

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Defending the Document

Why even the most advanced machine-readable technologies still rely on the robust and ICAO-recommended physical security features built into modern travel documents

Also in this issue:

Enthusiastic participation at Abuja Regional Symposium
Australian border control solutions • Control testing
Republic of Korea issuance and security • German biometric capture
CUPPS launch success and related Standards • MRTD Glossary of terms





Global Enterprise Technologies Corp.

230 Third Ave. ■ Waltham, MA 02451 ■ USA

T: +1 (781) 890 - 6700

F: +1 (781) 890 - 6320

www.getgroup.com



GET ■ Into the future

Secure Document Issuing Solutions



**ICAO MRTD REPORT
VOLUME 4, NUMBER 2, 2009**

Editorial

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

Content Development

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

Keith Miller, Advertising Representative
Tel: +01 (514) 954 8219, ext. 6293
Fax: +01 (514) 954 6769
E-mail: kmiller@icao.int

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.

Copyright © 2009
International Civil Aviation Organization

PRINTED BY ICAO

Contents

Message from the Editor 4

COVER STORY

Defending the Document

Mr. Charlie Stevens, former head of the National Document Fraud Unit of the United Kingdom's Border and Control Services, discusses the extensive physical security measures that ICAO and its partners have helped to implement in current generations of passports, and explains why these must be maintained as a solid security backbone for current and future MRTD enhancements. 6

Significant progress at Abuja Seminar

A recent Regional Seminar on MRTDs, Biometrics and Security Standards held in Abuja, Nigeria meets its objectives for the target Africa-Indian Ocean Region of ICAO, while drawing additional States from as far away as Latin America and clearly demonstrating that ICAO's outreach efforts in this field are highly appreciated and necessary with the April 2010 compliance deadline now rapidly approaching. 12

EAC conformity and interoperability testing

A review of the new ePassport Extended Access Control (EAC) Conformity & Interoperability Tests completed in late 2008 under the auspices of the Brussels Interoperability Group and the European Commission Joint Research Centre, Ispra 16

Australia's approach to automated border control

Discussing the challenges relating to the automated or semi-automated processing of biometric characteristics to determine or authenticate identity in the Australian context, and the new SmartGate technology that is helping to provide a solution at Australian's borders 17

CUPPS goes live at Las Vegas McCarran

Reviewing the world's first live tests of the next generation of airport passenger check-in technology, known as Common Use Passenger Processing Systems (CUPPS) 19

CUPPS in detail: An interview with Samuel Ingalls

Samuel G. Ingalls, 1998 Computerworld-Smithsonian Laureate for technological innovation in the transportation industry, discusses the new CUPPS technology and ICAO's role in providing a basis for its development 20

Republic of Korea issuance advances

The Republic of Korea launched its new electronic passport in August of last year, with plans and capacity now in place to personalize and issue more than 6 million new ePassports per year as its programme moves forward. 23

Biometric capture: The German fingerprint initiative

Dr. Uwe Seidel, Senior Scientist, Forensic Science Institute, Identity, Documents, Bundeskriminalamt, Germany, reports on the preparation, experience and results achieved so far as more than 5,000 municipal offices across Germany begin the process of fingerprint biometric capture. 24

MRTD Glossary of Terms 31



Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)

Member	Nominated by	Member	Nominated by
Mr. R. M. Greenwood	Australia	Ms. A. Offenberger	New Zealand
Mr. G. K. McDonald	Canada	Mr. A. Famodimu	Nigeria
Ms. M. Cabello	Chile	Mr. C. Ferreira Gonçalves	Portugal
Mr. M. Vacek	Czech Republic	Mr. O. Demidov	Russian Federation
Mr. Y. Dumareix	France	Mr. S. Tilling	Sweden
Dr. E. Brauer	Germany	Mr. R. Vanek	Switzerland
Mr. S. Ramachandran	India	Mr. R. Chalmers	United Kingdom
Mr. H. Fukuyaama	Japan	Mr. M. Holly	United States
Ms. E. Gosselink	Netherlands		

The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

The TAG/MRTD develops specifications for machine readable passports, visas and official travel documents, electronic machine readable travel documents and guidance material to assist States in implementing these specifications and exploiting modern techniques in inspection systems.

Observer organizations

- Airports Council International (ACI)
- European Commission (EC)
- International Air Transport Association (IATA)
- International Criminal Police Organization (INTERPOL)
- International Labour Organization (ILO)
- International Organization for Standardization (ISO)
- Organization for Security and Cooperation in Europe (OSCE)
- United Nations Counter-Terrorism Committee Executive Directorate (CTED)
- International Organization for Migration (IOM)

ICAO's Global Presence



ICAO MRTDs, Biometrics and Security Standards

21–23 September 2009

ICAO HQ, Montreal, Canada

ICAO will hold its Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards from 21–23 September 2009. An Exhibition will complement the Symposium and highlight important products and services related to MRTDs, biometric identification and border inspection systems.

The Symposium will focus on ICAO's pivotal role in coordinating the development and implementation of the MRTD Programme as a means of strengthening integral travel document issuance and border security programmes. It will also highlight the United Nations' Global Counter-terrorism Strategy and the importance of ensuring the integrity of the systems through which travel documents are issued. This includes the inspection, verification and examination of ID breeder documents, and serves to demonstrate how effective travel document security can significantly augment activities targeting the detection and prevention of criminal and terrorist mobility.

Your participation is encouraged. Presentations and handouts will be available only in English. Simultaneous interpretation will be available in English, French, Spanish and Russian, as required. For further information on the programme, exhibition, and arrangements for the Symposium, please be sure to visit:

www.icao.int/MRTDsymposium/2009

Efforts are being made to encourage currently non-compliant States to issue ICAO-Standard Machine Readable Travel Documents (MRTDs) by the April 2010 deadline. If your State is not yet issuing these documents please contact the ICAO MRTD Programme for further information.



Priorities and progress

This issue of ICAO's *MRTD Report* draws focus on two separate but key ongoing priorities that are moving forward the security and facilitation objectives associated with ICAO's Standard-setting in this area.

In our feature presentation from Mr. Charlie Stevens on "Defending the document", ICAO and the broader global border control community are reaffirming our belief that all technological and logistical progress being made with Machine-readable Passports (MRPs) still relies on the robust security features of the printed documents that provide the physical "platform", as it were, for existing and emerging MRTD and biometric advances. Decades of knowledge and expertise are reflected in these unassuming printed booklets and they still provide a robust and highly dependable first line of defence against would-be fraudsters and identity thieves.

Another key focus of this issue is the review of the recent Regional Seminar on MRTDs, Biometrics and Security Standards held in April 2009 in Abuja, Nigeria. This event not only met its objective of providing consolidated and cost-effective expert MRTD compliance advice to States in the target Africa-Indian Ocean Region of ICAO, but the additional turnout from States from as far away as Latin America, Europe, the Middle East and Asia-Pacific also clearly demonstrated that ICAO's outreach efforts in this field are highly appreciated and necessary with the April 2010 compliance deadline now rapidly approaching. More work of this sort will be done leading up to and after 2010 as ICAO

continues to provide the leadership and expertise in this field that States so clearly require.

Additionally in this issue, readers from States now considering the inclusion of biometric elements in their existing or planned MRTDs will find Uwe Seidel's review of biometric capture in Germany very worthwhile reading. He provides excellent and very practical perspectives on the challenges in this area. Elsewhere there are profiles of some of the effective solutions being developed by States such as the Republic of Korea (issuance and distribution) and Australia (border control automation).

Lastly, there are some interesting developments now occurring in airport passenger terminal technology and the new Common Use Passenger Processing Systems (CUPPS) Technical Specification that are profiled and detailed in an excellent Q&A with Mr. Samuel Ingalls—one of the foremost specialists in this field. The CUPPS development is yet another example of the excellent work which is now evolving from the fundamental ICAO Doc. 9303 Standards and Specifications and which is indicative, yet again, of the tremendously effective collaborative effort now ongoing among key aviation organizations and stakeholders.

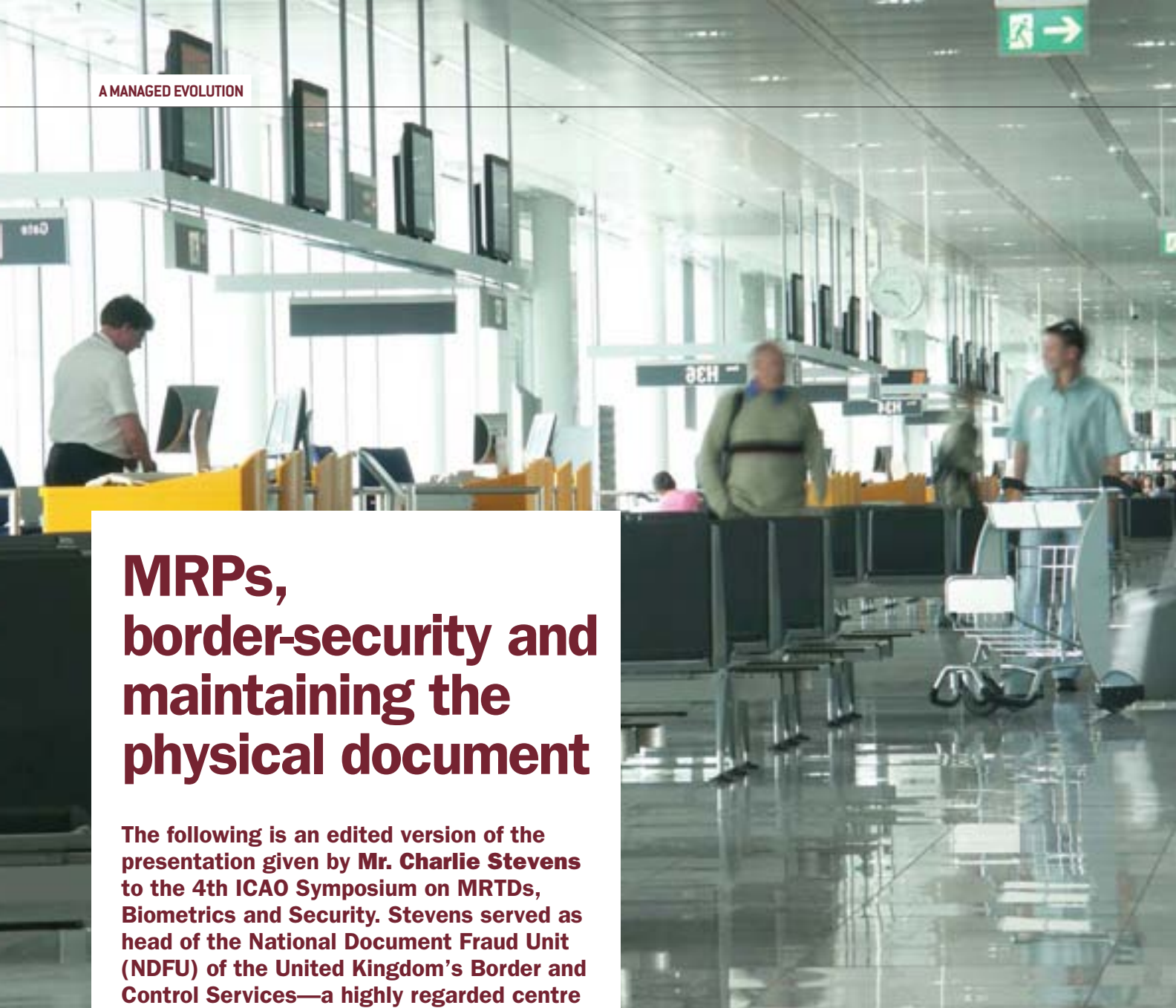
Happy reading,

Mauricio Siciliano
Editor



Leadership and Vision in Global Civil Aviation





MRPs, border-security and maintaining the physical document

The following is an edited version of the presentation given by **Mr. Charlie Stevens** to the 4th ICAO Symposium on MRTDs, Biometrics and Security. Stevens served as head of the National Document Fraud Unit (NDFU) of the United Kingdom's Border and Control Services—a highly regarded centre of expertise with respect to the examination of suspect travel documents and the gathering and disseminating of intelligence surrounding travel document fraud.

Stevens was involved with immigration services for more than 39 years, and has helped to develop the immigration control measures now in place at Gatwick and Heathrow airports. He has also spent extensive periods working on secondments to diplomatic services in India and Pakistan, consulting on entry clearance and visa matters. Stevens was also a long-standing and very active member of the ICAO New Technologies Working Group (NTWG).

I'd like to extend my thanks to ICAO for inviting me to speak to you today on the continuing importance of robust physical security features for passports and other identity documentation. This is particularly relevant in our "New World" of eDocuments and smart cards using stored biometric identifiers.

As you've just heard from the introduction, my background in this area derives not from the document-producing area but rather the "customer" side: in effect the men and women who use and test the documents at border control hubs and in immigration enforcement scenarios. The aim of my presentation today is firstly to talk about the role of ICAO in developing new ePassports and travel documents, and then to talk about the challenge of achieving full global adoption of ICAO-specified ePassports and travel documents.

I also intend to touch upon the need for backward compatibility and the continuing value of maintaining robust physical document security features as we evolve into the future. I realize other speakers have already broached this topic but I think it's a very, very important message to bring to you today.

ICAO's important role and the challenge of global adoption

ICAO has, for decades now, assumed a leadership role in the development of standard specifications for passports and travel documents. The first manual of guidance material for States was published by the Organization in 1980 as the first edition of Document 9303. This content has now evolved over the years into a three-part reference covering specifications and standards for machine-readable passports, visas and other travel documents—including card formats.

The aim of ICAO in developing these specifications was to facilitate international border crossing for an increasing numbers of travellers. This would be achieved by creating standardized layouts for machine-readable travel documents (MRTDs) to enable the 190 Member States of ICAO to have their respective passports and documents recognizable and verifiable by every Member State's border control officials.

ICAO also recognized the security and criminal threats posed by the abuse of travel documents and therefore built minimum specifications into their standards covering the physical security of new travel documents. This involved the incorporation of a minimum set of high-security features that could be checked and tested by properly trained border control officials, while at the same time frustrating forgers or counterfeiters attempting to compromise the documents. ICAO similarly provided advice and minimum standards for travel

document-issuing authorities in order to secure and maintain the integrity of the application and issuing processes for travel and identity documents. It bears repeating here that there's no point in producing a secure document unless the issuing and application processes are also equally secure.

An important and self-imposed measure of success of ICAO's work in this area was its target for global interoperability: i.e. the ability of all countries' passports and travel documents to be recognizable and their integrity able to be established by both visual examination and machine reading, in addition to verifying the identity and nationality of the person presenting the documents.

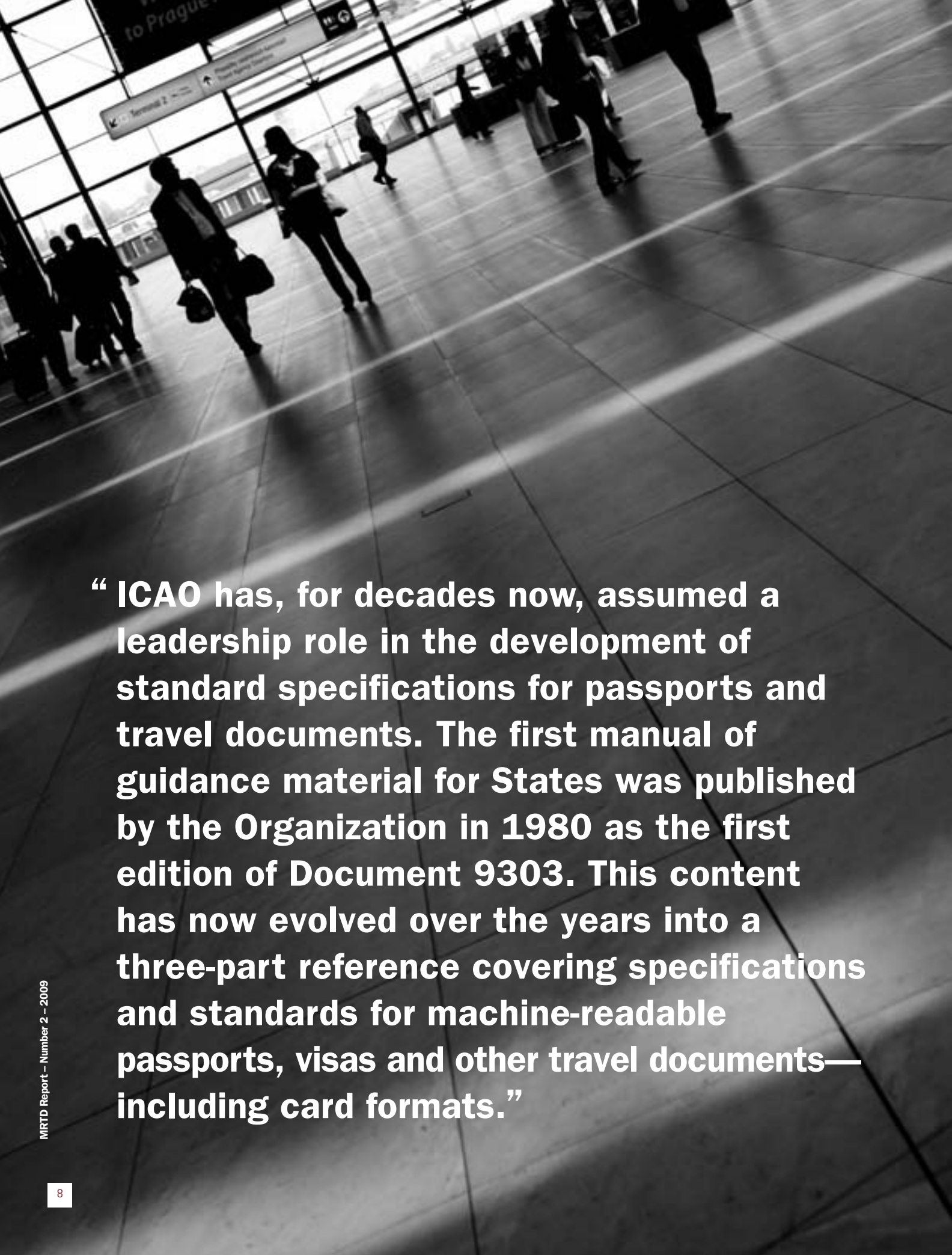
ICAO recognized that there would always be a risk of forgery or counterfeiting of travel documents, and, in particular, it was concerned that genuine documents presented by imposters (or look-alikes, as we call them) as well as stolen blank documents fraudulently made to look



Mühlbauer
High Tech International

**Your Proven Technology Partner For
Smart ID Documents**

- Complete equipment range for production, personalization, packaging & mailing of high quality ID documents
- Complete turnkey solutions for data enrollment, secure document management, personalization & production management and verification
- Excellent proximity & customer services worldwide



“ ICAO has, for decades now, assumed a leadership role in the development of standard specifications for passports and travel documents. The first manual of guidance material for States was published by the Organization in 1980 as the first edition of Document 9303. This content has now evolved over the years into a three-part reference covering specifications and standards for machine-readable passports, visas and other travel documents—including card formats.”

official, might still remain able to deceive border control officials and conventional reader devices that simply seek to verify the contents of a document's machine-readable zone, or MRZ.

So it was natural, therefore, for ICAO to look at new and developing technologies to assist in providing additional layers to the document security and verification process. In the 1990s, the ICAO NTWG started to consider the technical feasibility of the introduction of biometric technology into travel documents. This work was well under way at the time of the 9/11 attacks in New York in 2001, events which in turn led to political and legislative demands in the USA and the EU for more rapid introduction and issuance of biometric ePassports and travel documents. These demands finally came into effect in 2006 with the introduction of new eTravel documentation.

I must emphasize, however, that it was never the intention of ICAO for biometric identifiers to become a panacea for determining the identity of document holders. Biometrics were—and still are—considered by ICAO to be an extremely useful but additional security safeguard to the existing range of document security safeguards and features employed in machine-readable travel documents.

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

The question that may be asked, then, is why all countries are not currently issuing ICAO-specification travel and identity documents, or the new-specification ePassports?

The fact is that the majority of international travellers today do hold passports or documents issued by States that produce ICAO specification MRTDs. There is still a large number of countries, however, that have not yet introduced documents according to ICAO's relevant Standards. ICAO introduced the specifications for globally-interoperable MRTDs as far back as 1980—over 28 years ago. It has been a long and often a torturous



process in encouraging States worldwide to introduce these documents. While ICAO sets the global Standards and specifications, there's no legal mandate over States to comply and therefore ICAO Standards only become mandatory when certain States or groups of States, such as the EU, pass their own legislation requiring the introduction of these specifications by law.

It should be noted that it has not been the case where only developing countries that have been slow to accept ICAO Standards for their documents. Even in the UK it took until 1988 to introduce ICAO-compliant documents: eight years after the Standard's introduction by ICAO. And it was not until 1995 that my country had full machine-reading capability of the documents at our border control outposts. Indeed, ICAO was so concerned about the global uptake of machine-readable document specifications, setting aside for the moment the whole question of the newer ePassport Standards, that in 2005 it sought and achieved agreements to a new Standard in Annex 9 facilitation to the Convention adopted by its then 188 Member States. This new agreement stipulated that all ICAO States would need to be issuing ICAO-compliant, machine-readable passports by April 1, 2010.

Active encouragement of all States to meet this target is now being worked towards by ICAO and numerous governments and international bodies, such as the G8 group of States, and an ICAO programme called the Universal Implementation of Machine-Readable Travel Documents (UIMRTD). This programme aims to offer technical advice and assistance to non-compliant States to meet the 2010 deadline. While the aim is to achieve global interoperability of machine reading for passports, it is acknowledged that, even if the 2010 deadline is met, then there will still be a further period of up to ten years when non-compliant legacy documents could remain in circulation.



- Lastly, legislation to issue ePassports by individual States is growing, but it is still a long way short of achieving a global requirement on all States to move to ePassports.

Security and verification of chip data depends on a sophisticated public key infrastructure (PKI). This requires exchanges of vital information between all States globally on a regular basis and that, I'm afraid, is proving slow to achieve at present, despite the advent of the ICAO Public Key Directory (PKD). I can only hope that this 4th ICAO Symposium will act as a spur to encourage States to participate in the PKD, because it's vital for the long-term success of eDocuments.

The UIMRTD programme is focusing on standard MRTDs for the time being. Given the time scales that I've described to achieve global interoperability for standard or non-biometric MRTDs, it will be clearly many years into the future before full global uptake is achieved of the new ePassports and eTravel documents. The problems with uptake of these documents are in many respects greater than for the standard MRTDs for the following reasons:

- The cost of producing ePassports with the associated chip technology is greater than for non-chip passports.
- The cost of installing and using machine readers for ePassports and travel documents at all immigration and enforcement control points, and for training purposes, is substantial, particularly if verification of the chip data and one-to-one biometric comparison of document holders with chip data is to be achieved.
- Given the logistics of installing ePassport readers, it will be many years before all remote border crossings and other checkpoints globally are provided with ePassports biometric verification readers. In the interim, these checkpoints will require manual checking of documents.
- Chip technology in travel documents with validity periods of up to ten years is new. We've only had them in place for a couple of years now.
- If a chip fails to read in an ePassport, other than through malicious damage, then the passport will still remain a valid passport certifying the identity and nationality of the holder. We will then be relying on conventional, physical document security safeguards to confirm the veracity of the personal data contained therein and the entitlement of the person presenting the document to hold it.

All this being said, the situation is not necessarily one of "doom and gloom". Fifty-four States are now issuing ePassports. By the end of 2009, it is expected that this will increase to 90 States. This will then make the number of ePassports being issued worldwide equal to 70 to 80 percent of the total annual volume of passports now issued, or around 120 million documents. There is every good reason to be optimistic about the future therefore, despite any current shortcomings in compliance.

Backward compatibility

Given the problems that I have just mentioned to you, it is unlikely that global issuance standardization or interoperability of biometrics-based documents will be achievable for a number of years yet. ICAO is aware of this and so it has always emphasized the need for backward compatibility in its document developing processes. What we mean by this is that traditional standards for document layout and format are carried forward into any new, higher technology documents, and therefore that even the newest and most advanced ePassport readers will also be able to read older-generation MRTDs.

The layouts and physical security features built into new ePassports will also be of the same, robust standards seen in the previous model documents. ICAO, again, recognizes this need and is keen to ensure that States do not let traditional physical security safeguards and features deteriorate in any way.

I must also very strongly emphasize that the ability of enforcement staff and border control officials to examine any newly-issued documents remains of paramount importance. Unless document examiner skills remain relevant and up-to-date, you're not going to be able to ensure that you have a

“ I must also very strongly emphasize that the ability of enforcement staff and border control officials to examine any newly-issued documents remains of paramount importance. Unless document examiner skills remain relevant and up-to-date, you’re not going to be able to ensure that you have a comprehensive system of detecting fraud and testing the travel documents that are presented at border controls.”

comprehensive system of detecting fraud and testing the travel documents that are presented at border controls.

Importance of a high-quality physical document

In addition to the excitement now being expressed by border control and enforcement circles about the newest biometric ePassports, there is still a very firm requirement among control authority practitioners for the maintenance of high quality, robust physical security features in travel documents well into the future. I’d like to conclude now by providing you with a few illustrations of some of the types of document security features that have proved themselves robust and valuable for control authority inspections.

Firstly, quality passport covers with detailed embossing. One might think

yes, of course all States have attractive passport covers, but it’s the quality of the cover that is essential here.

A passport is a high-security as well as a high-quality document. This is what makes it difficult for forgers and counterfeiters to replicate. When we put golden embossing on a passport cover, it’s not simply to make it look pretty—it’s there because the fine detail that is used is an excellent security standard that forgers can often find frustrating in trying to overcome.

Some people similarly question the need for a document’s front-end paper and especially high quality intaglio printing. The practical usefulness here is that, if you’re going to get a passport issuant to change bio data page, you have to physically dismantle the passport. This often requires lifting the end papers to get at the security thread to dismantle it. Very highly secure end-paper is therefore

essential, and high quality security safeguards such as intaglio print, which gives you very fine and raised typeface, also provide an important high-quality safeguard which is very easy to test by border control officials who’ve been properly trained.

Another very important element is the high quality ultraviolet safeguards to show if the laminate has been lifted or if any of the data has been altered. This doesn’t just apply to a paper bio data page, such as in the UK document, but also in the Swedish passport, for example, which has got a polycarbonate insert.

And last but not least bio data pages. Most of the examples I’m showing you here are from the UK passport, but you’ll all recognize the layout, no matter which country you come from, thanks to the ICAO-specified layout. This commonality is vitally important to border control officials because they immediately know what to look for, and it helps to reinforce the importance of ICAO’s ongoing efforts to make the world’s documents as standardized as possible. ■

DILETTA

Inkjet ePassport Printer with UV Color Feature

**Your competent partner
for personalisation systems and
Machine Readable E-Passports**

**Votre partenaire compétent
pour les systèmes de personnalisation
et les passeports électroniques**





Cooperative Regional efforts continue to improve State compliance

Abuja MRTD event demonstrates usefulness and importance of ongoing Regional efforts by ICAO and partnering stakeholders

ICAO's Regional Seminar on Machine Readable Travel Documents (MRTDs), Biometrics and Security Standards, held this past April in Abuja, Nigeria, was a first of its kind for the Africa-Indian Ocean (AFI) Region. Participating international partners included the International Organization for Migration (IOM) and the Organization for Security and Co-operation in Europe (OSCE). The event was hosted by Nigeria and co-sponsored by the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), and organized pursuant to ICAO's commitment to assist States in their implementation of ICAO-Standard MRTDs—the deadline for which is April 1st, 2010.

From left to right: Mrs. Folasade Odotola, Director ICAO Air Transport Bureau; Dr. O.B. Aliu Representative of Nigeria on the ICAO Council; Dr. H.O. Demuren, Director General and Chief Executive Officer of the Nigerian CAA; Mr. Babatunde Omotoba, Nigeria's Minister of Aviation; Major General Godwin Abbe (retired), Nigeria's Minister of the Interior; and Mr. C.J. Udeh, Nigeria Comptroller General of Immigration.

ICAO's recent Regional Seminar on Machine Readable Travel Documents (MRTDs), Biometrics and Security Standards was a resoundingly successful event that drew over 300 participants from 25 States located in the ICAO AFI, European/North American (EURNAT), Middle East (MID) and South American (SAR) Regions. African representatives were by far the majority of those attending and both English and French-speaking States were well-represented in that respect. It is to be noted that, to-date, 10 of the 18 States which are still non-compliant with ICAO's MRTD Standards are located in Africa.

In addition to the International Organization for Migration (IOM), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), all of whom collaborated with ICAO on the Abuja event, the African Civil Aviation Commission (AFCAC) also took part and the ICAO West African (WACAF) Regional Office assisted with the event's organization and coordination. Several WACAF States were represented at the Abuja proceedings.



finally!

A new global hub for MRTD suppliers and information!

Whether you're an MRTD professional looking for the latest guidance, technology and assistance with your upcoming implementation project, or a supplier wanting to leverage the unmatched advertising potential of the web's most targeted location for MRTD decision-makers, **ICAO's new MRTD Community Web Site** is your one-stop shop for success.

For more information regarding listing your company on our site, or to enquire about new advertising opportunities, please contact:

Michelle Villemaire
mvillemaire@icao.int
+1.514.954.8219 ext.7090



www2.icao.int/en/MRTD2



Dr. O. B. Aliu, Representative of Nigeria on the ICAO Council, and Dr. H.O. Demuren, Director General and Chief Executive Officer of the Nigerian CAA.



Major General Godwin Abbe (retired), Nigeria's Minister of the Interior, and Mr. C.J. Udeh, Nigeria Comptroller General of Immigration.



Major General Godwin Abbe (retired), Nigeria's Minister of the Interior and Dr. H.O. Demuren, Director General and Chief Executive Officer of the Nigerian CAA, with vendors.



Mrs. Folasade Odutola, Director of the ICAO Air Transport Bureau; Dr. O.B. Aliu, Representative of Nigeria on the ICAO Council; and Dr. H.O. Demuren, Director General and Chief Executive Officer of the Nigerian CAA.

"The days of meetings and presentations that made up the Abuja Seminar were quite eventful and provided immense opportunities for the exchange of information, networking between Regional and international stakeholders and suppliers, as well as important education about the key issues at the heart of ICAO's desire to have all States compliant by the 2010 deadline," commented ICAO Air Transport Bureau Director, Mrs. Folasade Odutola.

"Personally, it was very gratifying to witness the enthusiasm with which the event was embraced," Odutola continued.

"I was pleasantly surprised at the levels of attendance and participation maintained throughout the proceedings."

Ten industry partners (*see sidebar, page 15*) provided information on the equipment and systems offerings available to assist AFI and additionally-participating States with their MRTD compliance efforts. This information was provided to delegates through an ongoing exhibition as well as via supplier presentations.

It was acknowledged by Mrs. Odutola that the event could not have been the success that it was without the helpful cooperation of the event host—the Nigerian government—primarily through its Civil Aviation Authority (CAA) and Immigration Services department. The State provided excellent facilities and logistical support and Nigeria's Representative to the ICAO Council, Dr. O.B. Aliu, was also present at the event and provided some opening as well as closing remarks during the Seminar.

"I can't over-estimate how important it is to AFI States to have ongoing and expert guidance from ICAO in these and other matters," remarked Dr. Aliu. "Given the turn-out from other Regions this is obviously the case."

"Nigeria has been MRTD compliant since 2003 and ePassports with biometric identifiers were brought in as of 2007," he continued. "We sponsored this event to help provide technical and administrative assistance to other States in our Region who have not moved their MRTD programmes forward to the same degree as Nigeria. This assistance is very useful for AFI States who have not yet had the chance to advance their own implementations and who also are seeking information regarding how to better safeguard their passport issuance procedures—a goal which is of equal importance as the document security measures where overall national security and identity confirmation objectives are concerned."

As well as Dr. Aliu, the Abuja event was also addressed with opening remarks from: Dr. H.O. Demuren, Director General and Chief Executive Officer of the Nigerian CAA; Mr. C.J. Udeh, Nigeria Comptroller General of Immigration; Major General Godwin Abbe (retired), Nigeria's Minister of the Interior; and lastly Mr. Babatunde Omotoba, Nigeria's Minister of Aviation.

EXHIBITORS AT THE ABUJA MRTD SYMPOSIUM INCLUDED:

- Vision-Box
- Giesecke and Devrient
- Digital Identification Solutions
- Trub
- Iris Corporation Berhad
- Indra
- Regula
- Canadian Bank Note Company
- Entrust
- Vlatacom

Specialized consultants addressed the event participants on wide-ranging issues of importance concerning the development and implementation of effective MRTD production and issuance systems, while key national specialists from organizations such as the U.S. Department of Homeland Security, the U.K. Border Agency Fraud Unit, Passport

Canada and the Portuguese Passport Programme also provided useful information and insights throughout the three-day event.

Session I of the Abuja Seminar focused on the foundations of the systems and standards surrounding Machine Readable Passports (MRPs); Session II dealt with identity management and document inspection, examination and handling; and lastly Session III saw presentations from the IOM and OSCE on international cooperation, assistance and data-sharing.

Event co-organizer UNCTED also provided funds in advance which were used to provide sponsorships for six participants from African States—two of whom were unfortunately unable to attend due to last minute inconveniences.

“My last word on this is that our experience at this event will further guide us in formulating future policies and activities in the MRTD field which will enable us to serve the States better,” concluded Mrs. Odotola. “The Abuja MRTD Seminar was a great example of international cooperation at the highest levels and served as an extremely useful tool for advancing ICAO’s Standards, specifications and best practices and priorities in the areas of travel documents issuance processes, border control, security and facilitation in the AFI Region.” ■

Principled
Pride
Honesty
Integrity
Independence
Reason

Principled Secure Solutions Since 1897

cbn
CANADIAN
BANK NOTE
COMPANY, LIMITED

More than 80 nations have engaged CBN as their partner for:

- Travel Documents
- National ID
- Driver Licences
- Civil Registry Documents
- Document Issuing Systems
- Border Management
- Travel Document Readers

Through a consultative approach, we develop and deliver tailored solutions that address the unique challenges encountered by our customers.

www.cbnco.com
identification@cbnco.com

ePassport Extended Access Control conformity & interoperability testing

Prague event returns informative results

New ePassport Extended Access Control (EAC) Conformity & Interoperability Tests were completed in late 2008 in Prague, Czech Republic, held under the auspices of European Commission, the Brussels Interoperability Group and the European Commission Joint Research Centre—Ispra.

Organization of the Prague Tests was provided under sponsorship of the Ministry of the Interior of the Czech Republic, the European Commission Joint Research Centre and partners: State Printing Works of Securities; Secunet. s.r.o.; and OKsystem. This prestigious event welcomed more than 500 delegates from more than 35 countries and was attended by: European and world specialists; suppliers; and State representatives responsible for ePassport issuance,

technical infrastructure implementation and border control.

The EAC tests were divided into three parts: a conformity test; a crossover test and an EAC Public Key Infrastructure (PKI) test. In total more than 1,400 ePassports were tested. Thirty-five world specialists presented briefs at the conference on topics that included security, data protection, cryptography and interoperability. The event also included an exhibition (26 stands of technical equipment and services) as well as meetings of the *European Commission's Article 6 Committee* and the *Brussels Interoperability Group*.

The key target of the Prague Tests was to allow European countries to verify the conformity of ePassports with finger-

print biometric data protected by EAC. A related target was the verification of cross-over interoperability of various EAC inspection systems and ePassports. Test results are reflected in the sidebar (*below*).

Twelve States (Austria, Czech Republic, Germany, Spain, UK, Hong Kong, Switzerland, Macao, Netherlands, Portugal, Sweden and Slovenia) participated in exchanging certificates and 11 of them provided passports for verification. Four States (Czech Republic, Germany, UK and Slovenia) brought their own Inspection systems.

More detailed information and test results are available on the Prague Tests official Web site at: www.e-passports2008.org ■

PRAGUE EAC TEST RESULTS AT A GLANCE

In addition to conformity and cross-over interoperability tests, the Prague event also featured a first attempt to verify process interoperability of the EAC PKI (according to European Certification Policy) for national border inspection systems, including official bilateral exchange of EAC certificates. In total the ePassport tests were conducted over a five-day period.

Conformity tests were organized for layer three and four and layer six and seven. They were performed by five registered laboratories:

- Secunet AG / CETECOM ICT
- European Commission Joint Research Centre, Ispra
- SOLIATIS
- FIME
- HJP Consulting / TÜViT / CETECOM ICT

The conformity tests were divided into two predefined parts:

- a) Guaranteed for EAC passports of the EU Members and;
- b) Optional for non-EU countries, non-European countries and for non-governmental representatives.

ePassport L3-L4 guaranteed part results

From 36 ePassports provided there were 33 without abnormalities.

ePassport L3-L4 optional part results

From 34 ePassports provided there were 24 without abnormalities, eight with abnormalities and two ePassports which required further investigation.

Passports L6-L7 guaranteed part results

Number of passports provided = 34. Of these:

- 10 used DH (CA) and RSA (TA)
- 24 had not implemented AA
- 22 used ECDH (CA) and ECDSA (TA)
- 21 had Type A chips
- 2 used DH (CA) and ECDSA (TA)
- 13 had Type B chips
- 10 had implemented AA

In cross-over tests, 77 passports were tested—from which 75 were implemented with EAC version 1.1.1 and two were Basic Access Control (BAC) only. 26 Inspection systems took part in the cross-over tests.

- 35 used DH (CA) and RSA (TA)
- 49 had not implemented AA
- 37 used ECDH (CA) and ECDSA (TA)
- 50 had Type A chip
- 5 used DH (CA) and ECDSA (TA)
- 27 had Type B chip
- 28 had implemented AA

PKI test

This was the first test session of its kind. During July and August participants exchanged particular requests and EAC PKI certificates between CVCA and DVs to simulate the process which should be realized in the future. During the Prague Tests they were able to perform ePassport verification on inspection systems.

Automated Border Control: The Australian example

Australia's international airports welcomed 23 million passengers in 2008, approximately five percent more than in 2006, according to the Australian Airports Association.

Because of this growing traffic demand, security systems at Australian airports have become stressed to their limits and increasingly vulnerable. Given this structural vulnerability, a situation now shared by many international airports, the Australian Customs Service has stipulated multi-biometric recognition based on ICAO specifications as a prerequisite for enhanced homeland and air transport security.

In this submission to the *ICAO MRTD Report*, Sagem Sécurité, developer of the new SmartGate technology recently implemented on a trial basis in certain Australian facilities, and Mr. Terry Wall, Australia's National Manager, Passenger Operations, discuss the challenges and solutions relating to the automated or semi-automated processing of biometric characteristics to determine or authenticate identity in the Australian context.

To guarantee homeland security in a comprehensive manner, any given State must first counter threats related to airport security. Identity theft is one of the more serious in this respect.

Multi-biometric systems are recommended as one of the most effective solutions now available to help minimize the unlawful entry of undesirable visitors via identity theft. Since each person has his or her own individual characteristics that cannot be changed, lost or stolen, biometric measures are considered the most reliable way of guaranteeing any traveller's identity,

To help it address its concerns in this area, Australian Customs chose Sagem Sécurité in 2004 to help it set up, on a trial basis, a new automated border control system based on the recognition and confirmation of a facial biometric. This system as installed is now more commonly known in the commercial realm as *SmartGate*.

The Australian SmartGate solution was designed not only to help with security concerns, but also to take advantage of the more automated passenger flows that ePassport technology and RFID identifiers now make available. Due to congestion issues in many airports and hubs around the world this is currently an area of significant interest to many additional States and airport authorities as well as Australia and its facilities.

"SmartGate gives eligible Australian and New Zealand travellers arriving into Australia's international airports the option to self-process through passport control," noted Mr. Terry Wall, Australia's National Manager, Passenger

Operations. "It uses the data in the ePassport and facial recognition technology to undertake the Customs and immigration checks that are usually performed at the Entry Control Point."

Benefits of the new Australian system include the ability to process increasing numbers of passengers within existing floor space and covered by existing facilitation rates. The system also enhances border protection and deters the use of forged or stolen passports.

"It's important to note that while SmartGate has the capability to detect imposters and fraudulent documents, it is not designed as a standalone security solution," elaborated Wall. "SmartGate is designed specifically as a border-processing tool in an airport environment and our Customs and Border Protection service has many other security controls in place to complement it."



A New Zealand traveller uses a SmartGate kiosk at Australia's Brisbane Airport facility.

SMARTGATE MILESTONES

2003:	Australian Customs issues request for proposals.
2004:	Sagem Sécurité selected as strategic partner for the SmartGate project.
2004–2007:	Development of the SmartGate system.
June 2007:	First deployment.
December 2008:	SmartGate passes the mark of 150,000 passages in Australia.

AUSTRALIAN CUSTOMS' RATIONALE FOR SELECTING FACIAL RECOGNITION

1. It's the ICAO primary interoperable biometric.
2. It's easy to use.
3. People are used to having their picture taken, particularly when applying for a passport or visa, or to get a driver's license.
4. The digital photograph in the ePassport provides a portable biometric identifier without the need for enrollment or registration.
5. A customs officer can undertake manual backup without needing to be a fingerprint or iris recognition expert.
6. A high degree of accuracy has already been established with facial biometric technology.

For more information please visit: www.customs.gov.au

To meet the challenges of protecting its borders, Australia's Customs and Border Protection uses a combination of well-trained and highly skilled staff, sophisticated intelligence analysis, profiling and strategic planning and state of the art technology. All travellers who use SmartGate are still subject to all existing Customs, immigration and quarantine requirements and will need to present a completed passenger card to a Customs and Border Protection officer at a secondary point in the arrivals hall.

Australian Customs and Border Protection constantly reviews its security procedures and methods and much of the work being done revolves around setting new benchmarks for other Customs and border administration agencies throughout the world.

Automating border control

Australia's main international airports, including Melbourne, Cairns, Brisbane and Adelaide, are now offering the SmartGate automated border crossing option for travellers flying between Australia and New Zealand with electronic travel documents (ePassports in this case).

Employing facial recognition measures using a photo embedded in the

ePassport chip, SmartGate meets all ICAO biometric specifications and enables automated border control when passengers arrive on international flights. The system comprises a biometric gate with three facial recognition cameras, as well as a station equipped with an ePassport reader. The automated system is linked to a computer that manages authorizations to enter Australian territory.

When a traveller enters the system, SmartGate technology acquires a photo of their facial image and compares its parameters to the digital photo contained on the passport. If the two photos match, the SmartGate system gives the traveller a green light. The system employs facial recognition



A typical SmartGate configuration.

algorithms and technologies developed specifically by the supplier.

Simplifying the control process

During the Australian border control process under discussion, qualifying Australian and New Zealand travellers are identified by an automated biometric reader (facial recognition) instead of presenting their passport to a customs official with commensurate line-ups and delays. The entire process takes about 40 seconds, compared to 15 minutes or more for the manual control process.

SmartGate not only bolsters the reliability of travel documents for passengers (since personal data is stored in a chip on the passport), it also fights fraud more effectively (counterfeiting, passport or identity thefts, willful damage of passports, etc.), while helping to speed up passenger traffic inside the airport.

Looking forward

Automated border control using biometric recognition is now a reality and is set for fast deployment, especially in Europe, with the first biometric passports being issued in that Region in the summer of 2009.

The SmartGate system itself has already passed the 150,000 passenger mark, and will be installed at all Australian international airports by the end of 2009.

"Rollout will occur throughout 2009, starting with Perth and Sydney airports before July," noted Wall. "SmartGate kiosks are now also available at Auckland Airport in New Zealand for use by eligible travellers departing for the SmartGate-equipped airports in Australia."

Sagem Sécurité is also working on solutions that include all steps in the passenger facilitation process, from check-in to boarding, through a number of pilot projects now being carried out within the scope of IATA's Simplifying Passenger Travel initiative. ■

New CUPPS platform goes live at Las Vegas McCarran International Airport

Hundreds of WestJet Airlines guests boarded their regularly scheduled flights from Las Vegas, NV to Calgary, Alberta, on January 15, 2009, without noticing anything unusual. Everyone involved had just participated in the world's first live test of the next generation of passenger check-in technology known as Common Use Passenger Processing Systems (CUPPS).

By introducing a new worldwide electronic standard, CUPPS promises to save millions of dollars for airlines and airports. Software developers at all airlines will now have a universal standard detailed enough to eliminate the variations that previously made interoperability next to impossible to achieve.

The glitch-free first test at Las Vegas McCarran includes Continental Airlines and American Airlines. It is the first of six pilot tests scheduled around the world to prove out the new CUPPS technology. A total of six airlines, six airports, and six platform suppliers are participating.

CUPPS distinguishes itself by allowing airline check-in applications to be fully portable, potentially saving individual airlines hundreds of thousands of dollars a year in reduced development and support costs. It can bring further savings to both airports and carriers through more efficient printing of boarding passes and baggage tags.

The CUPPS Technical Specification was published in 2008 after a collaborative effort between ARINC, IATA, the ATA and ACI. At Las Vegas McCarran the CUPPS team is led by Samuel Ingalls, the airport's Assistant Director of Aviation, Information Systems.

"CUPPS is a much-needed worldwide effort to replace the CUTE technology that has served airports and airlines very well for over 30 years," stated Ingalls. "We are very pleased with the first results from our CUPPS pilot test. Las Vegas McCarran continues to champion and embrace innovative technology that brings significant improvements in functionality, coupled with cost reductions for all stakeholders."

Common-use systems allow multiple airlines to share the same computer systems at airport check-in desks and boarding gates. The previous generation of common-use check-in systems—known as CUTE—lacked the detailed technical specifications in CUPPS that assure interoperability and portability.

For more on the CUPPS initiative please see the Q&A with Samuel Ingalls on page 20, immediately following this article. ■



The baggage area at Las Vegas McCarran International Airport. Passengers bound from Las Vegas to Calgary, Canada on WestJet Airlines (inset) were successfully checked in using new industry-standard CUPPS technology. The McCarran trial was the first of six CUPPS tests scheduled this year at airports around the world, five of which have now commenced.

A platform for the future

Q&A on the new CUPPS technology and Standard with Samuel Ingalls



Samuel G. Ingalls (A.A.E.) has been with the administration at McCarran International Airport for the past 16 years, serving in a variety of areas, including governmental affairs, planning and business administration. He has led the airport's information systems group for the past four years. His efforts in information systems for McCarran pre-date that time period, however, as he played a leading role in ushering in common use systems airport wide in the mid-1990s. In recognition of the success of that project, Ingalls was named a 1998 Computerworld–Smithsonian Laureate for technological innovation in the transportation industry.

Ingalls is immediate past-chair of the Business Information Technology Committee for Airports Council International. He writes frequently and speaks around the world on airport information systems issues, working closely with both airports and airlines on such matters. He is also a frequent user of the airport system on a personal basis, holding a commercial multi-engine pilot's rating.

What were the primary shortcomings of the former CUTE technology that helped instigate the CUPPS initiative?

CUPPS has been designed as a platform for the future, able to accommodate many things even beyond the agent-facing applications that it will initially address.

The biggest benefit will be that one air carrier application will be able to run anywhere on any CUPPS provider's platform. That has been the key foundational principle throughout the course of the initiative.

The issue currently is that many different companies are providing differing types of platforms and implementations, requiring the carriers to maintain (in some cases) as many as six different applications, including their own proprietary application. It can be a rather daunting task for them to update these many applications as their business demands change and/or as security changes or other changes occur in their respective operating environs.

I liken this to the rather public standards fights that we are all familiar with. Going back a couple of decades, it was the Beta vs. VHS fight, eventually won by VHS. More recently, it was the BlueRay vs. HD-DVD face-off. By all accounts, the lack of a standard greatly inhibited public acceptance and uptake of high-definition DVDs. When I play a movie, I don't want to have to think about whether I have the right manufacturer's player. I want to put the DVD in and sit back to relax and enjoy the movie.

In somewhat similar fashion, air carriers should be able to easily port their application from one venue to another, not having to consider the peculiarities of a specific vendor's platform in a particular airport. The efficiencies and cost savings of being able to accomplish that should be of significant benefit to the industry.

Have all the CUPPS tests concluded thus far returned positive results?

CUPPS is currently in the pilot phase of the initiative. The pilot phase is divided into four segments: the technical trials (now ongoing), the compliance trials, the specification update, and the specification release. While the technical trials are ongoing we are defining the compliance trial parameters as well as updating the technical specification with lessons learned. We're also addressing any errors and omissions so that the time required for executing the specification update segment can be minimized.

There are currently four active trials in progress: Las Vegas (ARINC); Orlando (SITA); Dublin (Ultra); and Brussels (RESA). The fifth trial is currently not active—Sacramento. While the actual execution of the trials has changed over time due to installation and site-specific needs, the overall progress is proceeding as planned. Our original goal was to have the technical trials completed by April 15, 2009, but we learned through the pilot process that the critical milestone in the schedule is the publication of the Technical Specification. Each of the four trials is progressing with different tasks, in different orders, based on the participants' views and needs, and therefore they are completing the trial milestones in different orders. This flexibility has allowed us to learn more in a shorter timeframe, as well as giving everyone the freedom to complete their tasks in a manner that is comfortable for them.

In Las Vegas, tens of thousands of passengers have been checked in and are now being boarded on a CUPPS platform and application. The system has worked virtually flawlessly to date.

“ ICAO Standards play a foundational role in everything that is aviation-related in the world. CUPPS has been no exception. A close look at the reference section of the CUPPS documentation shows that many different organization’s standards have been utilized in developing the standard, such as IEEE, ISO, AEA, IATA and ATA. But, of course, the ICAO Standard on Machine Readable Travel Documents (MRTD), Document 9303, was also an important document relative to the CUPPS recommended practice.”



Some of the lessons learned thus far include:

1. The importance of independent compliance testing.
2. Identifying achievable milestones.
3. The skills required to manage a project which spans multiple organizations, companies and backgrounds.

The International Air Transport Association (IATA), the Air Transport Association (ATA) and Airports Council International (ACI) all played a role in developing the new CUPPS standard. Briefly outline the timeline and process that helped these stakeholders to succeed at this undertaking, providing credit where due to any exceptional contributions to the process.

The CUPPS standard represents the first time that a recommended practice has been jointly owned by both airports and air carriers. It has consequently been approved by all three of the organizations you mention: IATA (RP 1797); the ATA (RP 30.201); and ACI (RP 500A07).

CUPPS AND AIDX

The new CUPPS technology employs an additional innovation by making use of Aviation Information Data Exchange (AIDX). Like CUPPS, AIDX evolved out of conclusions from the “Seattle Summit” meeting in 2003, a gathering of airports and air carriers looking for ways to cooperate and drive economic efficiency.

AIDX provides a way for aviation stakeholders to easily communicate data in a standardized fashion. In its initial implementation, AIDX provides a very simplified way to transmit real-time flight data to Flight Information Display Systems (FIDS). Rather than having to develop and maintain customized interfaces with various systems (or have none at all), an air carrier can easily communicate to AIDX-based systems worldwide.

More than mere theory, AIDX is up and running at both the Denver and Las Vegas airports, with other facilities around the world scheduled to come online shortly.

The CUPPS initiative grew out of a gathering of air carriers and airports in 2003, called the “Seattle Summit,” which looked for ways that the two industry groups could work together to achieve economic efficiency. The project received official approval to move forward towards recommended practice development on the IATA and ATA sides at the Joint Passenger Service Conference in 2004. I was elected to chair that effort, with co-vice-chairs, Bill Heppner from Alaska Airlines and Thomas Jeske from Lufthansa Airlines.

The four plus years have been very busy ones for the group, which has grown steadily in size. It now numbers more than 100 companies, from many varied industry segments, in addition to air carriers and airports. The team that comprises the CUPPS group has produced a recommended practice and associated Technical Requirements and Technical Specification documentation. It is this documentation on which the platforms and applications have been coded and are now under test in the pilot trials.

The organizations have all been very actively involved and supportive of the initiative. The fact is that CUPPS will bring significant business benefit to the industry, on a worldwide basis.

What role do the applicable ICAO Standards play in supporting the development of the CUPPS technology and functionality?

ICAO Standards play a foundational role in everything that is aviation-related in the world. CUPPS has been no exception. A close look at the reference section of the CUPPS documentation shows that many different organization’s standards have been utilized in developing the standard, such as IEEE, ISO, AEA, IATA and ATA. But, of course, the ICAO Standard on Machine Readable Travel Documents (MRTD), Document 9303, was also an important document relative to the CUPPS recommended practice. ■



Issuance and security: The Republic of Korea solution

The Republic of Korea launched its new electronic passport in August of last year, with plans and capacity now in place to personalize and issue more than 6 million new ePassports per year as its programme moves forward.

Due to security concerns, the government of the Republic of Korea decided to centralize the personalization and issuance of its new ePassport rather than establishing decentralized instant issuing. For this reason the state owned Korea Minting and Security Printing Corporation (KOMSCO) was awarded the new ePassport issuing responsibility.

In the programme's early stages the new Republic of Korea ePassport will store only citizen data and a facial image on the chip, but as of 2010 Korea is also considering the addition of a fingerprint biometric.

KOMSCO was given a very short time frame to migrate the Republic of Korea issuance system from instant to central processing. The project commenced in April, 2007, meaning that stages relating to the design, construction and installation of the new issuance equipment were all accomplished in just 16 months.

KOMSCO will continue to make use of existing desktop personalization systems to print and encode the new Republic of Korea passport. For verification, sorting and packaging, KOMSCO has partnered with the firm Otto Kuennecke in Germany. The challenge for the German partner was to develop a solution for the specific requirements of KOMSCO.

Upon personalization, the Republic of Korea ePassports are sent to 250 different travel document registration offices all over the country. Some offices receive up to 1,000 passports a day while others, especially in rural areas, have much smaller administrative requirements. The challenge was to develop an automated system which could verify, sort, group and package the passports according to their final location. An additional challenge in this regard arose from the fact that the passports cannot be personalized in sequence in order for a sorting machine to sort the incoming passports to the final locations. With daily amounts of up to 20,000 passports being issued, the early challenges for the new system were formidable.

The vendor responded by developing and installing three different machines as well as software to control and monitor the aggregate process. The verification system feeds the passports automatically and opens the holder page which is—in the case of the Republic of Korea document—the second page. After verification of the passport personal data, an online connection to the Foreign Ministry transmits the final packaging information. The system is designed to be upgraded with additional features such as photo, UV and chip verification which will be installed during a second phase. Other data received from KOMSCO's internal network and the Foreign Ministry is used to print a label with Korean characters on the back cover of the ePassport.

The document sorting process includes a sorting machine equipped with 50 removable magazines which can each represent unique registration office locations. These magazines can store up to 200 documents and when a given location requires more than this maximum the system automatically adjusts to employ multiple magazines until that office's documents have been completed. The process is fully monitored and the magazines can be equipped with RFID chips for tracking through subsequent sorting and transport processes.

After sorting, the passports are fed into the packaging system where each document's barcode is read. A turning unit then automatically turns the passport to avoid tangential deviation in the assembling station. After every five passports the direction is changed. In the following assembling station groups of 2-to-50 passports can be created depending on their final destination.

After grouping, the passports are transported to the banding stations where they are cross-banded. A label printer prints a label with the final information of destination and the number of passports grouped in the stack. If a group is not complete the entire group is automatically rejected. Audit files monitor the complete run of each passport in each group. The entire system is able to process more than 4,000 passports per hour. ■



Fingerprint capture and the German Experience

Germany is the first EU State to introduce secondary biometrics into ePassports as required by the European Commission. The following presentation, submitted to the 2008 ICAO MRTD Symposium by Dr. Uwe Seidel, Senior Scientist, Forensic Science Institute, Identity, Documents, Bundeskriminalamt, Germany, reports on the preparation, experience and results achieved so far in more than 5,000 offices across Germany.

Dr. Uwe Seidel is the Senior Scientific Officer at the Forensic Institute of the Federal Criminal Police Office of Germany (Bundeskriminalamt or BKA). He has a PhD in experimental physics and optics from the University of Jena and worked for a leading photographic imaging company in quality assurance and research and development before joining the BKA in 2000. Dr. Seidel is an expert in forensic document examination and in the development of security documents. He is an active member of the ICAO New Technologies Working Group and has made considerable contributions to the development of the biometric passport.

The German ePassport system went live on November 1, 2005, in what became the first generation of electronic Machine Readable Travel Documents (eMRTDs). They were ICAO-compliant, complete with a facial image, personal data and a Radio Frequency (RF) chip. This primary biometric system was

the precursor to a secondary phase which was introduced in November 2007.

This second generation document now includes a fingerprint biometric. European Union Member States were required to have fingerprint biometrics included in their ePassports as of the summer of 2008. Germany was the first to meet this deadline and as of the end of 2008 it had issued a combined total of 7 million ePassports, of which 2.5 million are second generation.

There are a number of passport regulations detailed in the German law that all of the 5,300 passport offices in my country must follow when collecting facial image data and fingerprint data. Let me give you a quick overview of the quality assurance process that is involved here.

In Germany, people usually go to a photographer to have their passport photos taken. Once they have their photo, they take it to the local issuance office in their municipality, where it is checked visually based on ICAO guidelines. The offices have a template that can be placed over the photo to verify its validity. If the image meets the appropriate specifications an official will scan the photo. If the numerous ICAO parameters are not met, the official can send the customer back to have another taken.

The customer, of course, returns to the photographer and blames them for not meeting the standards. Thus far we've had quite a number of complaints due to potential registrants being made to go back and forth to their photographers. This is simply an issue we must face with registering facial images.

When the submitted photo is compliant, it is sent to the document producer electronically. Germany is, due to privacy regulations, one of the few countries without a central passport database.

We are probably one of the very few countries, however, that does have a quality assurance statistical database where we store neither the images nor the fingerprints, but rather the data associated with the quality of all images submitted. With this tool we can determine the quality of the facial images and fingerprints submitted on an office-by-office basis.

For fingerprint enrollment, we have what is known as "live enrollment." Obviously there's no point in having fingerprints taken somewhere else and then brought back to the municipality office and scanned. Instead we have live enrollment on-site and quality standards for fingerprints that are captured.

We have had some interesting experiences with facial image quality assurance. According to an International Organization for Standardization (ISO) regulation, the quality information of each image should appear on a passport and even in the chip. Germany's experience was such that we were supported by

As individual as your identity

Secure identification systems from Giesecke & Devrient.

G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport systems, ID card solutions and have become a trusted adviser and supplier to governments.

We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. Giesecke & Devrient will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards.

ID system implementation by G&D – individual, international and secure.

Creating Confidence.



Giesecke & Devrient

www.gi-de.com

Prinzregentenstrasse 159 - P.O. Box 80 07 29
81607 Munich, GERMANY
Phone +49 89 41 19-18 37
Fax +49 89 41 19-27 78
government@gi-de.com



some other States, and this cooperation led to some modifications of the Standards. ICAO and the ISO have since relaxed a few of those parameters in order to make it easier for municipalities and enrollment offices to meet the new Standards.

By July 1, 2008, ISO published what they call a Technical Corrigendum, in which all the changes just discussed were incorporated. This is the final regulation that must be obeyed and the final step to qualify an image as compliant. The process is easier now than it was before, but we still have a few issues in Germany with our facial image enrollment. We're continuing to make some improvements with a new graphical user interface and we want to get rid of the acetate sheet; the photo template. We would like to have some interactive controls and, of course, we had to introduce parameters for children.

We changed completely the software engine for the quality assurance algorithm and we added some additional parameters. We're piloting this programme right now in a few municipalities and hopefully we'll roll it out later in 2008.

Overview of 2008 German biometric capture systems

If you scan an image and it is ICAO-compliant, the officer will see a green frame around the image. If it's not compliant, the officer will see some shaded areas on the image. There is some tolerance for certain areas of the image that is allowed by ICAO. A yellow frame will appear if the positioning of the face on the image is problematic. The software will tell you in great detail (in German of course) what the problem is.

For instance, the eyes can be 16 degrees beyond the defined area where the parameters allow them to be. A slight variance of up to five degrees is acceptable. The rules change for children as they are typically more tolerant of variances. The software also works with many geometric parameters, photographic requirements such as exposure, sharpness, and additionally digital parameters like the colour scheme you're operating in.

Compared to facial image capture, fingerprint capture is quite different because only digital/live enrollment is possible. As I explained earlier, you cannot send somebody to have his fingers inked and rolled at one location, and then scanned at another. More importantly, a visual inspection is simply not feasible. An official in a municipality office can easily tell if a photo is good or bad—it's sharp, the head size is approximately correct—but nobody, at least not in German municipality offices, can tell if a fingerprint is valid.

As there are very few fingerprint experts in our offices, the software has to do the job. The most important point is that, unlike the face, where you can have a photo of anybody taken at any time, fingerprint enrollment is always subject to possible failure. There is a certain percentage of people you cannot enroll and you have to deal with the exceptions. About 80 percent of all the time we have spent discussing our laws and regulations thus far has been with these exceptions.

So who then **is** permitted to have a German passport without fingerprints and under what circumstances is that allowable? There is still no standard available on high quality fingerprint enrollment and we have also faced difficulties because certified hardware is only available for four-finger scanners. The Federal Bureau of Investigation (FBI) maintains a list of certified hardware for fingerprint scanners, but only for the rather expensive four-finger variety. Germany needed reliable single-finger scanners.

Another, less obvious problem is detecting the authenticity of a finger. People are not very aware that this can happen, but if somebody shows up at the municipal passport office with a silicone finger there is no technology available at the moment to detect it. There is, however, research being done at the moment to produce hardware which can detect—without any negative side-effects—if the finger is genuine or not.

Another issue is that there is currently no programme to record what reference measure was used at time of fingerprint capture; never mind what the algorithm or thresholds were. It is impossible to say at this point what sort of verification device a German traveller, especially after they've had their passport for a

number of years, will come into contact with at a receiving State's border.

All we could do was to capture our fingerprints to the best of our ability for use throughout Europe and, of course, the rest of the world based on current specifications and capabilities. We decided to take existing FBI standards and created our own national certification scheme, involving a physics lab doing all of the optical measurements on the sensors.

There are the two sensors which are currently in use in German municipalities. We employ a very German approach, where everything is explained in the regulations and in compliance with EU requirements. The process works as follows: the index finger is scanned first. If the scan is not good enough, we will take the thumb, then the middle finger and, finally, the ring finger. Never the baby finger. There is a mandatory process whereby you have to attempt at least two fingers before moving on.

There is a special process used when we enroll each finger. We capture three images of each individual finger and from these three images we then select the best one by matching them against the others. The image which receives the highest match score against the other two is the print/finger that is ultimately selected.

In practice, the process we follow in all the municipality offices is as follows: You are told to start with the right hand and index fingers. You place your finger on the pad; it has real-time quality measurement capabilities. If it is good enough, you pick your finger up and repeat the process a second and third time. It matches each finger image against the other, to ensure I haven't switched fingers and then images of the left hand index finger are taken.

Now, from all of those images, the best two are selected; one from either hand. There is a quality threshold, a quality value and a match score that was achieved with the other two fingerprints. The quality score is stored in the passport in order to show the receiving State what the quality of the fingerprint was at the time of enrollment.

It's possible for the situation to arise whereby you end up having a 50-year-old construction worker, who has been bricklaying for 30 years, and who now shows up to have his fingerprint captured for his brand new ePassport. After you've tried two of his fingers and they still will not scan properly, the bricklayer is then released from requiring fingerprint enrollment. We would, however, store a fingerprint even if it has not met our quality requirements, simply choosing to store the best of the bad fingerprints captured.



Standing guard. Entrust ePassport security solutions are the most scalable, interoperable and proven in the world.

As the global PKI leader, Entrust provides trusted security solutions for first-generation (BAC) & second-generation (EAC) ePassport environments. In fact, Entrust is the No. 1 provider of ePassport security solutions and is leading the migration to the EAC standard.

No matter if you're just beginning development or evolving your ePassport strategy, Entrust is the choice for ePassport security.

Visit entrust.com/epassport

Entrust[®] Securing Digital Identities & Information

“ We have many critics saying that our final concept, with three images per finger, is time-consuming, to say the least. But has it been successful or not? The first image captured does not tend to be of good quality, because people are not really used to putting their fingers on sensors. Our data reveals that the first image was captured successfully only 15 percent of the time. With repetition you would think that the third image would tend to be the best one, but that’s not the case. Surprisingly, in about 50 percent of the cases, the second image was used and the third image was used just 33 percent of the time. In general, we can say that our concept of using the three images has been pretty successful and we will keep using this system.”



With the second generation fingerprint system we of course carried out some pilot testing. To highlight the funny situation we had to deal with, our 5,300 municipal offices were served by no less than 14 independent software vendors running all kinds of different software.

If you had a German electronic passport issued before November 1, 2007, it was a first generation model and every single passport issued beyond that date has been of the second, biometric generation. Timing was of major concern. From the time an applicant says, 'hello' to the time they say 'goodbye,' it is eight minutes. Of course, it varies. We had an interesting case of an old gentleman who voluntarily took part in our procedures and after 12 minutes finally let the officials know that he just wanted to register his dog and pay the taxes for it. He left without giving us any fingerprints and this kind of thing has simply been known to happen.

I'm very lucky (or unlucky, depending on how you view the matter) to have rather good fingerprints. It usually takes about two and a half minutes maximum in the municipality office to enroll my fingerprints; a couple of seconds, at minimum. An interesting point to note after having described what our process is like, is that various things are done throughout the process and time is not the main concern. Quality is all-important and the question we ask ourselves at the end of the procedure is, 'did it all work out?'

What exactly is inside German passports? What is the quality? For those answers, we have a central Q&A repository, and I've done some number-crunching over recent months.

Germany has between 200,000 and 230,000 applications per month and they come out of about 5,500 municipalities (according to July 2008 statistics). Among these are some overseas applications. An interesting question is, 'what did we enroll?' How many fingerprints do we have and are there passports that contain no fingerprints at all?

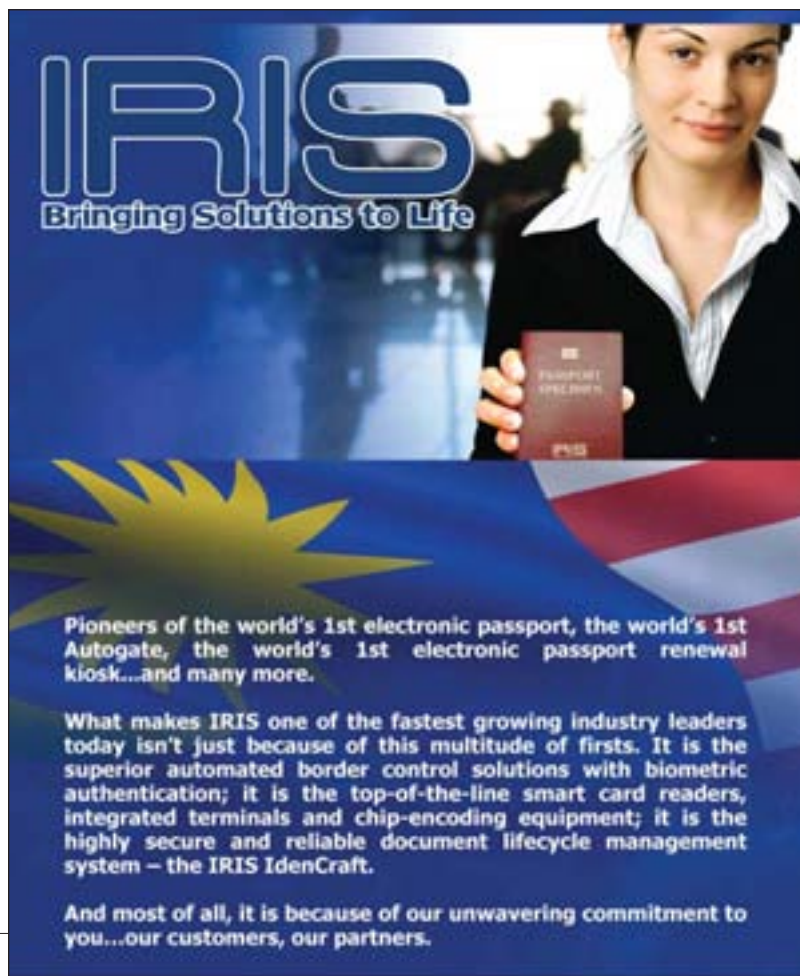
Throughout the three month sample period, 99 percent of passports had a photograph and two fingerprints which were above the quality threshold. This is good news because it is an ICAO requirement. 0.1 percent were issued with only a photograph of the face. For various reasons, some people were not able to enroll their fingerprints. They may not have hands, their fingerprints could not be properly read by the scanner, or people in the municipality office simply gave up—any reason is possible.

Some passports were issued with a headshot and only one fingerprint; this can also happen for the same reasons. Some have a picture and two fingerprints, but the fingerprints are below the quality threshold; they were nonetheless included in the passport.

The next interesting question is what fingers are included in German ePassports (that's if they still have their fingers after they've finish our process). EU regulations make it mandatory, where possible, to use index fingers. The good news is that 97 or 98 percent during this three-month period examined used their index fingers.

The next concern is the thumbs. We usually see index-index combinations and, failing that, a thumb-index combination. If the index finger does not produce a good scan, you have to use the thumb, and then from there to the middle fingers. All this adds to the enrollment time. But if 90 percent of the passports have successfully enrolled the index finger, we can, in most of the cases, shorten our enrollment time.

We have many critics saying that our final concept, with three images per finger, is time-consuming, to say the least. But has it been successful or not? The first image captured does not tend to be of good quality, because people are not really used to putting their fingers on sensors. Our data reveals that the first image was captured successfully only 15 percent of the time. With repetition you would think that the third image would tend to be the best one, but that's not the case. Surprisingly, in about 50 percent of the cases, the second image was used and the third image was used just 33 percent of the time.



IRIS
Bringing Solutions to Life

Pioneers of the world's 1st electronic passport, the world's 1st Autogate, the world's 1st electronic passport renewal kiosk...and many more.

What makes IRIS one of the fastest growing industry leaders today isn't just because of this multitude of firsts. It is the superior automated border control solutions with biometric authentication; it is the top-of-the-line smart card readers, integrated terminals and chip-encoding equipment; it is the highly secure and reliable document lifecycle management system – the IRIS IdenCraft.

And most of all, it is because of our unwavering commitment to you...our customers, our partners.



“Compared to facial image capture, fingerprint capture is quite different because only digital/live enrollment is possible. You cannot send somebody to have his fingers inked and rolled at one location, and then scanned at another. More importantly, a visual inspection is simply not feasible. An official in a municipality office can easily tell if a photo is good or bad—it’s sharp, the head size is approximately correct—but nobody, at least not in German municipality offices, can tell if a fingerprint is valid.”

In general, we can say that our concept of using the three images has been pretty successful and we will keep using this system.

Finally then the most important question of all: What is the quality of the fingerprints used in German electronic passports?

There is no real standard, no ISO standard, for fingerprint image quality, but there is the factor standard which is the Missed Fingerprint Image Quality (MFIQ) metric. It has just five levels and we scaled it to 100, 75, 50, and so on. About 75 percent of all fingerprints in German databases, representing about 600,000 passports, are of the best quality level. About 15 percent fall under the second-highest ranking. Therefore about 90 percent of all German ePassports have the MFIQ level one or two, which is rather good.

On the other hand, we have two percent that fall under level four or five, which represents poor quality images. The hope is that people will have a look at the quality indicator. If there is a low grade scored by German authorities, it is explainable because the image captured at enrollment was sub-par. This is not monitored, but it may be something that needs to be taken into consideration once people begin verifying fingerprints at borders.

The enrollment of biometric features on a large scale requires constant diligence. We still have standards that need to be modified. Hopefully, this kind of software enhancement will be initiated by Germany and other countries. The fingerprint enrollment, at least for us and, I would suspect, for everybody else, creates unknown challenges—especially for the municipalities involved with the procedure.

I will not elaborate on the extended access control infrastructure; that is another subject entirely. Pilot testing is very important, as is education and training. We have given our municipalities support by providing them with instructional movies, brochures and a Web site, including an FAQ page. As I have demonstrated, we have a rather quality-centred enrollment process. We’ve allowed a few compromises for faster handling, but only a few.

As the first results from the central repository reveal, at least in my opinion, this strategy looks to have been a success. As always, however, there is continued room for improvement. ■

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.

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.”

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.

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 appearance 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.

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.

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.

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 centres 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. ■

2009 ICAO CALENDAR OF EVENTS

	Title	Location	Date
EAD	Traffic Forecasting Group	Nairobi/Africa	September
EAD	Forecasting Workshop	Nairobi/Africa	September
EAD	Statistical Workshop	Nairobi/Africa	September
EAD	Global Conference on Crisis Impact	Montreal	Sep/Oct
ATB	ICAO-World Bank Symposium	Beijing	14-15 September
EPM	ICAN2009		Sep/Oct
EPM	Joint AEP/ANSEP Meeting	Montreal	November
EAD	CNS/ATM Business Case Workshop	TBD	TBD
EAD	Forecasting Workshop	Africa	TBD
SFP	Immigration Seminar on API, PNR, Chapter 5 of Annex 9	Singapore	4th quarter
ISFP	ICAO-OAS CICTE Workshop on MRTDs and Biometric Identification	Caribbean – RD Mexico suggests Trinidad	
EPM	Post CEANS Joint ICAO/AFCAC Symposium	Africa	TBD
ENV	ENV Workshop	Dominican Republic	TBD
ENV	ENV Workshop	Singapore	TBD
EAD	Forecasting and Statistics Workshop	TBD	TBD
SFP	Conference on Roadmap for Aviation Security	AFI Region	TBD
SFP	Workshop on Liquids, Aerosols and Gels (LAGS)	AFI Region	TBD
SFP	Workshop for the Aviation Security Points of Contacts	AFI Region	TBD

2010 ICAO CALENDAR OF EVENTS

	Title	Location	Date
	Airport and Air Navigation Services Economics Workshop	MID Region	TBD
	ICAN2010	CAR Region	TBD
	ICAO/ACI training course on airport charges	CAR Region	TBD
	NAM/CAR/SAM on Environment	CAR Region	TBD



Who is 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 21 national ePassport programs worldwide including Côte d'Ivoire, Estonia, Denmark, France, India (diplomatic), Norway, Poland, Portugal, Qatar, Singapore, Slovenia, Sweden and the United States of America.

Now you know who's behind.

* 2.6 seconds for a full EAC transaction with 48 KB of data, RSA 1024 and extended length (EAC tests in September 2008)



www.gemalto.com

gemalto[★]
security to be free

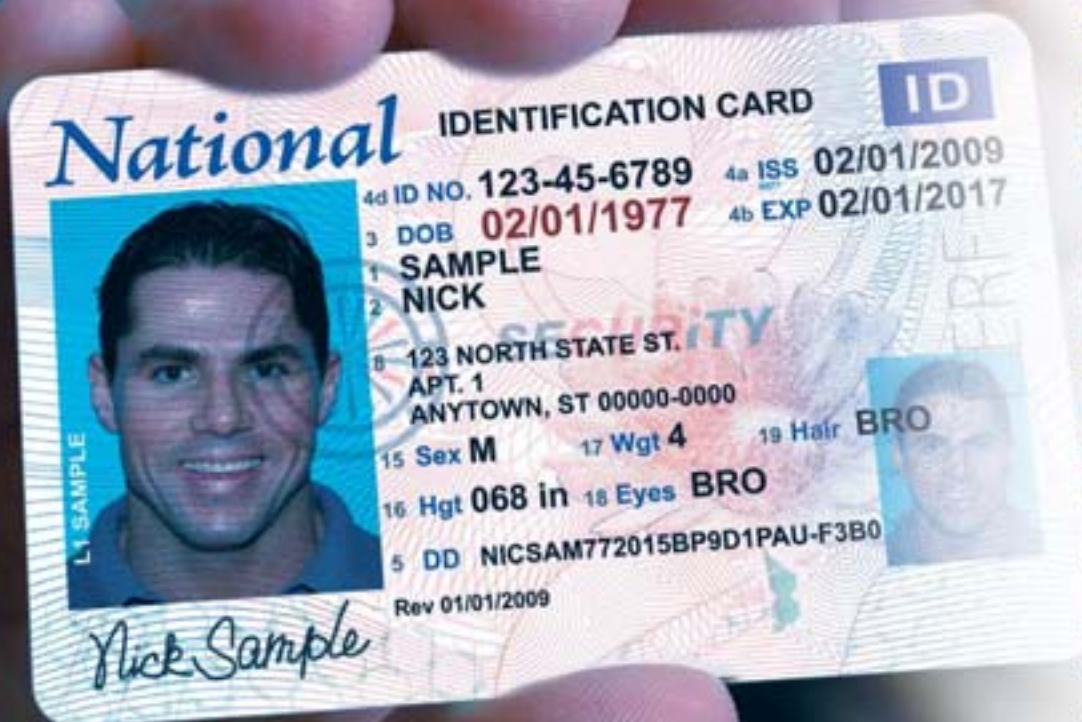
Better Identity Management for a Safer and More **Secure** Aviation Industry

Ensuring that travelers are who they claim to be, and assuring the legitimacy of credentials presented at ticket counters and border crossings as proof of identity, is no longer an issue of national concern. It is a matter of global security affecting the entire aviation industry. Federal agencies and international governments depend on L-1 Identity Solutions to help them protect citizens against crime perpetrated by fraudulent identities.

L-1 identity Solutions produces millions of secure government-issued IDs each year, including ID solutions for more than 20 countries. Our solutions and services for the aviation industry include:

- Credential and Passport Book Production
- Document Authentication
- Enrollment Services
- Knowledge Testing
- Multi-Biometric Identification
- Verification Applications

L-1 solutions are modular and can be used alone or together to form a complete identity management system. Visit us online to find out more: www.L1id.com.



Visit us at the 2009 ICAO Tradeshow.

Protecting and Securing Personal Identities and Assets

BIOMETRICS • SECURE CREDENTIALING • ENTERPRISE ACCESS SOLUTIONS
ENROLLMENT SERVICES • GOVERNMENT CONSULTING SERVICES

L-1
IDENTITY
SOLUTIONS™

SECURE CREDENTIALING DIVISION

978-932-2200 / info@L1ID.com