ICAO MRTD REPORT

VOLUME 1 / NUMBER 1

OPTIMIZING SECURITY AND EFFICIENCY
THROUGH ENHANCED ID TECHNOLOGY

INAUGURAL ISSUE

SECURE PASSPORTS FROM DE LA RUE

DE LA RUE IDENTITY SYSTEMS

Complete solutions to design, produce, personalise and program passports, conforming to all the recommendations of ICAO, the European Union and the US visa waiver programme.

If you would like to receive a copy of our 'Secure Passports' brochure then please call +44 (0)1256 605259, or send an email to Jonathon.Inskip@uk.delarue.com

A trusted partner in major projects worldwide

DeLaRue

ICAO MRTD Report

Vol. 1, No. 1, 2006

Editor: Mary McMunn

Content Coordinator: Mauricio Siciliano

Graphic Art Design: Sylvie Schoufs,
FCM Communications Inc.

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

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

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

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

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

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

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

Table of contents

Editor's welcome

Dear Reader,

This new journal was developed in ICAO to serve the broad spectrum of persons in government agencies, industry and the public who are interested in our work in machine readable travel document specifications and related technology. In this publication you will find articles elaborating on ICAO standards and MRTD related technology. You will also find information about our programmes, the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), States' experiences in implementing MRTDs, and information on the publications and guidance material developed by ICAO with the assistance of the TAG/MRTD.

The journal will be published at least twice a year, and an index of the articles published in every issue will be printed once a year. We encourage readers to build a collection of issues for future reference.

Thank you for reading the MRTD Report; we hope you find it interesting. Let us know if you have any comments on the content or suggestions for what you might like to see in future issues.

Mary K. McMunn

Top of its class in official interoperability tests

ACG readers feature:

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

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

Benchmark performance

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

ACG readers offer you:

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

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

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

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

ACG id

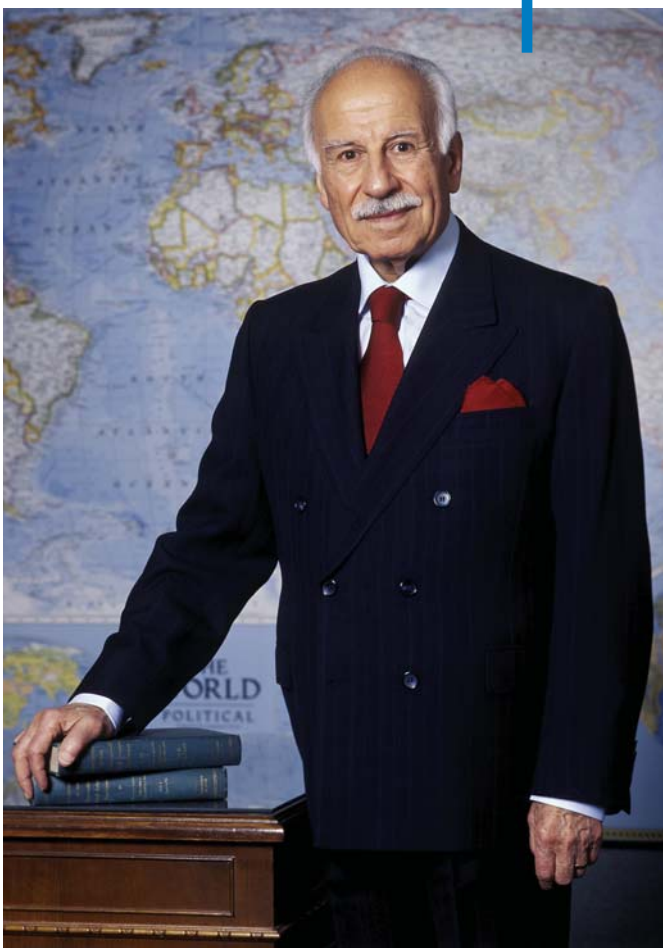
Advertising in ICAO Publications positions you worldwide.

For further advertising information,
please contact us.

FCM Communications Inc.
835 Montarville St.
Longueuil, Québec
Canada J4H 2M5

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

Message from the President of the Council, Dr. Assad Kotaite



Last year, the airlines of ICAO Contracting States carried a record 2 billion passengers on their scheduled services. Eliminating congestion at departure and arrival control points is essential to efficient air travel and to the security of the global air transport system.

Over the years, the ICAO Council adopted measures to facilitate the inspection and clearance of persons – measures that are effective, internationally coordinated, and applied with the greatest possible consideration for passenger convenience and efficiency, while remaining mindful of privacy considerations.

A key to smoother departure processing and border control is strict adherence to standards using modern technologies. Under the leadership of ICAO, much progress has been achieved over more than two decades in the development of specifications for Machine Readable Travel Documents (MRTDs) and biometric identification.

In 2005, ICAO adopted a new standard that all Contracting States begin to issue only ICAO-standard machine readable passports (MRPs), no later than 1 April 2010. Some 110 States currently do so, and ICAO offers technical assistance to those States that need it to meet the new objective.

ICAO has always worked from the premise that global cooperation is the only solution to the many challenges faced by society. The Council and the Assembly it represents have placed a high priority on our work on MRTDs and related systems. This journal is a significant step to increase the world's understanding of the standards we have developed for the international travel system.

MRTDs: Status of the ICAO Standards

Annex 9 to the Convention on International Civil Aviation - *Facilitation* 3.10 Contracting States shall begin issuing only Machine Readable Passports in accordance with the specifications of Doc 9303, Part 1, no later than 1 April 2010. 3.10.1 For passports issued after 24 November 2005 and which are not machine readable, Contracting States shall ensure the expiration date falls before 24 November 2015.	Twelfth Edition, July 2005.
Doc 9303, Part 1 - Machine Readable Passports Vol. I - conventional MRP Vol. I and II - ePassport	Sixth Edition (in 2 volumes) to be published 1st Quarter 2006.
Doc 9303, Part 2 - Machine Readable Visas	Third Edition, 2005 eVisas are under study.
Doc 9303, Part 3 - Size 1 and Size 2 Machine Readable Official Travel Documents	Second Edition, 2002 Third Edition (in 2 volumes) is under development; expected publication by end of 2006.

Note: Annex 9, Twelfth Edition and current editions of all three parts of Doc 9303 may be ordered online through the ICAO website at www.icao.int, or by e-mail at sales@icao.int.

Message from the Secretary General, Dr. Taïeb Chérif

It is with great pleasure that I introduce the MRTD Report, an innovative communications vehicle by which ICAO intends to share with a broad readership its work on machine readable travel document (MRTD) standards and the knowledge of its expert advisors.

ICAO establishes standards and procedures for application worldwide in a pertinent and practical manner, with input from States, international organizations, and industry. Multinational consensus building is an essential element of this process and helps ensure the harmonized and consistent application of the standards by all States.

In recent years, through such cooperative effort, ICAO has produced detailed specifications for biometric identification in travel documents, known collectively as the "Blueprint". Together with the standards for traditional machine readable passports, the "Blueprint" has become the ICAO standard for "ePassports".

The "Blueprint" was highlighted at the MRTD Symposium hosted by ICAO in the Fall of 2005. This very successful meeting brought together experts from civil aviation administrations, operators and manufacturers in a productive exchange of experiences and lessons learned. The first issues of the MRTD Report will elaborate on some of the themes of this symposium.

The Secretariat of ICAO, along with its Technical Advisory Group, looks forward to working with all partners in achieving a new level of travel document security and global interoperability, to the great benefit of the civil aviation system and the nations of the world that depend on it.

ICAO Hosts Symposium on MRTDs and Biometrics

by ICAO Secretariat

To showcase the work of ICAO and member States to improve the quality and integrity of passports and other travel documents worldwide, ICAO convened a comprehensive Symposium on ICAO-Standard Machine Readable Travel Documents (MRTDs) and Biometric Enhancement at ICAO Headquarters in Montreal on 28-29 September 2005.

Since all of ICAO's 189 Contracting States must issue only ICAO-standard Machine Readable Passports (MRPs) by 1 April 2010, a key objective of the Symposium was to provide participants with an overview of the main elements and benefits of globally interoperable ICAO-Standard MRTDs and the new biometrically-enhanced ePassports. About 110 States currently issue ICAO-Standard MRPs, with more than 40 planning to upgrade to the biometrically-enhanced version by the end of 2006.

Considering that some two billion passengers a year now fly on scheduled air services alone, the comment made by Dr. Assad Kotaite, President of the ICAO Council in his opening remarks to the Symposium is even more pertinent - that it would be an understatement to say that facilitation and security challenges faced by civil aviation today are greater than ever. He added that security remains a top priority, with the universal implementation of MRTDs one of the objectives of the Aviation Security Plan of Action of ICAO.

Dr. Kotaite encouraged all States to issue MRPs, eventually with biometric identity confirmation, and operate reading systems at their border control points. He said ICAO would provide assistance in the form of project planning, technical and policy guidance, arrangements for financing and project management, if requested by an individual State.

Attended by some 300 participants from 58 ICAO member States, eight international organizations and more than 50 companies and institutions, the Symposium featured presentations by experts from ICAO member States, ISO and Interpol. An accompanying exhibition highlighted MRTD-related products and services from prominent companies in this field.

ICAO MRTD Programme

Mary McMunn, Chief of the Facilitation Section at ICAO, moderated the opening session and gave a comprehensive overview of *The ICAO MRTD Doctrine and Progress in Document Security*. This

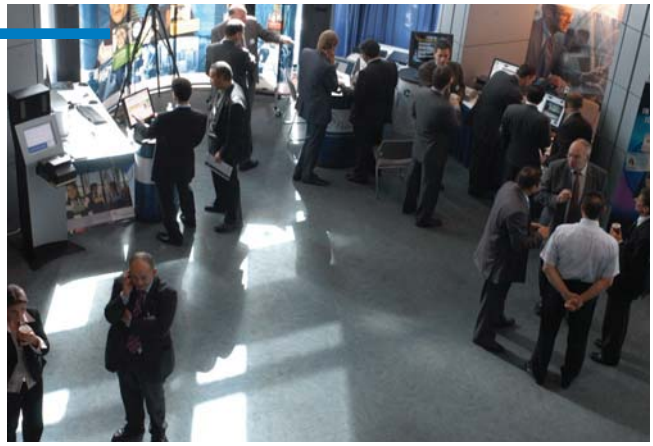
included the legal basis for ICAO's work in travel document security; the framework of standards and recommended practices for border control formalities; the work of the Technical Advisory Group on MRTDs and ISO to develop specifications for travel documents in ICAO Doc 9303 and Technical Reports; and the guidance material and educational events to help member States implement MRTDs and biometrics.

The legal framework includes the 1944 Chicago Convention which created ICAO, its Annex 9 – Facilitation, which addresses customs, immigration and other border control issues and Resolutions of the ICAO Assembly. The sixth edition of Doc 9303, Part 1 on MRPs, which includes specifications on biometric ePassports, is in the final stages of preparation. The specifications can be downloaded from the ICAO website.

Joel Shaw, President and CEO of BioDentity Systems Corp. and an ISO Convenor, outlined the *ICAO/ISO Partnership in the Development and Publication of MRTD Standards*. He said the partnership, which helps facilitate endorsement of the ICAO MRTD specifications as ISO standards, derives its effectiveness from the authority and leadership of ICAO and the standard-setting competency of ISO. He noted that the two organizations have, since the mid-1990s, worked steadily towards an international Standard for a more secure, next generation, biometrically-enhanced MRTD.

Addressing *Basic Principles of MRTDs and Intended Benefits*, Malcolm Cuthbertson, of DeLaRue Identity Systems and ISO, said MRPs must conform to the specifications in ICAO Doc 9303. Developed to enable global interoperability and enhance passenger facilitation and security, MRPs must be of standard size, shape and layout, and contain standard information on the holder and issuing State.

Doc 9303 standards enhance border processing by accommodating both manual and machine-assisted inspection. Containing a visual zone with eye-readable data and a machine-readable zone, the MRP data page is vital to MRP integrity. So is the design. Materials, security features and data storage devices must be selected carefully and brought together in a controlled way so as to create a compatible, complimentary and multi-layered defence against any potential fraud or counterfeiting.



Gary McDonald, Director General, Policy and Planning, Passport Canada, detailed the development of the *ICAO Blueprint for Biometrically Enhanced Passports* and why face was chosen as the globally interoperable biometric for MRTDs, with iris and fingerprint as optional second biometrics. He also reviewed the three other elements: IC Chips for data storage, logical data structure (LDS) for programming the chip, and a security system to ensure data can be confirmed as authentic and unaltered, for which a public key infrastructure is specified.

He emphasized that the focus of the Blueprint was on requirements, which technology solutions were designed to address. Objectives achieved include the use of biometrics to create a strong link between document and bearer, compatibility of biometrics and technology with the issuance and inspection of travel documents, and global interoperability.

Security of MRTDs and use in Border Control

The second session, moderated by Joel Shaw, opened with a joint presentation by Dr. Uwe Seidel, Senior Scientist, Forensic Science Institute,

Bundeskriminalamt, Germany, and Tom Kinneging, of Sdu-Identification and ISO. Titled *Establishing Trust in eMRTDs – Physical and Electronic Security Features and Privacy*, the presentations showed that physical and digital security measures complement each other to form a modern, machine verifiable document that can be trusted by travellers and control authorities alike. Features to protect blank documents from counterfeiting and forgery must be included, and special attention must be given to protect biographical data.

David Philp, Passports Manager, Identity Services, at the New Zealand Department of Internal Affairs, emphasized that the *Issuance of MRTDs* is about more than producing a secure book. It entails an integrated workflow system of phased verification processes, including verification of identity, technology, internal controls and security management. He outlined a thorough step-by-step approach to secure the process of issuance.

Bernard Herdan, Chief Executive, UK Passport Service, stressed the need for a holistic approach in *Securing the Integrity of MRTDs through Identity Authentication*. Noting that a comprehensive approach to document security, application, enrolment and issuance is essential, he placed equal importance on establishing the identity of the person applying for the MRTD and verifying the document presented.

A presentation by Charlie Stevens, Head of the National Fraud Unit, UK Immigration Service titled *Border Control Inspection Enhanced through MRTDs* demonstrated the importance of ICAO-Standard MRTDs for the border crossing process. Calling identifiable and highly secure travel documents vital to processing large numbers of passengers in conditions of high security, he said the new ICAO biometrics standards will be a valuable tool in improving the security of the border control process. He said they offer real, high-value benefits to all citizens in passing through border controls, obtaining visas, making travel arrangements and dealing with airlines.

Concluding the first day's sessions, Joel Shaw gave a summary presentation on *MRTD Programme Features/Benefits to States of Implementation Now*. He referred to the ICAO MRTD programme as more than a set of standardized documents. By specifying technology and recommended procedures to facilitate and make more secure the issuance process, as well as the inspection of persons, and their travel and identity documents, the programme offers numerous and significant benefits to States and society.

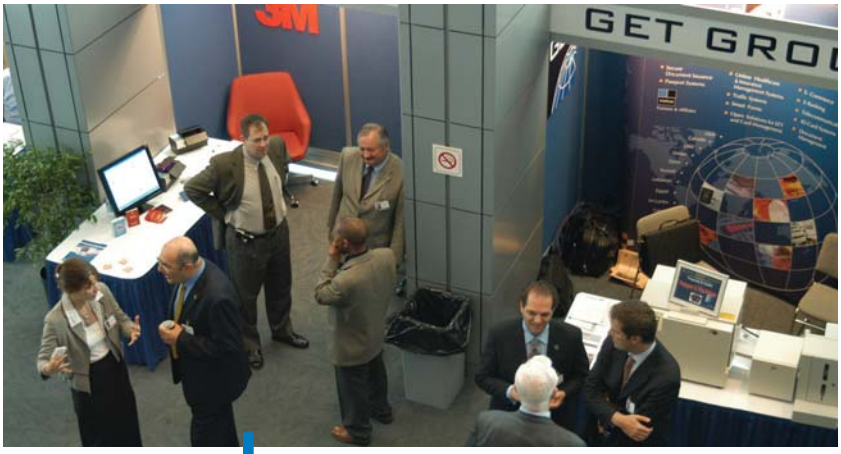
This, he said, is particularly the case with eMRTDS, as they provide an enhanced ability to confirm identity for passport and visa issuance, border controls and airline check-in. He added that impostor detection and interception is another benefit. Stolen blank eMRTDs have no value and are of no use.

He encouraged States to implement either the basic ICAO MRTD or the biometric-enhanced eMRTD now, as both offer much greater levels of security to deal with the threats of identity theft, illegal migration, trafficking/smuggling and terrorism.

Face Biometric, Lost and Stolen Passports, ICAO PKD

Moderated by Sjef Broekhaar, R&D Manager in the Ministry of Interior and Kingdom Relations, Netherlands, the second day's sessions started with a presentation by Terry Hartmann, Director, Secure Identification & Biometrics at UNISYS, and ISO, on *Face Biometric Capture & Processing Systems*. He explained face recognition, how it works, and how it can be effectively used to support document issuance, border control inspection, access control and lookout checks. Because human verification against the photograph is also possible, quality capture of the face is important and quality photographs have to be incorporated in the enrolment process for documents and databases. He added that face recognition is being enhanced through such processes as morphing and 3D facial technology.

A presentation on *Integrated Solutions to Access Interpol Stolen Travel Documents Database* was given by Ivanka Spadina, STD Project Manager at Interpol. She outlined the Interpol worldwide communications system and its application to its Stolen Travel Document Database in serving the needs of its member States on an online, 24-hour basis and playing an important part in document issuance security and border control.



David Clark, a Consultant to ICAO, described the *ICAO Public Key Directory (PKD)*. All public keys and key revocations from issuing States will be available worldwide through the ICAO PKD, with States and airlines able to access the pool of public key certificates and certificate revocations by regular download. The ICAO PKD Operations Office at ICAO Headquarters in Montreal will ensure that the PKD is properly updated. ICAO will also manage the policies, procedures, regulations and fee collection necessary for the PKD. The PKD itself will be maintained securely by the contractor, Netrust Pte Ltd., in Singapore and Thailand.

Sjef Broekhaar concluded the session with a wide-ranging presentation titled *How Does it Come Together in Real Life?* He explained how the MRTD system uses an interlocking, chain-like series of elements to meet government needs for increased security and to bring together all parties involved – issuing authorities, immigration services, police agencies, airport operators, international organizations, and the document industry.

The chain comprises four main processes: new travel documents, application and issuance, management of status of travel documents in circulation, and use of the documents. He said the security of the chain would be greatly enhanced when all States issue only ICAO-Standard MRPs.

John Mercer, retired from the US State Department, served as the moderator for the last session of the Symposium.

Four States gave presentations on their experience with issuing MRPs and e-MRPs. The four—Pakistan (Brig. Saleem Ahmed Moeen, Chairman, National Database and Registration Authority), Antigua and Barbuda (Amb. Colin Murdoch, Ministry of Foreign Affairs), New Zealand (David Philp) and Sweden (Staffan Tilling, Chief Superintendent, Swedish Police)—all emphasized the importance to their States and their citizens of issuing ICAO-Standard MRPs in accordance with Doc 9303 for increased security, global interoperability and acceptance.

The United States presented its experience with the use of MRTDs and biometric identification at airports and other ports of entry. Bradford Wing, Biometrics Systems and Standards Coordinator at the US Department of Homeland Security, highlighted some of the ergonomic factors that will impact on the usability of ePassport readers and ePassports, which have been the subject of intense testing.

In his closing statement to participants, Mohamed Elamiri, Director of the ICAO Air Transport Bureau concluded that the Symposium had been very successful and met its objectives. Given the deadline of 2010 for all member States to begin issuing only ICAO-Standard MRPs and the need for increased security, he said ICAO would aggressively encourage that both these requirements be met. He added that following the success of this Symposium, ICAO is planning to hold a second event in September 2006. ◆

ICAO Doctrine on Travel Documents

by ICAO Secretariat

ICAO's primary purpose is to set standards that enable and maintain a seamless and efficient international civil aviation system worldwide. Security and facilitation of air travel across international borders are two key areas of focus.

In 1968, it was anticipated that the advent of wide-bodied aircraft would lead to a significant and consistent increase in the number of airline passengers worldwide. This would require procedures to process passengers more quickly and more efficiently through customs and immigration. Accordingly, ICAO initiated the development of a standardised passport document that could be read and verified by machine. The first specification was published in 1980.

The ICAO Doctrine on travel documents is based on the Convention on International Civil Aviation of 1944, often referred to as the Chicago Convention, Annex 9 to the Convention, ICAO Assembly Resolution 33-18, ICAO Doc 9303 and the ICAO Blueprint for the implementation of biometric identification. Following is a brief description of each document.

The Chicago Convention

ICAO's mandate to develop standards and specifications stems from the Chicago Convention, which created ICAO and which covers the full range of requirements for the efficient and orderly operation of international civil aviation worldwide, including provisions for clearance of persons through border controls, i.e.:

a) the requirement for persons travelling by air and aircraft crews to comply with immigration, customs and passport regulations (Article 13);

b) the requirement for States to facilitate border clearance formalities and prevent unnecessary delays (Article 22) while establishing customs and immigration procedures that are harmonious with civil aviation (Article 23); and

c) the requirement for States to develop and adopt internationally acceptable standards for immigration and customs clearance (Article 37 (j)).

Annex 9 to the Chicago Convention

A fundamental precept in the development of standards under Annex 9 to the Chicago Convention (Facilitation) is that, if public authorities are to comply with the requirements, they must have confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardized specifications for travel documents aims at ensuring that confidence. Hence *Annex 9* covers such issues as:

- Travel documents, including formats, issuance and control procedures;
- Immigration and customs procedures and systems;
- The prevention and handling of document fraud cases and other security problems.

In particular, the new edition of *Annex 9* (July 2005) includes new issues affecting travel documents, such as:

- Standards on travel documents and security (3.7 and 3.8) ;
- A Standard by which all States shall issue only Machine Readable Passports (MRPs) by 1 April 2010 (3.10) – *see sidebar*;

- A Standard whereby all non-MRPs will expire by 2015 (3.10.1);
- A Recommended Practice that encourages States to incorporate biometric data in their machine readable document, using one or more optional data storage technologies to supplement the machine readable zone (3.9).

Assembly Resolution 33-18

Another legal instrument for establishing standards, specifications and cooperation among States is the Assembly Resolution. Within the framework of the Chicago Convention, the ICAO Assembly – consisting of all 189 Contracting States – meets every three years to provide direction to the Organization's work by way of Resolutions. In 1998, the Assembly passed *Resolution 32-18*, which clearly establishes the wishes of all member States for global cooperation in protecting the security and integrity of passports. The Assembly updated this resolution in 2001 and maintained it in 2004.

Resolution 32-18 reflects the high importance of passport security in our global society, citing premises that:

- the passport is the basic official document which denotes a person's identity and citizenship and provides an assurance for the State of transit or destination that the bearer can return to the State of issuance;
- international confidence in the integrity of the passport is the very essence of the functioning of the international travel system;
- the United Nations General Assembly has requested that ICAO consider ways and means to enhance international cooperation to combat the smuggling of aliens, without undercutting the protection provided by international law to refugees;
- the United Nations General Assembly and the Economic and Social Council have requested that member States establish or improve procedures to permit the ready discovery of false travel documents, to cooperate bilaterally and on a multilateral basis to prevent the use of fraudulent documents, to take measures to provide penalties for the production and distribution of false travel documents and the misuse of international commercial aviation; also,

- a high level of cooperation among States is required in order to strengthen resistance to passport fraud; including the forgery or counterfeiting of passports, the use of forged or counterfeit passports, the use of valid passports by imposters, the misuse of authentic passports by rightful holders, the use of expired or revoked passports, and the use of fraudulently obtained passports.

Therefore, the Resolution urges Contracting States to intensify efforts to safeguard the security and integrity of their passports, to protect them against passport fraud, and to assist one another in these matters.

ICAO Doc 9303

While Annex 9 calls for the standardization of travel documents, ICAO also develops specifications for Machine Readable Travel Documents (MRTDs) to be issued by States. These specifications are contained in ICAO Doc 9303. To help with the development of Doc 9303, ICAO in 1987 created the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), consisting of government representatives as well as observers from the Airports Council International (ACI), the International Air Transport Association (IATA), the International Criminal Police Organization (INTERPOL) and the International Organization for Standardization (ISO).

With the expert assistance of the TAG/MRTD, ICAO structured Doc 9303 for MRTDs in three distinct sections: Passports (Part 1), Visas (Part 2), and Official Travel Documents (Part 3). Official Travel Documents are official documents of identity issued by a State or international organization that may be accepted in lieu of a passport or visa for international travel. These may include national ID cards (e.g. as issued in Europe), air crew member certificates and certificates of identity.

In the first quarter of 2006, ICAO plans to issue a new version of Doc 9303, Part 1 (Passports) consisting of two volumes: Volume I will include specifications for the issuance of MRPs and Volume II will contain the specifications for the enhancement of MRP with biometric data encoded in an integrated circuit chip, thereby making it an ePassport.

ICAO Blueprint for the implementation of biometric identification

Finally, the Air Transport Committee of the ICAO Council in May 2003 adopted a four-part "Blueprint" for incorporating biometrics in travel documents. The Blueprint includes: specifications for the face as the primary biometric, mandatory for global interoperability; the contactless integrated circuit chip as the electronic data storage medium; a logical data structure for programming the chip; and the public key infrastructure to secure the data against unauthorized alteration. These specifications will be elaborated in Volume I of the sixth edition of Doc 9303, Part 1. For more on this subject, please refer to the Article on ePassports.

To sum up, ICAO's role in travel documents is to set standards and establish specifications for implementation by Contracting States in such a way as to foster optimum reliability of travel documents and effectiveness of inspection procedures, in support of a seamless, efficient and secure global infrastructure for processing persons crossing international borders. ◆ MM & MS

Annex 9, twefth edition - 2005
Standard 3.10

Contracting States shall begin issuing only Machine Readable Passports in accordance with the specifications of Doc 9303, Part 1, no later than 1 April 2010.

Note. - This provision does not intend to preclude the issuance of non-machine readable passports or temporary travel documents of limited validity in cases of emergency.

Iris: THE BIOMETRIC OF CHOICE - SPEED, ACCURACY, AND CONVENIENCE

When it comes to operational performance, iris recognition is becoming the biometric of choice. Iris is now utilized in many of the more demanding applications such as country-wide identity management, passports, expedited border passage, facilitated passenger applications, and simplified passenger traveler.

"Increasingly, ICAO members have recognized that iris presents a definitive method for verifying the identity of the person presenting a travel document," says Frank Fitzsimmons President and CEO of Iridian Technologies, the developer of iris recognition. "By incorporating unique iris biometric data into a card or passport, agencies are able to authenticate the identity of the bearer in real time – faster and more conveniently – via iris recognition at the contact point, be it a border crossing, airport, or immigration portal."

SCALABILITY IS KEY

Iridian's small and compact IrisCode® and its standards-compliant highly-scalable architecture make the technology easily supportive of large databases encompassing millions of individual enrollees. Even for the largest populations, highly efficient search and match capabilities allow for two-second identifications under high-traffic field conditions. In deployments such as the United Nations repatriation program at the Afghan border crossings and the United Arab Emirates Immigration and Expellee Tracking Program, iris has effortlessly supported the matching and identification requirements across populations of millions of individuals.

Iridian has extended the range and scalability of iris with the OpenIris® platform, which provides a web-based architecture designed to flexibly support multiple iris recognition locations over broadly dispersed government enterprise systems.

"Iridian's platform allows an authority to deploy an iris-based identity program nationwide," says Fitzsimmons. "Identities can be verified via iris at remote or central locations without compromising the speed or accuracy of the identifications."

When the requirement is for rapid, definitive identifications in real-world conditions, ICAO members are increasingly turning to Iridian iris technologies for trusted biometric solutions.

TAG-MRTD 16th Meeting

by ICAO Secretariat

ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD) held its 16th meeting at ICAO Headquarters in Montreal, Canada, on 26-28 September 2005.

The TAG-MRTD is comprised of government specialists in the issuance of passports and other travel documents, from 13 ICAO member States. It meets approximately every 18 months to review progress of its working groups, and to discuss and vote on proposals from working group and member States.

This year's meeting saw 26 working papers submitted for consideration. High on the agenda was the development of specifications for the Sixth Edition of Doc 9303, Part 1, in its new two-volume format.

Volume 1 of the revised edition will contain the specifications for the basic Machine Readable Passport (MRP), to which all MRPs, be they electronically enabled or not, would have to conform. Volume 2 will contain the additional specifications extracted and edited from the technical reports for enhancing the MRP with biometric identification using a contactless integrated circuit (IC), better known as the ePassport.

Thus Section III covers security matters with appendices on document security, machine-assisted document verification and security of document issuance. All specifications relating to a basic MRP now appear in Section IV, and include upgraded portrait specifications to allow for the establishment of a portraits database to be used for face recognition as well as machine-assisted identity confirmation using the portrait displayed on the document.

While the TAG decided that specifications related to bar codes would not be included in the new edition, it did not exclude the use of one-and two-dimensional bar codes for additional data storage. But because they are not globally interoperable, the group emphasized that these technologies are for the issuing State only or under bilateral agreements; they cannot be considered for global use in the border inspection process.

Based on the successful results of updating Doc 9303, Part 1, the TAG continues its work updating Part 3 of the document on official travel documents (cards), to reflect the same changes included in Part 1. Expected to be ready for publication by the end of 2006, Part 3 will also be issued in two volumes.

Regarding the interoperability of steganography and digital watermarking, it was confirmed that digital watermarks do add to the security of the document in avoiding manipulation of the visual data contained in the visual data page and in the chip. But that said, a specification for an interoperable technique is not presently viable since all decoding software packages are proprietary systems. It was reported that two major market leaders have recently announced a co-operative effort to produce and make available a single reading platform that can read watermarks from both companies. This platform can then be expanded to include other digital watermark variations from other companies. Provided interoperability can be technically guaranteed, the

TAG intends to continue studying the market and work towards a recommendation to be included in Doc 9303.

As the group responsible for the research, analysis and reporting on new technologies available today or in the future for use in MRTDs, the New Technologies Working Group (NTWG) has set the following objectives over the short term:

- Create a plan to ensure effective means of disseminating appropriate information to both Member States and vendors on new developments;
- Provide expertise in the development of an eMRTD testing facility;
- Finalize technical report on eVisas;
- Complete research on a machine readable zone identifier for ePassports;
- Finalize technical report on hybrid travel documents;
- Research the development of RF writer/reader technology, emphasizing ergonomics and the mitigation of risks such as eavesdropping; and
- Provide guidance material on data sharing between States to support international initiatives related to lost and stolen travel documents.

The NTWG is also responsible for effective support and oversight of the development, implementation and management of the ICAO Public Key Directory (PKD).

Long-term goals include developing guidance material and standards to potentially enable States to leverage the storage capacity of RF Chips. While current technical reports relating to ePassports support the implementation of a "write once read many" deployment, over time, issuing authorities may wish to broaden the functionality to enable additional information to be written to this chip post issue. This may be as simple as updating the holder's portrait or as complex as allowing third parties to write data.

Additional activities either envisioned or currently underway include developing guidance material and standards in relation to real time data sharing between States through the positive validation of travel documents at check-in or border control, the receipt and processing of Internet-based travel document applications; the use of biometrics in the travel document issuance process; and automated border clearance of travellers presenting ePassports.

The TAG also approved the ongoing study of possibilities for electronic visas. A presentation summarizing the types of eVisas under consideration concluded that the collision of signals from two or more chips may not be as significant as originally thought. It suggested that as an alternative to placing a chip under a visa label, some authorities might be interested in placing visa information on the passport chip.

Regarding the NTWG's work on developing a technical report on hybrid card/book options for biomentric-enabled passports, it was reported that member States have expressed great interest in making this technology work. Airports Council International said the development of this technology is of particular interest to airport operators since some of its members are running programmes that may be compatible with it. The

report will be available and open for comment through the ICAO website (www.icao.int/mrtd).

As for the universal implementation of MRTDs, the Education and Promotion Working Group (EPWG), which helps the ICAO Secretariat develop means of presenting information to governments not currently issuing MRTDs or ICAO-compliant passports, has been involved in various workshops, reviews and seminars around the world. Some of these were in collaboration with the International Organization for Migration (IOM).

The group further reported that the profile of Doc 9303 has been raised in the G-8 Lyon-Roma group, which developed a best practice identity authentication paper, to be forwarded shortly to ICAO. Guidelines for secure issuance process and prevention of external fraud have also been developed by this group.

PKD Implementation

The ICAO Secretariat presented a set of draft regulations for the operation of the PKD, which clearly define what the PKD is intended to do. This includes how it will operate in terms of update frequency, response time to action requests, limitations of liability regarding the various entities involved with the PKD, and the fees and participation payment requirements.

Together with the PKD MoU to be signed between ICAO and the participating States, the adoption of the draft is of fundamental importance to the implementation and operation of the PKD.

Participation in the PKD is considered to be essential for the distribution of the public keys of a State that issues ePassports to all entities that need to use them to validate ePassports. Hence the TAG decided to form a PKD Advisory Group, comprised of a member from each participating State for the purpose of governance.

Finally, the TAG-MRTD heard several country reports, including a presentation on the Belgian ePassport project. Belgium has been issuing ePassports since 15 November 2004. Other reports came from Canada, updating the Canadian passport project; India, on the status of the Indian machine readable passport project, machine readable visa, and ICAO compliant ID card; Thailand, on the Thai ePassport project. Thailand has been issuing ePassports since 1 August 2005; the United Kingdom, updating the UK passport and national ID cards projects; and Singapore, updating the Singapore ePassport project.

Present for the meeting were the 11 members and two alternate members of the TAG, their advisors, and observers from 26 Contracting States and six international organizations. Countries currently comprising the TAG-MRTD are Australia, Canada, Czech Republic, France, Germany, India, Japan, New Zealand, Netherlands, Russian Federation, Sweden, United Kingdom and the United States. ◆

Note: Interested readers may download the complete report of TAG-MRTD/16 from the ICAO website (www.icao.int/mrtd).

Asia Software is a leader among the developers and integrators of biometric facial recognition technologies.

Facial Recognition Systems based on Asia Software's technology are now being effectively operated in activities of law enforcement agencies as they are applied in:

- Criminal divisions for database searches and criminal identification in the process of investigation;
- Migration services for reliable control of migration flow;
- Documentation centers for checks of all citizens while issuing documentation (Passports, IDs, Driving Licenses).

Using this technology, 3-5 particularly dangerous criminals and terrorists are identified every day.

At the moment a range of systems are designed especially for migration services to improve the efficiency of passport and visa control of travelers: Consul, Checkpoint, Migrant, VideoStream. These systems are intended to read MRTDs and include an ability to scan a photo from all types of passports, and check information obtained from the traveller against databases.

The above-mentioned systems became a basis for the Intergovernmental project CIS-VISIT the program of passport and visas control of all travellers in the countries of the Commonwealth of Independent States. From 2005, the CIS countries started implementing the CIS-VISIT program.

The technology can be easily integrated to MRTDs and the Republic of Kazkahstan has already issued the first biometric driving licenses on the basis of Asia Software's technology.

The technology has already proved its high efficiency and is currently in use as an actual tool for criminal detection and can also be applied in various biometric projects.
Asia Software has business partners around the world and is always open to new mutually beneficial cooperation.

46, 20-th Line st., Almaty,
The Republic of Kazakhstan
phones: +7 3272 757671, 757672
fax: +7 3272 584902

www.asia-soft.com
e-mail: info@asia-soft.com

ASIA SOFTWARE
the art of identification

EDAPS
CONSORTIUM

Who We Are

EDAPS CONSORTIUM, being a system integrator, develops and implements computer-control recording and information management systems in all spheres of government and production activities that allows us to offer "turn-key" solutions utilizing state of the art integrated products.

A Consortium that includes:

- A company that produces plastic cards and polycarbonate pages
- A company that develops and supplies equipment and software used in personalization of documents
- A security paper and printing complex
- A company that develops implements and maintains information technology systems
- A company that develops and produces holographic security elements for identity documents, payment cards and other security documents
- A Software development and database operations
- A bank offering a full range of services for corporate and private clients

What Do We Do

Provide integrated high-tech solutions to develop, introduce, and issue identity documents

Develop and implement modern information and production complexes for "turn-key issuance" of identity documents

Develop and implement information management systems and databases for state and local authorities, as well as the private sector

Provide automated citizen registration systems for the introduction of European and International standards for identity documents production

Development and implementation of biometric technologies and their application in the protection of state, society and personal interests

We can provide these solutions and products in a very cost effective way for your government or private sector project.

Contact us to learn more!

Our Experience

In Ukraine:

- Development of the Citizens Registry
- Development of Uniform State Automated Passport System
- The New Travel Passport
- Development of computer-control recording system for the national driving licenses and vehicle registration documents production and issue
- The New Driving License
- The New Vehicle Registration Certificate

Address:

EDAPS Consortium
64, Lenina Str.,
Kiev, 02088, Ukraine

Tel.: +38 (044) 561-25-80 (Olga Lyubimova)
+38 (044) 561-25-77
Fax: +38 (044) 561-25-85

e-mail: edaps@edaps.biz
http://www.edaps.biz

Machine Readable Travel Documents with biometric enhancement: the ICAO Standard

by Mary K. McMunn

This article is adapted from a briefing by the author to the World Customs Organization Biometrics 2005 Conference and Exhibition, Brussels, 8-9 December 2005.

News headline: ICAO to publish its Standard for ePassports

I begin with the current news – that early in 2006 ICAO plans a formal publication of its Standard – a standard that is already in use by the many member States that are developing the new-generation, electronically enabled machine readable passport, or "ePassport". This article reviews briefly the work ICAO has been doing over the past nine years to specify how to make use of biometric technology to enhance the security of travel documents and to facilitate inspection of international travellers at border control points.

© Imaging Automation - Viisage

As is outlined in another article in this issue, the Convention on International Civil Aviation and Annex 9 (*Facilitation*) together provide a framework of obligations of member States and Standards and Recommended Practices pertaining to the immigration and customs inspection and clearance of persons in airports. In this context ICAO, since 1980, has been publishing specifications for standard formats for machine readable passports, visas and official travel documents. Document 9303, *Machine Readable Travel Documents*, is now a suite with three parts. Part 1, *Machine Readable Passports*, is about to be published in its sixth edition.

Most readers and administrations are by now very familiar with the basic machine readable passport, which is now being issued by at least 110 States and territories, a number that is steadily increasing. The standardized format is comprised of two parts – a visual inspection zone or VIZ, containing mandatory and optional data elements in a prescribed layout; and a machine readable zone or MRZ, containing mandatory data elements in a form and position that are absolutely mandatory.

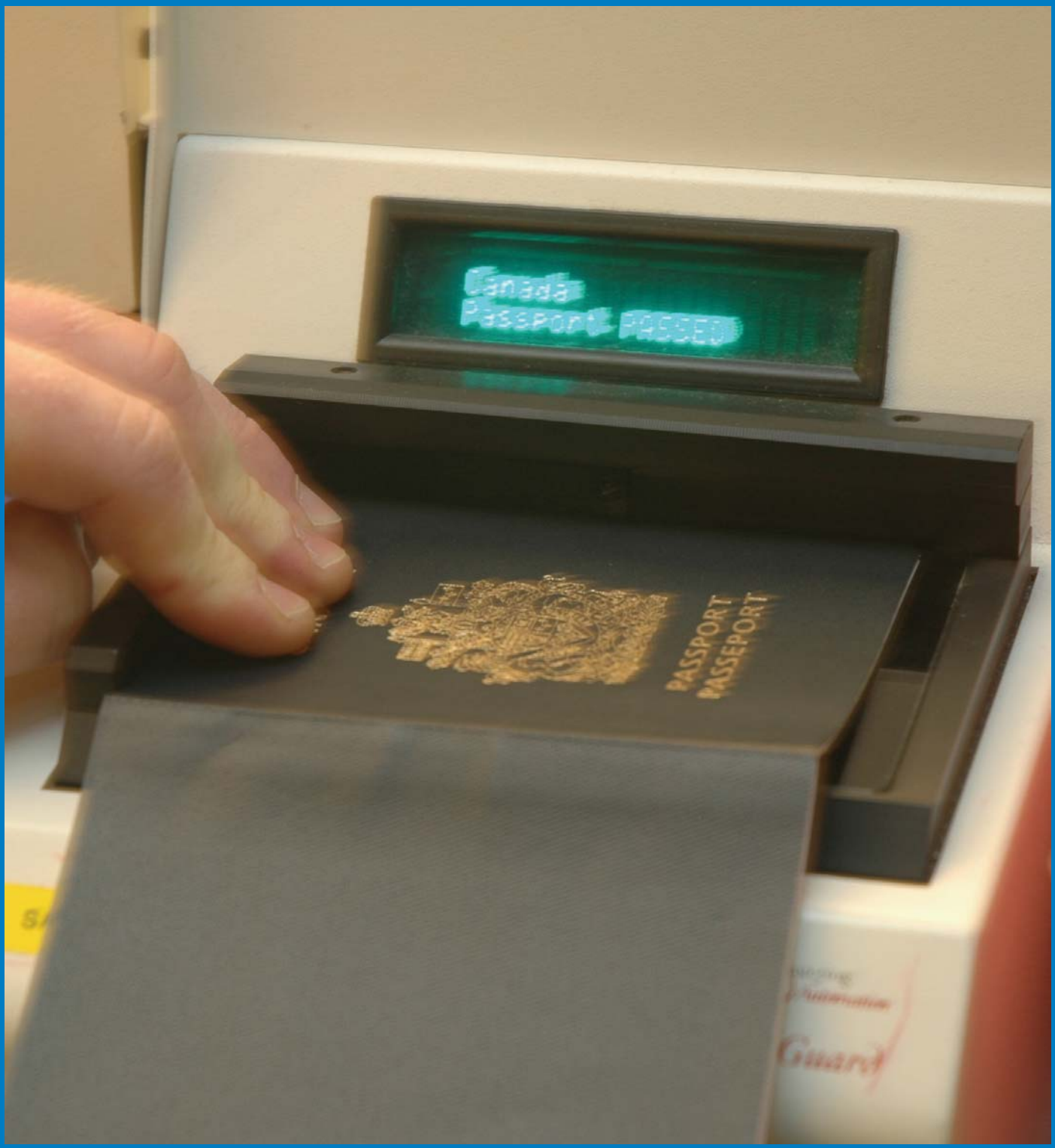
The two machine readable lines of OCR-B typeface, with their standard format, data elements, field lengths, and check digits, comprise the first security measure that ICAO invented for a passport.

Another security measure inherent in the document and in the inspection procedure is the use of a mandatory photo image to link the holder of the document to the document itself, in order to confirm identity. In recent editions of Doc 9303 ICAO has been tightening up the specifications for the photo, to insist on high-quality images of adequate size, preferably digital images printed directly onto the data page, in order both to prevent photo substitution and to offer more confidence to the inspector or airline agent making a visual comparison between the photo and the person presenting the passport.

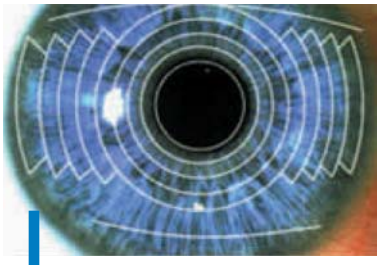
But over the years – and well before 9/11 – member States identified the need to confirm identity of travellers more effectively, due to the myriad cross-border social, political and criminal problems that emanate from identity theft. So in 1997 the ICAO TAG/MRTD asked its New Technologies Working Group (NTWG) to begin a systematic study of biometrics and their potential to enhance identity confirmation with passports and other travel documents.

In search of the "right biometric" for travel documents, the chosen approach was to first identify *requirements* instead of just reviewing industry-based technology studies. This set ICAO apart from mainstream thinking at the time, and incidentally invited criticism from purveyors and users. But we felt that to choose the "best-performing" biometric based on laboratory tests and then try to adjust our requirements to it would not be the right approach. Instead we chose to evaluate the different biometrics against the unique requirements of travel document issuance and inspection.

And what are these requirements? Briefly, they are: compatibility with travel document issuance and renewal; compatibility with machine-


Canada
Passport PASSED
PASSPORT
PASSEPORT

assisted identity verification requirements in the issuance and inspection processes; redundancy; global public perception of the biometric and its capture procedure; storage requirements; and performance. Considering all of these factors and using a quantitative scoring methodology, the group found that *face* came out on top with an 85% compatibility rating while *finger* and *iris* were tied in second place with a 60-65% compatibility rating. Therefore face was recommended as the primary biometric, mandatory for global interoperability, and finger and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing State.

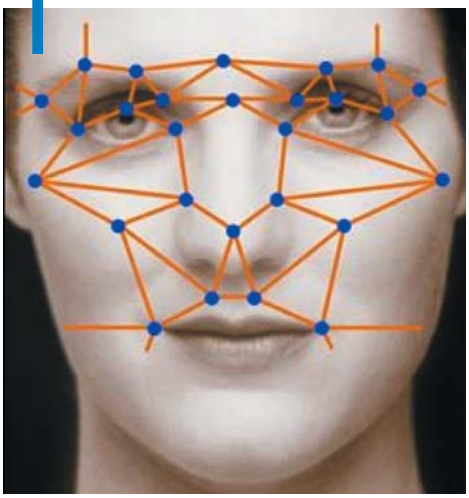


The face as primary biometric addresses numerous identity-related requirements. It supports lookout identification, as prior enrolment and cooperation of the subject are not required for successful image capture, and facial images are available on virtually every person in the world. Face also permits 100% identity confirmation in the inspection process, as the travel document photo of quality specified by ICAO could be used for machine assisted checks in the absence of an electronically stored image. Moreover, with the photo, facial recognition can be done visually, even when the equipment malfunctions!

After deciding that the face would be the primary biometric the NTWG looked for an appropriate storage medium. The medium chosen would have to offer

© Imaging Automation - Viisage

enough data storage space for *images* of the face and possibly other biometrics, as the concept of using templates had been abandoned due to the fact that templates and their readers are not internationally standard. The technology had to be non-proprietary, available in the public domain worldwide, in the interests of global interoperability. And of course the technology had to be compatible with book-style (paper and cloth) documents. Ease of use, without a requirement to position or fit the document into a reading device, was also a factor. The technology that met all of these requirements was the contactless integrated circuit, and the NTWG decided that of the two ISO-standard options, the "proximity" type (ISO/IEC 14443) should be specified.



Next, a standardized "logical data structure" for programming the chip was specified to ensure that chips programmed in any country could be read in any other country. And because data written to a chip can be written over, a public key infrastructure (PKI) scheme was required, in order to give the reader of the chip assurance that the data had been placed there by the authorized issuer and that it had not been altered in any way since then. Thus an expert group within the NTWG developed specifications for a specialized PKI for application to travel document issuance and inspection. (For more information on PKI, see the article by David Clark, in this issue.)

Finally, during the testing of chips and readers there arose issues of skimming and eavesdropping. The physical possibility of skimming – the surreptitious reading of the data in the passport chip by means of a concealed device and unnoticed by the holder – is considered to be extremely remote, but nevertheless it is a concern. Eavesdropping – illegally listening in on a communication between the chip and the reader – though unlikely, is feasible. To address these concerns a scheme for "basic access control" (BAC) was developed and recommended for use by issuing States. Under BAC the inspection system uses a "key" derived from numeric data elements in the MRZ to "unlock" the chip so that the system can read it. Thus the passport must be open in order for the chip to be read, and the holder is assured that his data can be read only when he hands over his passport.

So there you have it – what ICAO calls its biometric blueprint, consisting of four parts – the facial image, the contactless proximity chip, the logical data structure, and the ICAO PKI. These "four pillars" are each essential to the ePassport, and are inseparable from one another. Technical details about the blueprint and the ePassport standard and other aspects of ICAO work in MRTDs can be found on our dedicated web site – www.icao.int/mrtd. ◆

First ePassports, then eVisas

by John W. Mercer

This article, adapted from "eVisa vs ePassport – The Way Forward" by the same author, published in 2005 in the Keesing Journal of Documents & Identity, addresses the prospect of an ICAO standard for eVisas as a companion to its work on ePassports recounted elsewhere in this journal.

So what to do about the visa? Before machine readability standards, a visa was usually a stamped notation with manual in-filling of data pertaining to the holder, and sometimes the holder was not even named, resulting in the "bearer" visa. The non-uniform optical characteristics of various passport visa pages, and interference from the background printing made it not possible to print the visa data onto the visa page, thus requiring that the ICAO machine readable visa be a label.

The ICAO-compliant visa is a label of two sizes, ID-2 and Format A, which is almost ID-3. The smaller, ID-2 size allows the perforated numbers commonly in passports to be read on the visa page, while the larger Format A visa has more room for printing of data. Current specifications (Doc 9303, Part 2, 3rd Edition, 2005) allow only one person to be named on each visa and require a space for a portrait.

There is no one visa issuance procedure, but many, answering to a multiplicity of commercial and national requirements. Even so, a solid and workable, standardized methodology for making machine readable visas has developed, and the trick now is to add biometric identifiers to the visa issuance process.

One method of providing a biometric identifier is to capture the biometrics of the visa applicant upon application, and then store those biometric images in the electronic data file of the visa applicant, not on the visa. Through Advance Passenger Information (API) the receiving country, who issued the visa, will know in advance the passengers listed on the airline passenger manifest. Biometrics associated with the passengers known to have visas can be called up to a local (and transient) file which can be quickly accessed and opened when the traveler arrives at the border, by reading the machine readable data from the visa. This works well, keeping the person's biometric data in the system, only accessing it when they and their visa document are present for comparison. But other nations and airlines may not be privy to the biometric file, and thus the positive identification benefits of the biometric are limited.

The ICAO New Technologies Working Group is developing a technical report on eVisas, the current version of which was presented to the last TAG-MRTD meeting, 27-28 September 2005. This paper suggests that ICAO can play a positive role in establishing an interoperable standard compatible with the existing specifications for machine readable visas. At the same time it is important to "ensure that eVisa techniques employed by different States do not interfere with the global interoperation of ePassports and e-travel cards."

The report outlines three options for the chip in visa applications: by writing to the chip contained in the ePassport, by use of a chip under a visa sticker, and a separate chip visa card. An unstated fourth option, of the chip incorporated into the visa sticker before security printing, is a non-starter, because any chip/antenna combination passing through the pressures of intaglio printing nip would likely be broken and thus unusable. However, there are significant implementation challenges associated with each option. Moreover, the amount of available data storage data storage is an issue, as only a few compressed face (15-20Kb) or fingerprint images (10Kb) can fit in a chip of 64Kb memory capacity.

Two intriguing possibilities are suggested. One is that eventually minutia may be able to be stored and used as the basis for global data interchange. Present technologies and standards do not allow this, but should it occur, the need for chips of great memory capacity will be reduced, and faster reading times will result. The second possibility points to the future when eVisas are compatible with ePassports, and traveler "verification using a single suite of document and biometric reader technology" would not only contribute to security, but facilitate travel as well.

The report concludes with a series of policy questions: How can you notify the country of issuance that a chip visa has been added to their passport? What can provide visual indication of the presence of the eVisa in a passport (analogous to the e-pass logo on the cover of ICAO compliant ePassports)? How can an eVisa be cancelled? Are there privacy considerations inherent in the eVisa?

In sum, there are significant areas of overlap where the work that has led to the progress and implementation of the ePassport can be used in the development of the eVisa. But there are areas of significant difference where the future is unknown and technical and policy challenges exist that have not yet been resolved. One thing is clear. It is not a simple transition from the ePassport to the eVisa! ◆

New Symbol Allows ePassport to be Recognised Instantly

by Sjef Broekhaar

ICAO's New Technologies Working Group (NTWG) has spent the last few years assessing the most suitable biometric for travel documents, drafting technical reports and finding solutions to secure and protect the electronic data carrier. Following extensive research and careful evaluation, the group put forward the contactless integrated circuit (IC) chip as the most suitable storage medium for passport applications. However, because the inclusion of contactless chips in travel documents was not – at that time – governed by ISO standards, the group immediately faced another challenge. Apart from highlighting the most suitable positions to embed a contactless chip in a passport, this article discusses the introduction of a new symbol that makes it much easier to recognise ePassports.

Eight years ago the NTWG initiated a four-year study into the inclusion of biometrics in travel documents, that resulted in a short list of three suitable biometric techniques (as most readers are undoubtedly aware, these are facial, fingerprint and iris recognition). The decision to advise the Technical Advisory Group (TAG) to recommend the facial image as the 'globally interoperable biometric' for MRTDs was taken in 2002, in Berlin. This proposal was subsequently adopted by ICAO and announced to the world on 28 May 2003.

Selection of Storage Medium

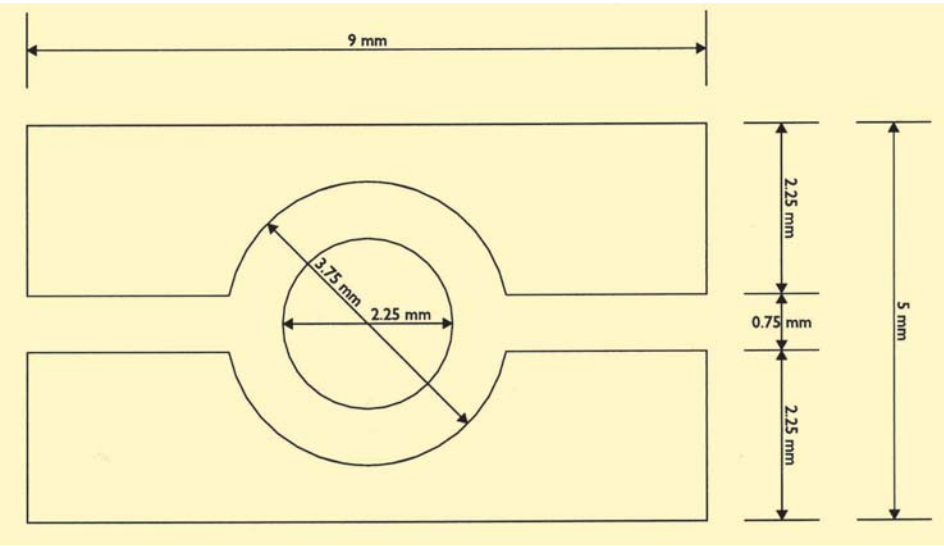
While evaluating the various biometric techniques, the NTWG also faced the challenge of selecting a suitable data carrier. Although several alternatives were evaluated, the group eventually opted for the contactless IC chip. It did so for the following reasons:

- Interoperability: in addition to being laid down in ISO/IEC14443 and ISO/IEC 15693, the radio frequency (RF) used by contactless IC chips is used around the world.
- Durability: more than 100 million IC chips are currently in use across hundreds of applications.
- Flexible embedding: unlike contact IC chips, which must be embedded in a fixed position, contactless IC chip/antenna assemblies may be embedded in any position.

Invisible

Embedding the IC chip/antenna assembly in a passport proved less straightforward that it would seem. The following alternatives were/are available:

- The biographical data page;
- Between the end paper and the cover (both at the front and the back);
- Between the centre pages of the document (where the binding is visible); or
- Within a separate page.



Dimensions of the ChipInside symbol, size A (scaled 10:1)

Size A, 5.25 x 9 mm
(actual size)

Size B, 4.2 x 7.2 mm
(actual size)

As the above solutions hide the IC chip from sight, inspectors would find it difficult to establish whether a given passport contained a chip at all. In recognition of this potential problem the NTWG reviewed a number of options, including the use of (i) an MRZ-based identifier or (ii) a visible symbol (possibly in combination with text). In the end, the group decided in favour of a symbol on the face of the passport, allowing the document to be recognised at a glance. After all, a symbol has strong communicative properties.

The Selection Process

The ePassport symbol was jointly developed by the Document Content and Format Working Group (DCFWG) and the NTWG. A short list of nine was prepared, and from these the TAG/MRTD, at its 15th meeting in May 2004, picked the design of Dutchman Joost van Roon.

The ePassport Symbol Explained

The symbol chosen had to recognise that a country's design preferences (and concepts) should be respected. The symbol and the guidelines for its positioning should allow as much space as is required for all the different characteristics on existing passport covers.

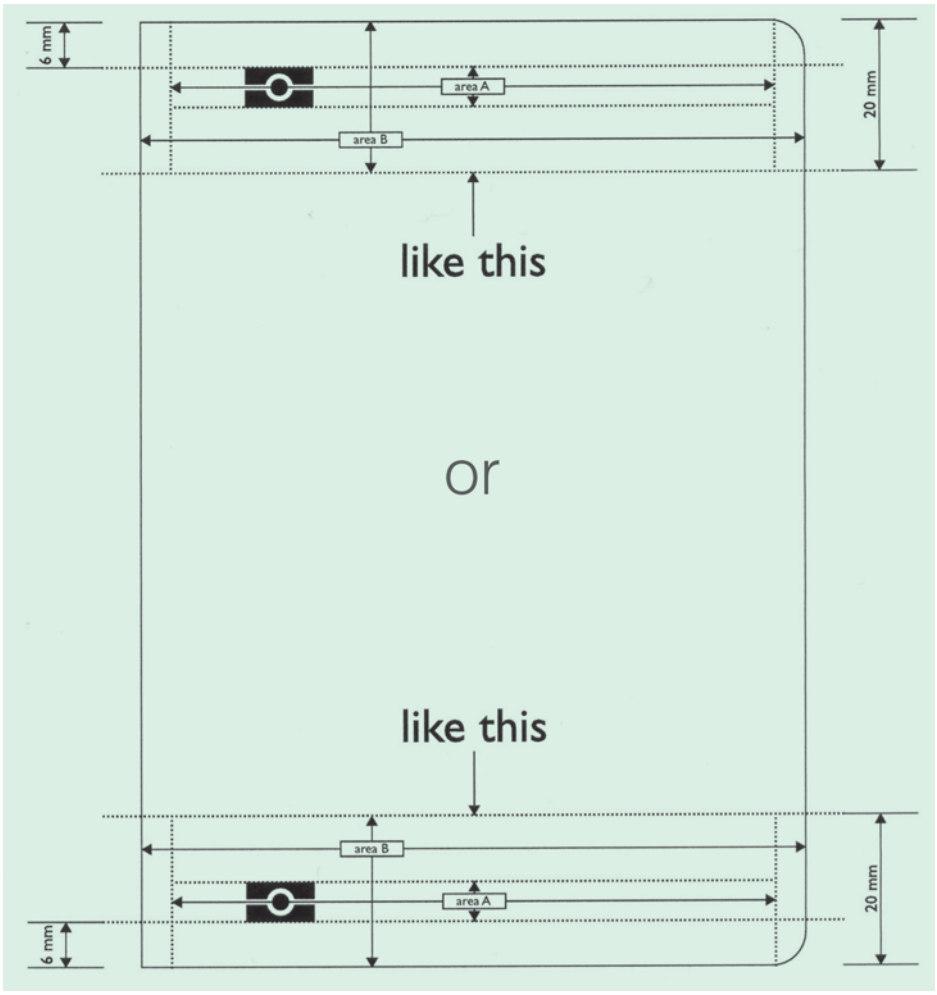
In view of the above, the designer opted for a neutral symbol that can be included in a variety of design concepts. At the same time, the symbol is easily recognised and easily associated with ePassports. In short, it is a neutral symbol based on an uncomplicated design.

As shown above, the ePassport symbol consists of a small circle enclosed by two horizontal rectangles, representing the chip sandwiched between two layers of material. The level of detail is such that the symbol can be produced in the desired size and by means of gold foil blocking, using silk screen printing techniques.

Van Roon has transferred all design rights to ICAO, which has included a technical description of the symbol in Doc 9303, Part 1, sixth edition, 2006, Volume 2.

Other Applications

In addition to being used on ePassports, eIdentity cards and other eDocuments, the new symbol can be used at airports and seaports or rail stations around the world. The symbol can, for example, be used to guide visitors to special ePassport desks. Indeed, some passport reading machines already display the new symbol.



Area and position of the size A symbol on passport covers

Conclusion

The inclusion of a symbol on ePassports and other electronic travel documents facilitates unambiguous communication (as of the moment the documents are issued). On seeing the symbol, an inspector knows that the document contains a chip, that it should be inspected using electronic equipment, and that it should be treated with due care. Issuing authorities can also use the symbol – in combination with supporting text, if necessary - to point to the location of the chip. In turn, inspectors can bear this information in mind when stamping the passport with entry/exit stamps. At the end of the day, it is in everyone's interests that ePassports function as they are supposed to, allowing for quick and efficient inspection. Only then will it be possible to process large numbers of people quickly. ◆

ICAO Contracting States

NORTH AMERICA
Canada
United States

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

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

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

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

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

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

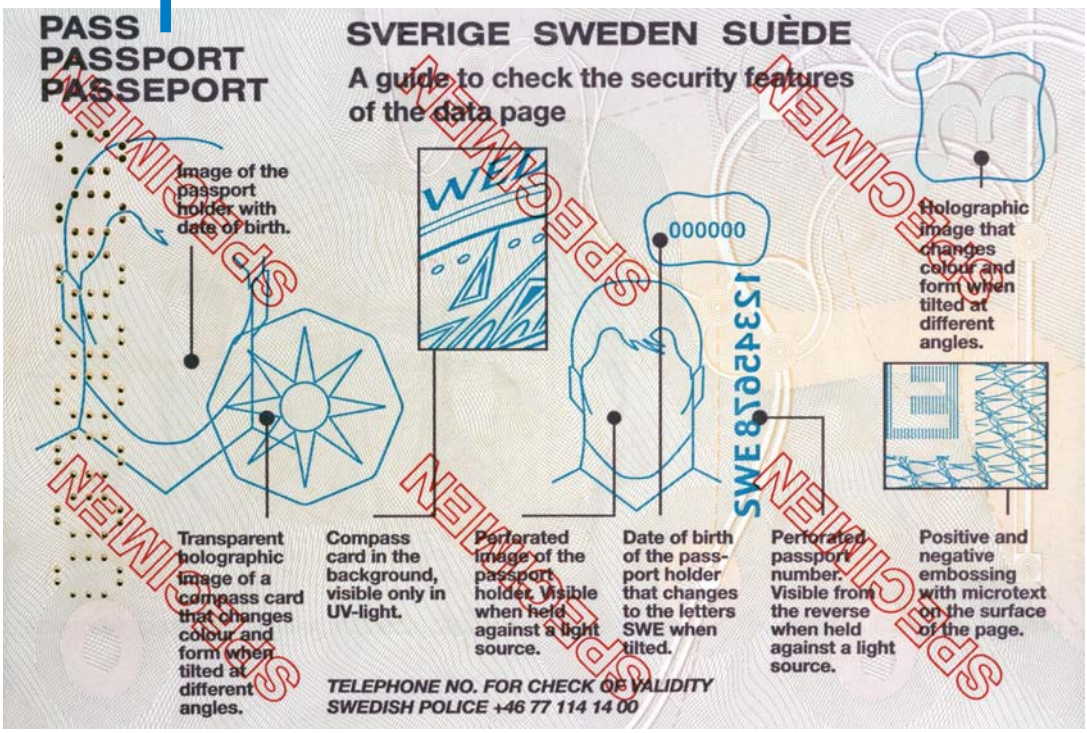
ASIA/PACIFIC
Afghanistan
Australia
Bangladesh
Bhutan
Brunei Darussalam
Cambodia
China
Comoros
Cook Islands
Fiji
India
Indonesia
Japan
Kiribati
Korea, Democratic People's Republic
Lao People's Democratic Republic
Malaysia
Maldives
Marshall Islands
Micronesia, Fed. States of
Mongolia
Myanmar
Nauru
Nepal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

Country Update: Sweden Introduces ePassports

by ICAO Secretariat

Sweden has become the second European country, following Belgium, to start issuing biometrically-enhanced passports compliant with ICAO standards for biometrics in machine readable travel documents.

The new Swedish ePassport, introduced 1 October 2005, has a Radio Frequency Identification microchip embedded in its data page. The chip contains a digital photo and passport information of the holder. To authenticate passport holders and reduce the risk of theft or fraud, the digital photo can be measured against the facial features of the traveler using the passport, using an electronic document reader and a camera located at the control point. As recommended by Annex 9 to the Convention on International Civil Aviation, ICAO's charter, the passport is valid for five years.



Dark red in colour, as compared to the previous blue, the new passport is further distinguished by the easily recognizable ePassport logo—a small circle enclosed by two horizontal rectangles—jointly developed by ICAO's Document Content and Format Working Group and New Technologies Working Group.

Together with state-of-the-art technology, new photo regulations have also been introduced. Again according to ICAO standards, passport photos must now be taken from straight-ahead, as opposed to the previously required half profile. The facial expression must be neutral, no smiling, with black and white photos preferred.

And whereas Swedish citizens applying for passports could in the past get their picture taken at photo shops, they must now be photographed at one of the country's police offices. According to the Swedish Police, this guarantees better picture quality and nullifies the risk of photos changing hands.

Currently Sweden has 246 police offices scattered across the country, but rather than introduce new technology into all existing offices, the number of police offices handling passport applications has been reduced to 100. Since the new passports are valid five years, compared to the previous ten, these 100 offices will have to deal with number of applications expected by the Swedish government to reach 1.4 million per year.

In addition, the price of the passport has increased from SEK 270 to 400 (approximately EUR 29-43, USD 34-50). For added security, applicants are required to pick up their passport in person. Citizens holding a Swedish passport issued before 1 October 2005 do not have to renew their passport until the expiration date.

The rapid Swedish switch to ePassports is due to several factors. The expiry last year of the previous contract for the supply of Swedish passports helped enable a shift to the new biometric technology sooner rather than later. Another incentive was the Swedish government's desire to comply with the United States Visa Waiver Programme (VWP). The 27 States participating in the VWP, such as Sweden, are required to issue machine readable passports with digitized photos by 26 October 2005 and present a plan to begin issuing passports with integrated circuit chips within one year. According to ICAO, some 40 countries are currently planning to upgrade to biometrically enhanced ePassports by the end of 2006. About 25 of these are EU States.

Besides being ICAO-compliant, the new Swedish ePassport also abides with the European Union Regulation on standards for security features and biometrics in passports and travel documents, as adopted on 13 December 2004.

Using the same biometrics technology as in the passport, Sweden has also introduced a new national ID card. While not a required document, the ID card is valid for five years and can be used in place of passports in the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, and Switzerland. ◆

States planning to upgrade to ePassports

The States that have indicated their intention to upgrade to ePassports en the next two years are: Andorra, Australia, Austria, Belgium, Brunei, Canada, Czech Republic, Denmark, Finland, France, Germany, Hong Kong Special Administrative Region of China, Hungary, Iceland, Indonesia, Ireland, Italy, Japan, Republic of Korea, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Monaco, the Netherlands, New Zealand, Nigeria, Norway, Pakistan, Portugal, San Marino, Serbia and Montenegro, Singapore, Slovenia, South Africa, Spain, Sweden, Switzerland, the United Kingdom, United States.

PKI and Public Key Directory – an ICAO programme for ePassport Security

by David Clark, P.Eng.

As a major measure to improve the security of machine readable passports, a number of ICAO member States are planning to issue an electronically enabled passport, or "ePassport". This new-generation document contains an integrated circuit chip (ICC), embedded either in the cover or within an inner page and containing electronically all of the machine readable passport data as well as a biometric measurement (face image and possibly others) that can be verified with computer algorithms.

Computerized biometric checks are intended to augment the normal visual inspection process by a human government official or airline agent, and provide additional confidence in the document's validity. EPassports also present increased challenges to a counterfeiter. Nonetheless it is possible to create a completely counterfeit passport with fraudulent electronic as well as printed data

The ICAO Public Key Infrastructure (PKI) has been designed to prevent such counterfeiting opportunities, by effectively guaranteeing the authenticity of the electronic data. The ICAO Public Key Directory, or PKD, is an essential component of that PKI.

Data Protection

Data stored on an ePassport chip can be forged, rendering the ePassport untrustworthy. In fact, *electronic ePassport data must be authenticated each time it is read, using the protective features of the ICAO PKI, if the data is to be trusted at all.*

Two actions are essential to ensure that the electronic data is valid, namely;

- Verifying that the data has been recorded in the ePassport by the proper issuing country; and

- Verifying that the electronic data has not been altered in any way.

The PKI specification that ICAO has developed to carry this out features the use of "asymmetric cryptographic keys", consisting of a pair of keys for each set of data to be encrypted. This key pair is mathematically unique in that:

1. One key of the pair is used to encrypt the data, but cannot be used to decrypt the data. This key is called a private key, and is kept secret by the issuing country.

2. Only the other key of the pair can decrypt the data. This is called the public key.

3. The public key does not provide any information regarding the companion (private) key. As a result the public key can be made available publicly to verify the source and validity of the data encrypted, without revealing the private key that was originally used to encrypt the data.

This is very powerful technology. Anyone reading encrypted data and decrypting it with the valid public key knows with certainty that a) the data was created and encrypted by the proper

sender (using the corresponding private key), and b) that the data has not been changed in any way.

Digital Signatures

The ICAO PKI uses this technology on ePassport data by encrypting a *hash calculation* on the data rather than encrypting the data itself. This hash digest is an arbitrary mathematical process analogous to a sophisticated check-digit calculation. The mathematical process produces a very unique result that is then encrypted by the country and stored as a *digital signature* on the ePassport. This process is shown in Figure 1 below.

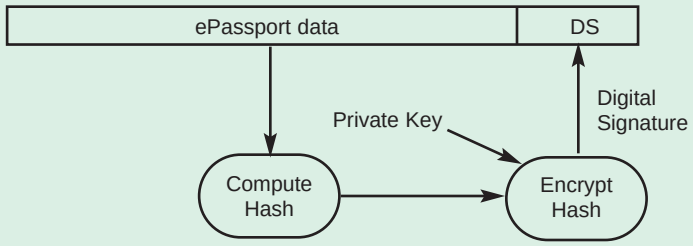


Figure 1 - Creating the Digital Signature for an ePassport

Security is achieved because of the uniqueness of the hash value. Other entities reading the non-encrypted electronic data re-compute the hash value from the data, decrypt the encrypted hash digital signature using the valid country public key, and compare the two. If they are the same, the reader then knows with certainty that a) the ePassport electronic data was inserted in the ICC by the issuing country, and b) that the data has not since been altered in any way.

In this way the forger is stymied. The ePassport data cannot realistically be changed or forged, since the resulting new hash value cannot be properly signed; the private signing key of the country is not known by the counterfeiter. The forgery will therefore be detected when the ePassport is read and the digital signature checked. Therefore, forging of electronic data without being detected is effectively impossible, *assuming the digital signature is checked in each instance*.

This process is shown in figure 2 below.

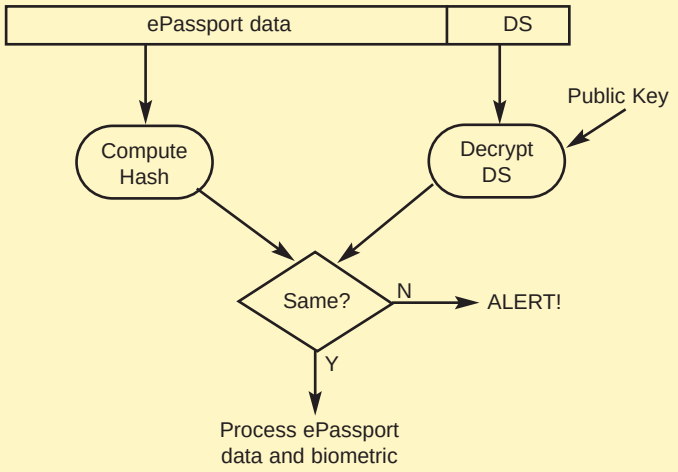


Figure 2 - Verifying the Digital Signature on an ePassport

Valid Country Keys

An integral part of the above process is: *knowing that the purported public key for each ePassport is valid*. It would be quite easy to record false data, including a biometric matching the counterfeiter and a digital signature using a false key. It would also be easy for an imposter to use the counterfeit passport for travel and get away with it, if the key itself were not validated.

Countries will address this by publishing their public signing keys in the form of key certificates that are in turn digitally signed by a master key of the country, called the country CA (Certificate Authority) key. The corresponding CA public keys will be distributed through diplomatic means amongst all ePassport issuing countries, and will be used by these countries to validate signing keys by checking the CA digital signatures.

However, airlines, non-ePassport issuers or border inspection agencies of any country will not have access to the secret country CA public keys

and will not be on the distribution list for public signing keys.

If such inspecting entities do not know or cannot verify that a public key is valid, the electronic data in an ePassport cannot be relied upon. Even if a public key certificate were provided on the ePassport, it must still be validated with the country CA public key; otherwise it too could be false. *It is paramount that all entities understand that validating the key is as important as validating the data; checking the digital signature is otherwise a meaningless exercise*.

Role of the PKD

The ICAO PKD has a central role in this regard as the main global distribution point for all signing key certificates from all issuers of ePassports. Significantly, ICAO will also have the master CA public keys from each issuer, so that it can validate every public signing key certificate sent to it for publication. As a result, every certificate on the PKD will have been validated.

Inspectors of ePassports throughout the world can therefore access the PKD and use the public signing keys to validate ePassports in confidence. They can therefore take full advantage, as intended, of the security provided by the new ePassport and biometrics technologies being adopted for international travel.

Validating ePassports with trusted public keys prevents people from wrongfully crossing a border and it also prevents people from wrongfully boarding an airplane. If you are a passenger on that flight, the latter concern is of paramount importance. The PKD is fundamental to achieving this objective. ◆

ICAO assistance mission to Colombia

In 2005 ICAO adopted a new standard, that all Contracting States issue only ICAO-standard machine readable passports (MRPs), by no later than 1 April 2010. The 79 or so countries that do not yet do so recognize the high value of ICAO-standardized documents for travel and tourism, and are seeking assistance to upgrade their passport issuance systems.

ICAO stands ready to provide such assistance, in the form of project planning, technical and policy guidance, education, arrangements for financing, and project management, as may be requested by an individual State. In addition, States can request objective evaluations of their prototype documents to assure compliance with ICAO specifications.

In November 2005, ICAO organized an assistance mission to Colombia, and in December to Brazil. The testimonial on the opposite page attests to the value of this initiative.

From left to Right:
Coronel Germán Paez Huertas, Secretario de Seguridad Aérea UAE de aerocivil
Maria del Pilar Yepes Moncada, Jefe Oficina Centro de Estudios de Ciencias Aeronáuticas UAE de aerocivil
Rocio Mantilla, Secretaria General Ministerio de Relaciones Exteriores
Dr. Fernando Sanclemente Alzate, Director General U.A.E de Aeronáutica Civil
Jair Orlando Fajardo Fajardo, Jefe Oficina Asesora de Planeación (OAP) UAE de aerocivil
Alvaro Andrés Motta Navas, Secretario de Sistemas Operacionales UAE de aerocivil
Julio Enrique Ortiz Cuenca, Representante Permanente de Colombia ante el Consejo de la OACI.

Mr. José Sandoval

Mr. Mauricio Siciliano

DELEGACIÓN DE COLOMBIA
ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNATIONAL

Montreal, January 19th of 2006

06-011 E
AT-Dir/ICAO

Mr. Mohamed Elamiri
Director
Air Transport Bureau
International Civil Aviation Organization
Suite 11.20

Dear Mr. Elamiri,

The Permanent Representative of Colombia on the Council of the International Civil Aviation Organization would like to thank ICAO for organizing and participating in the Mission to Colombia under the Universal Implementation of Machine Readable Travel Documents (UIMRTD) programme, to assist the government in the implementation of the ICAO - compliant machine readable passport.

In this context the Facilitation Section, with the support of Colombia's Ministry of Foreign Affairs and the Colombia Civil Aviation Authorities, organized and participated in the seminar on Machine Readable Travel Documents, held in Bogota the 2nd and 3rd of November 2005. Presentations were made by Mr. Mauricio Siciliano, with the cooperation of the Government of Ecuador in the person of Mr. José Sandoval, former Director General of Travel Documents and former project manager of the new machine readable passport project, who assisted our government in streamlining the tender documents and process of the coming Colombia MRP.

Colombia received comprehensive technical information about the new international travel documents standards, to facilitate their implementation within the time frame established by ICAO in Annex 9, Standard 3.10.

We would like to highlight and reiterate the importance that this event had for Colombia and the surrounding States who are in the process of implementing the Machine Readable Travel Documents, the Andean Passport, and the new generation of electronic passports, which will place us on the same level as the most developed States of the world. Therefore, we would like to keep counting on the valuable support ICAO provides in this field.

Please accept, Sir, the assurance of our highest consideration.

JULIO ENRIQUE ORTIZ CUENCA
Permanent Representative of Colombia on the Council of the
International Civil Aviation Organization

DO YOU KNOW WHO'S TRAVELING?

iA-thenticate® Smartchip

A full page document authentication scanner with RFID contactless chip reader for ePassports and government issued identification cards. It includes Basic Access Control (BAC) and 1 pass read with automatic authentication.

Massachusetts 978.932.2200 Washington D.C. 703.414.5800
EMEA +49 234.9787.0 www.viisage.com email: sales@viisage.com

ViiSAGE

18 years
60,000,000 secure passports
and moving forward....

GET. Into the future of secure travel and ID documents

When you need the newest and most secure passport, visa, and ID issuing solutions, talk to us. Global Enterprise Technologies is the world leader in state-of-the-art passport and ID solutions. With 10 international offices and affiliates and extraordinary resources and experience, we are strongly positioned to meet the needs of all clients, irrespective of size and issuing volumes, and wherever located.

As distributor of **TOPPAN** digital passport and ID printers worldwide for over a decade, developers of our own proprietary software solutions, and with unparalleled integration experience, GET is proud to offer a wide array of exclusive printing solutions that can be designed to meet your needs. Our newest printer, the **TOPPAN** E2000 passport printer, is specifically designed to fully meet the requirements for ICAO/ISO e-Passports and features on-line chip encoding, automatic book feeding and user-friendly operation.

With references in Canada, Egypt, Korea, Malaysia, Mauritius, New Zealand, Oman, Tanzania, Zimbabwe, the United Arab Emirates and the United States of America, contact us to find out why our **TOPPAN** based solutions are setting the standards for secure passports. Around the corner or around the world. GET. Into the future.

GET

GLOBAL ENTERPRISE TECHNOLOGIES CORP.

275 Wyman Street, Waltham, MA 02451 USA

Tel: +1 781 890-6700, Fax: +1 781 890-6320

info@getgroup.ca

Applying ingenious technologies to protect your security.

More than 100 years of developing practical and ingenious products has made 3M one of the most trusted and respected companies in the world. Our technology expertise is broad and deep, which has allowed us to develop some of the most secure products in the industry. Products such as 3M™ Confirm™ Laminates, 3M™ ePassport Readers, 3M™ Identity Document Issuance Systems and 3M™ Border Management Systems. Find out more at **www.3M.com/security.**

Local Service. Global Support.