes "failure to acquire" errors.

Fibres Small, thread-like particles embedded in a substrate during manufacture.

Fluorescent ink Ink containing material that glows when exposed to light at a specific wavelength (usually UV) and that, unlike phosphorescent material, ceases to glow immediately after the illuminating light source has been extinguished.

Forgery Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.

Front-to-back (see-through) register A design printed on both sides of the document or an inner page of the document which, when the page is viewed by transmitted light, forms an interlocking image.

Full frontal (facial) image A portrait of the holder of the MRP produced in accordance with the specifications established in Doc. 9303, Part 1, Volume 1, Section IV, 7.

Gallery The database of biometric templates of persons previously enrolled, which may be searched to find a probe.

Global interoperability The capability of inspection systems (either manual or automated) in different States throughout the world to obtain and exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States. Global interoperability is a major objective of the standardized specifications for placement of both eye readable and machine readable data in all ePassports.

Guilloche design A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re-originated by access to the equipment, software and parameters used in creating the original design.

Heat-sealed laminate A laminate designed to be bonded to the biographical data page of a passport book, or to a travel card or visa, by the application of heat and pressure.

Holder A person possessing an ePassport, submitting a biometric sample for verification or identification while claiming a legitimate or false identity. A person who interacts with a biometric system to enroll or have their identity checked.

Identifier A unique data string used as a key in the biometric system to name a person's identity and its associated attributes. An example of an identifier would be a passport number.

Identity The collective set of distinct personal and physical features, data and qualities that enable a person to be definitively identified from others. In a biometric system, identity is typically established when the person is registered in the system through the use of so-called "breeder documents" such as birth certificate and citizenship certificate.

Identification/Identify The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the ePassport holder whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with "Verification."

Image A representation of a biometric as typically captured via a video, camera or scanning device. For biometric purposes this is stored in digital form.

Impostor A person who applies for and obtains a document by assuming a false name and identity, or a person who alters his physical appearance to represent himself as another person for the purpose of using that person's document.

Infrared drop-out ink An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be detected in the infrared region.

Inspection The act of a State examining an ePassport presented to it by a traveler (the ePassport holder) and verifying its authenticity.

Intaglio A printing process used in the production of security documents in which high printing pressure and special inks are used to create a relief image with tactile feel on the surface of the document.

Issuing State The country writing the biometric to enable a receiving State (which could also be itself) to verify it.

JPEG and JPEG 2000 Standards for the data compression of images, used particularly in the storage of facial images.

Laminate A clear material, which may have security features such as optically variable properties, designed to be securely bonded to the biographical data or other page of the document.

Laser engraving A process whereby images (usually personalized images) are created by "burning" them into the substrate with a laser. The images may consist of both text, portraits and other security features and are of machine readable quality.

Laser-perforation A process whereby images (usually personalized images) are created by perforating the substrate with a laser. The images may consist of both text and portrait

images and appear as positive images when viewed in reflected light and as negative images when viewed in transmitted light.

Latent image A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, most commonly achieved by intaglio printing.

LDS The Logical Data Structure describing how biometric data is to be written to and formatted in ePassports.

Live capture The process of capturing a biometric sample by an interaction between an ePassport holder and a biometric system.

Machine-verifiable biometric feature A unique physical personal identification feature (e.g. an iris pattern, fingerprint or facial characteristics) stored on a travel document in a form that can be read and verified by machine.

Match/Matching The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. A decision to accept or reject is then based upon whether this score exceeds the given threshold.

Metallic ink Ink exhibiting a metallic-like appearance.

Metameric inks A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths.

Microprinted text Very small text printed in positive and or negative form, which can only be read with the aid of a magnifying glass.

MRTD Machine Readable Travel Document, e.g. passport, visa or official document of identity accepted for travel purposes.

Multiple biometric The use of more than one biometric.

One-to-a-few A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals, terrorists, etc.

One-to-many Synonym for "Identification."

One-to-one Synonym for "Verification."

Operating system A programme which manages the various application programmes used by a computer.

Optically Variable Feature (OVF) An image or feature whose appea-rance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are. features including diffraction structures with high resolution (Diffractive Optically Variable Image Device (DOVID), holograms, colour-shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.

Optional data capacity expansion technologies Data storage devices (e.g. integrated circuit chips) that may be added to a travel document to increase the amount of machine readable data stored in the document. See Doc. 9303, Part 1, Volume 2, for guidance on the use of these technologies.

Overlay An ultra-thin film or protective coating that may be applied to the surface of a biographical data or other page of a document in place of a laminate.

Penetrating numbering ink Ink containing a component that penetrates deep into a substrate.

Personalization The process by which the portrait, signature and biographical data are applied to the document.

Phosphorescent ink Ink containing a pigment that glows when exposed to light of a specific wavelength, the reactive glow remaining visible and then decaying after the light source is removed.

Photochromic ink An ink that undergoes a reversible colour change when exposed to UV light.

Photo substitution A type of forgery in which the portrait in a document is substituted for a different one after the document has been issued.

Physical security The range of security measures applied within the production environment to prevent theft and unauthorized access to the process.

PKI The Public Key Infrastructure methodology of enabling detection as to whether data in an ePassport has been tampered with.

Planchettes Small visible (fluorescent) or invisible fluorescent platelets incorporated into a document material at the time of its manufacture.

Probe The biometric template of the enrollee whose identity is sought to be established.

Rainbow (split-duct) printing A technique whereby two or more colours of ink are printed simultaneously by the same unit on a press to create a controlled merging of the colours similar to the effect seen in a rainbow.

Random access A means of storing data whereby specific items of data can be retrieved without the need to sequence through all the stored data.

Reactive inks Inks that contain security reagents to guard against attempts at tampering by chemical erasure (deletion), such that a detectable reaction occurs when bleach and solvents come into contact with the document.

Read range The maximum practical distance between the contactless IC with its antenna and the reading device.

Relief (3-D) design (Medallion) A security background design incorporating an image generated in such a way as to create the illusion that it is embossed or debossed on the substrate surface.

Receiving State The country reading the biometric and wanting to verify it.

Registration The process of making a person's identity known to a biometric system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Score A number on a scale from low to high, measuring the success that a biometric probe record (the person being searched for) matches a particular gallery record (a person previously enrolled).

Secondary image A repeat image of the holder's portrait reproduced elsewhere in the document by whatever means.

Security thread A thin strip of plastic or other material embedded or partially embedded in the substrate during the paper manufacturing process. The strip may be metallized or partially de-metallized.

Tactile feature A surface feature giving a distinctive "feel" to the document.

Tagged ink Inks containing compounds that are not naturally occurring substances and which can be detected using special equipment.

Template/Reference template Data which represent the biometric measurement of an enrollee used by a biometric system for comparison against subsequently submitted biometric samples.

Template size The amount of computer memory taken up by the biometric data.

Thermochromic ink An ink which undergoes a reversible colour change when the printed image is exposed to heat (e.g. body heat).

Threshold A "benchmark" score above which the match between the stored biometric and the person is considered acceptable or below which it is considered unacceptable.

Token image A portrait of the holder of the MRP, typically a full frontal image, which has been adjusted in size to ensure a fixed distance between the eyes. It may also have been slightly rotated to ensure that an imaginary horizontal line drawn between the centers of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured (see Section 2, 13 in this volume of Doc. 9303, Part 1).

UV Ultraviolet light.

UV dull substrate A substrate that exhibits no visibly detectable fluorescence when illuminated with UV light.

Validation The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Variable laser image A feature generated by laser engraving or laser perforation displaying changing information or images dependent upon the viewing angle.

Verification/Verify The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with "Identification".

Watermark A custom design, typically containing tonal gradation, formed in the paper or other substrate during its manufacture, created by the displacement of materials therein, and traditionally viewable by transmitted light.

Wavelet Scalar Quantization A means of compressing data used particularly in relation to the storage of fingerprint images. ■

DeLaRue

performance innovation partnership
a force for authentication

passport

ePassport

visa

national ID card

driver's licence

voter registration

DE LA RUE
IDENTITY SYSTEMS

Tel: +44 (0)1256 605000 Email: IdentitySystems@uk.delarue.com **www.delarue.com**

Trusted Technology

Secure World

Solving Today's Security Challenges

As a global leader in the security industry for more than 30 years, 3M provides reliable and responsive solutions, including:

- Secure Credentials that have security features for passports, cards, and other documents
- Reliable Issuance Systems for enrollment, entitlement, personalization and delivery
- Efficient Authentication Solutions with data capture, document evaluation, person authentication and response

To learn more visit www.3M.com/security/ICAO.

3M