ICAO MRTD REPORT

VOLUME 2 / NUMBER 1

OPTIMIZING SECURITY AND EFFICIENCY THROUGH ENHANCED ID TECHNOLOGY

The ICAO Public Key Directory (PKD) is operational

The Face as the Primary Biometric Identification for use with ICAO eMRTDs

The E2000 ePassport Printer

20 years

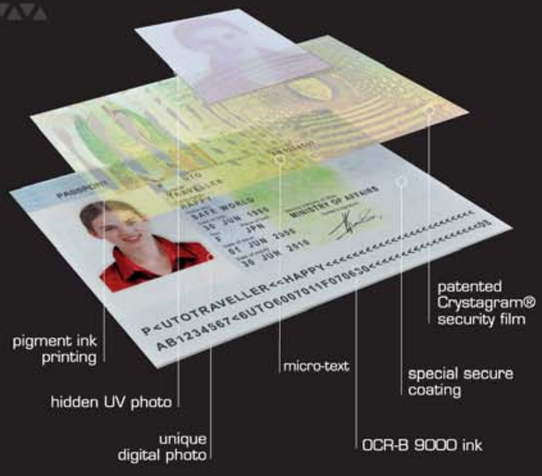
100,000,000 secure passports and counting…

When you need the newest and most secure passport issuing solutions, talk to us.

Global Enterprise Technologies is the world leader in state-of-the-art passport solutions. With an international network of 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 exclusive distributor of **TOPPAN** digital passport printers worldwide for over a decade, developers of our own proprietary software solutions with biometric modules, and with unparalleled integration experience, GET is proud to offer a wide array of unique passport printing solutions that can be designed to meet your specific needs. Our newest printer, the **TOPPAN** E2000 passport printer, is specifically designed to fully meet the requirements for ICAO/ISO ePassports and features on-line chip encoding, automatic book feeding and user-friendly operation.

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



The E2000 Passport

GET. Into the future

Global Enterprise Technologies Corp.
275 Wyman Street, Waltham, MA 02451 USA
Tel: +1 781 890-6700 Fax: +1 781 890-6320
www.getgroup.com

GET™

ICAO MRTD Report

Vol. 2, No. 1 2007

Editor: Mauricio Siciliano

Assistant Editor: Gillian Dupont

Chief, Security and Facilitation Branch:
Haile Belai

Chief, Specifications and Guidance Material:
Dominique R. Antonini

Graphic Art Design: Sylvie Schoufs,
FCM Communications Inc.

Cover: Studio Idées en Page inc.

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

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

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

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

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

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

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

Table of contents

Editor’s message

Dear Reader,

The present issue of the MRTD Report focuses on two subjects relating to the ICAO Biometric Blueprint: the use of the face as the primary biometric for interoperability of ePassports, and the launch of the ICAO Public Key Directory (PKD) as the main global distribution point for all signing certificates from all issuers of ePassports.

In this edition, you will read about face selection as the primary biometric identification tool to be used with the ICAO specified electronic machine readable travel documents (MRTDs), and its use in performing the verification and identification function of States. We have also included an article on how to prepare and store the biometric digital images on the ICAO specified radio frequency integrated circuit (RFIC) as well as practical and illustrative guidelines for portraits in MRTDs. At the end of the journal, you will find a list of definitions and terms related to biometrics to be used as reference.

This issue highlights the conclusion of the development and implementation of the ICAO PKD. In February, the Council gave its full support to the establishment, under ICAO aegis, of this key element of the “ICAO Blueprint” for the issuance of ePassports. The PKD will allow for the verification and authentication of ePassports worldwide. In March, the ICAO Secretary General presided over a ribbon-cutting ceremony inaugurating the ICAO PKD Office, thus culminating the development and implementation stage of this project. The ICAO PKD is a significant milestone in the development of ICAO specifications and has been well received in ICAO as an asset, not only for border controls and passport security but for aviation security objectives, as well. States participating in the PKD have already started loading their certificates onto this directory, and the system is open to all Contracting States for membership. In this context, an article outlining the procedures for States to become a Participants in the ICAO PKD has also been also included.

Finally, you will read about our very successful Second Symposium on ICAO-Standard MRTDs, Biometrics and Security with Exhibition, which took place in September 2006; and about the upcoming Third Symposium which is scheduled to take place from 1 to 3 October 2007 at ICAO Headquarters.

Enjoy your reading and please feel free to share the information in this magazine among your colleagues, State organizations, businesses, and the general public. A PDF version of this magazine is available free of charge from our web site http://mrtd.icao.int. Paper copies can also be ordered on-line. Visit: http://icaodsu.openface.ca/mainpage.ch2 for more information.

Mauricio Siciliano
Editor

Government

360° competence in contactless ID

As an innovative forward-looking company we work on the contactless ideas of tomorrow. By selecting the ideal technology platform and creating contactless ID sub-systems that work in the real world, ASSA ABLOY ITG supports system integrators worldwide.

Fare collection goes contactless

Maintaining maximum security is important, especially when it comes to personal identity authentication. Traditional forms of identification just aren't enough in today's world. The answer: electronic personal identification systems that are easy to use – but hard to misuse. With ASSA ABLOY ITG, security professionals in business and government have a global partner to help them develop and implement secure, reliable and interoperable ePassport, eNational ID, eDrivers' licence and eHealth projects.

Products and services for your secure identification solution

As a leading supplier in the ID management and RFID markets, ASSA ABLOY ITG can address requirements – in both hardware and software – to create and customize superior secure ID document solutions, including inlays and operating systems as well as reader components and plug-in readers, initialization services and training.

Inlays for ePassports, eNational ID cards, eDrivers' licences

OEM, plug&play, customized readers

ASSA ABLOY

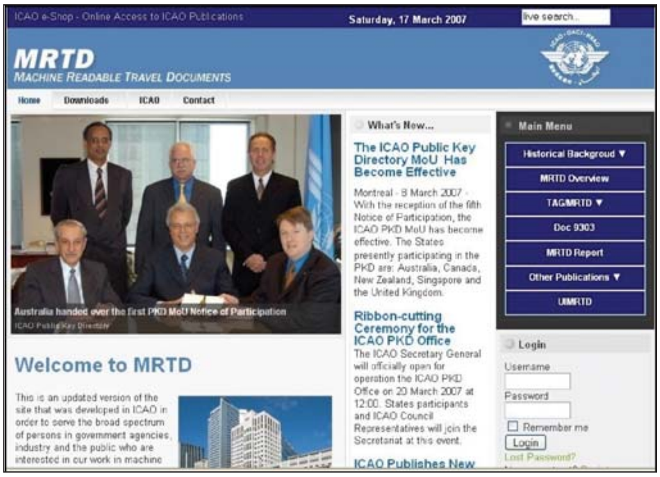
ITG

Identification Technologies

www.aaitg.com

The ICAO Machine Readable Travel Documents (MRTD) Web Site

ICAO Secretariat has updated the MRTD site 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.



Australia handed over the first PKD MoU Notice of Participation

ICAO Public Key Directory

The ICAO Public Key Directory MoU Has Become Effective

Montreal - 8 March 2007 - With the reception of the fifth Notice of Participation, the ICAO PKD MoU has become effective. The States presently participating in the PKD are: Australia, Canada, New Zealand, Singapore and the United Kingdom.

Ribbon-cutting Ceremony for the ICAO PKD Office

The ICAO Secretary General will officially open for operation the ICAO PKD Office on 20 March 2007 at 12:00. States participants and ICAO Council Representatives will join the Secretariat at this event.

ICAO Publishes New

Welcome to MRTD

This is an updated version of the site that was developed in ICAO in order to serve the broad spectrum of persons in government agencies, industry and the public who are interested in our work in machine

On this site you will find information about our Technical Advisory Group, the latest versions of publications developed, MRTD-related worldwide events, news items, downloadable technical reports and a PDF version of this magazine. In the near future, users will be able to register and benefit from receiving a newsletter with the latest information on the worldwide development and implementation of ICAO MRTD-related standards and other services. Finally, this web site will also point to an industry community portal on MRTDs, which will provide industry information and reference in this area of expertise.

For more information please visit the web site at **http://mrtd.icao.int**

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 September 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 website at www.mrtd.icao.int, or by e-mail at sales@icao.int.	

VISOTEC® Expert 300 and VISOTEC® Expert 500

www.bundesdruckerei.de

Functionality	**Identifying and checking optical security features:** • Check number • Plausibility • Print pattern (e.g. line patterns, microlettering) • OVD structures • Security paper **Identifying and checking electrical security features:** • RF chip (ISO 14443)
Document database	• 120 countries • 650 international documents (e.g. passports, ID cards, visas).
Security methods	• Passive authentication • Active authentication • Basic Access Control • Extended Access Control
Illumination	• White light • IR • UV • Laser detector

► VISOTEC®

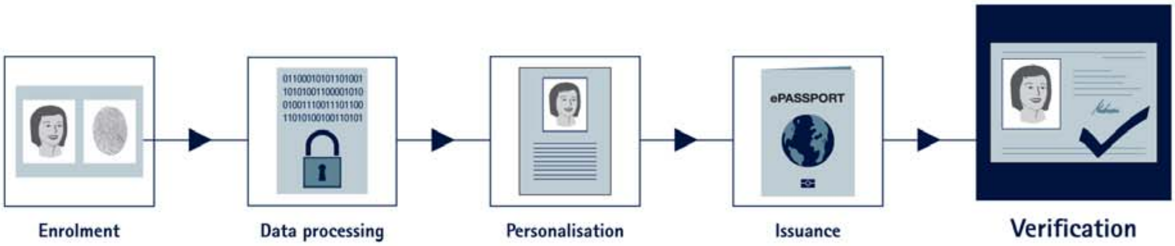
DOCUMENT CHECKING AT THE HIGHEST TECHNICAL LEVEL

► With its high-end document checking devices from the VISOTEC product family, Bundesdruckerei supplies reliable solutions for protection against identity fraud. The devices feature a document database that currently includes more than 650 international, machine-readable ID documents. Within a matter of seconds, a host of electrical and optical security features, such as print pattern or laser image, can be checked for a document placed on the device. This means more security, more convenience and much faster checking procedures every time.

Opt for VISOTEC and benefit from the technological experience and expertise of a leading international systems supplier! ◄

VISOTEC – Expertise serving security

BUNDESDRUCKEREI SYSTEM PORTFOLIO



Enrolment → Data processing → Personalisation → Issuance → **Verification**

BUNDES DRUCKEREI

The ICAO Public Key Directory (PKD) is Operational

by ICAO Secretariat

The ICAO PKD MoU

To complete the implementation of what is known as the "ICAO Blueprint" for the issuance of electronic Machine Readable Travel Documents (eMRTDs), Doc 9303, Part 1, Volume 2 specified the establishment of a Public Key Directory (PKD) under ICAO aegis. Last February, the ICAO Council gave its full support to the establishment of this key element by approving the final version of the *"Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory"* (the ICAO PKD MoU). This MoU has been effective since 8 March 2007, when the Secretary General received the fifth Notice of Participation required by Section 11.

During a brief ceremony at ICAO headquarters on 20 March 2007, the ICAO Secretary General presided the ribbon-cutting ceremony for the ICAO PKD Office. Shown on the occasion are (l-r) ICAO Secretary General Dr. Taieb Chérif and John Begin, Acting Director Air Transport Bureau.

Role of the PKD

The ICAO PKD is the main global distribution point for public signing key certificates from all issuers of ePassports who are required to validate and authenticate such documents. Inspectors of ePassports throughout the world will be able to access the PKD and use the public signing keys to validate ePassports in confidence. With this, they will be able to take full advantage, as intended, of the security provided by the new ePassport and biometrics ICAO standards and specifications being adopted for international travel.

Validating e-passports with trusted public keys prevents people from wrongfully crossing a border or 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.

This is a significant milestone in the development of ICAO standards and specifications and has been well received in ICAO as an asset, not only for border controls and passport security but for aviation security objectives as well.

The ICAO PKD Infrastructure

On 20 March 2007, the ICAO Secretary General presided over a ribbon-cutting ceremony inaugurating the ICAO PKD Office, culminating the development and implementation stage of this project. Several States have already become participants to the ICAO PKD MoU and have loaded their certificates onto this directory for public sharing.

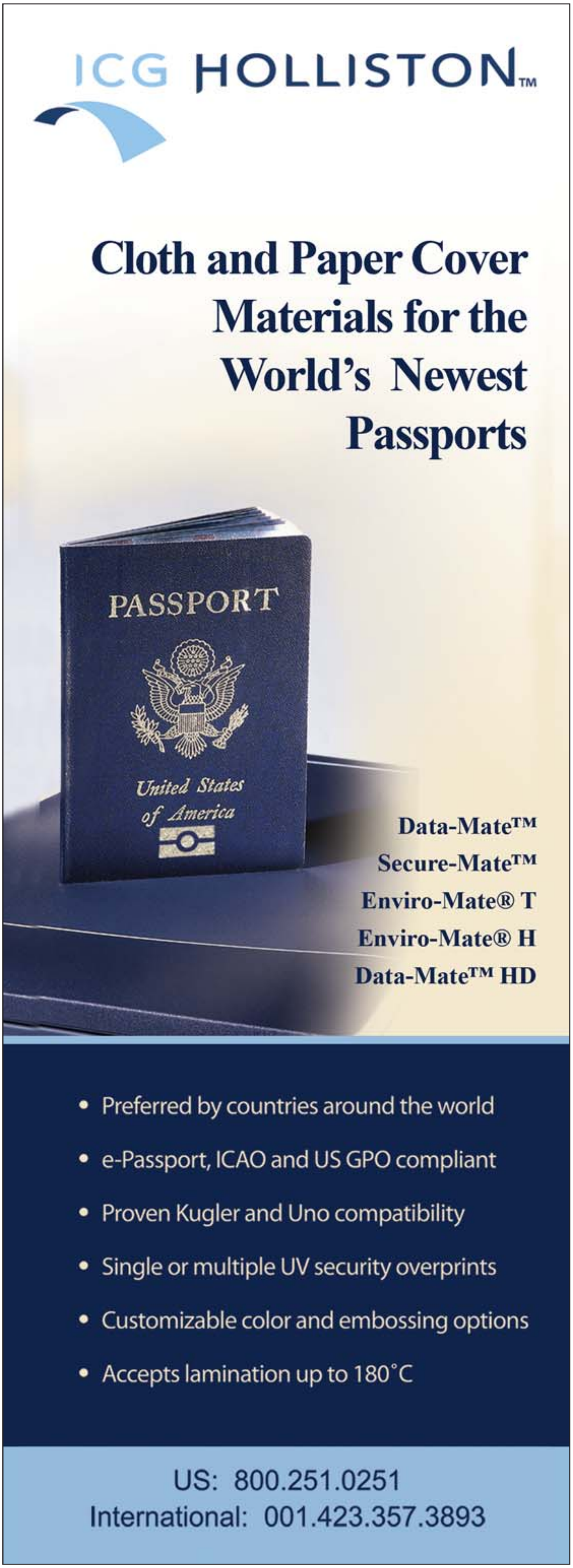
How to Participate in the ICAO PKD?

To participate in the ICAO PKD, States will have to take the following steps:

1. Review the information packet available in the MRTD web site, on the PKD infrastructure available, the business model and the security features built;
2. Complete and send to the ICAO Secretary General the Notice of Participation to the PKD MoU included in Attachment A of the ICAO PKD MoU. You will find a copy of the MoU in http://mrtd.icao.int under the menu "PKD";
3. Establish with the ICAO PKD Office the administrative arrangements necessary for paying the PKD Registration Fee as established in Attachment B of the ICAO PKD MoU. This can be done by way of an invoice, grant, contribution, etc;
4. Once payment is credited to ICAO's account, you will receive the required documentation for establishing communication with the ICAO PKD and performing the required tests;
5. Follow the ICAO PKD Procedures, which are found in http://mrtd.icao.int under the menu "PKD".

Visit our web site under the "PKD" menu.

References:
The following articles on the ICAO PKD have been published in the MRTD Report. You may download the full Acrobat version of each MRTD Report number from our web site: http://mrtd.icao.int, under "MRTD Report" menu.
1) *PKI and Public Key Directory – an ICAO programme for ePassport Security*, by David Clark; MRTD Report, Volume 1, Number 1, page 35.
2) *ePassports: Are we there yet?*, by Barry J. Kefauver; MRTD Report, Volume 1, Number 2, page 10.
3) *ePassports and the Implications of ICAO Standards*, by Simon Lofthouse; MRTD Report, Volume 1, Number 2, page 14. MS◆



Second Symposium on ICAO-Standard MRTDs, Biometrics and Security with Exhibition

by ICAO Secretariat

Report on the Second Symposium on ICAO-Standard MRTDs, Biometrics and Security with Exhibition

The Second Symposium on ICAO-Standard MRTDs and biometric enhancement was held on 6 and 7 September 2006 at ICAO Headquarters in Montreal. It was attended by over 550 participants from 65 ICAO Member States, twelve international organizations and more than 80 companies and institutions.

Opening Statement

The Symposium was opened by Dr Taïeb Chérif, Secretary General of ICAO who stated that he was pleased to showcase again the excellent work of ICAO and its Member States to improve the quality and integrity of passports and other travel documents worldwide. The emphasis given to this Symposium was on the issuance of ePassports that include biometric identification. He emphasized, however, that this in no way diminishes the importance of the conventional Machine Readable Passport, as the MRP will continue to be the baseline for secure travel documents. The vast majority of States already issue them and for those that need help to meet the prescribed deadline of April 2010, ICAO stands ready to offer technical and policy guidance, provide advice to the tender process; facilitate financing arrangements, manage a project, and perform quality checks on prototype documents. As always, security is considered a top priority and the universal implementation of MRTDs is one of the objectives of ICAO's Aviation Security Plan of Action.

Overview – MRTDs and Security

Mr. Barry Kefauver moderated the first session, which started with a *key address* from Mr. Jean-Michel Louboutin, Executive Director of Police Services, Interpol, who described the main activities and core functions of his organization to face the challenges in the fight against terrorism and international organized crime.

The following speaker was Mr. Jim Marriott, Director of Regulatory Affairs, Security and Executive Director, Security Review of Transport Canada, who made a presentation on the *World Aviation Security and MRTDs*, highlighting the work of ICAO Contracting States in strengthening security measures in response to the ICAO security programme, based on ICAO Annex 17 – Security and Annex 9 – Facilitation subject to ICAO Security Audits. It was also mentioned that MRTDs, biometrics and document reading systems form an essential part of aviation security, and the importance for an interdisciplinary approach to aviation security, border security and facilitation.

Next, Ms. Mary McMunn (former Chief, Specifications and Guidance Material Section, ICAO) gave a comprehensive *Overview of the ICAO MRTD Standards Development*. 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 TAG-MRTD in cooperation with ISO for the development of specifications for travel documents in ICAO Doc 9303 and Technical Reports. She also highlighted the benefits to the traveller of MRPs and eMRPs.

Then Mr. Joel Shaw, convenor of WG3 of the International Organization for Standardization (ISO) presented the effective *ICAO Partnership with ISO* and the industry in the development and publication of ICAO MRTD Standards and the endorsement as ISO Standards and how this cooperative process worked.

During the final presentation in this session, Mr. Gary McDonald, Director General, Policy and Planning, Passport Canada, explained the importance of implementing the ICAO *Standard Biometric ePassport* to enhance document security.

MRTDs, Issuance and Identity Management

The second session was moderated by Mr. Sjef Broekhaar. He introduced Mr. Malcolm Cuthbertson from DeLaRue Identity Systems who presented issues involving the issuance of *Basic MRTDs to Biometric ePassports.* Mr. Cuthbertson covered issues on standardization of document and data presentation, including size, shape, names, dates, layout, the visual reading of data page, machine readability (OCR B and IC Chip), ID confirmation of rightful holder and the importance of global interoperability. To enhance border processing, Doc 9303 Standards accommodate both manual and machine-assisted inspection.

Mr. Terry Hartmann, Director, Secure Identification & Biometrics, UNISYS, ISO, made a presentation on *Face Biometric Capture & Applications*, explaining that face recognition is the globally interoperable biometric for MRTDs, how it works, and how it can be effectively used to support document issuance, border control inspection, as well as access control and lookout checks. He highlighted the importance of quality capture of the face and the use of quality photographs in the enrolment process for documents and data bases.

A presentation on *MRP Data Security Features and Privacy* was made jointly by Dr Uwe Seidel, Senior Scientist, Forensic Science Institute, Bundeskriminalamt, Germany, and Tom Kinneging, Senior Project Manager, Sdu-Identification, ISO. Physical and digital security measures applied in the eMRTD complement each other to form a modern, machine-verifiable document which can be trusted by travellers and inspection authorities alike.

Mr. David Clark, Principal Consultant, Caicos Technologies, Inc. and Consultant to ICAO on PKD, presented the *ICAO Public Key Directory (PKD.)* Mr. Clark presented the elements conforming the ICAO PKD, including the Operations Office at ICAO Headquarters in Montreal, which will ensure that the PKD is properly updated. ICAO will also manage the policies, procedures, regulations and fee collection necessary for the PKD.

Finally, David Philp, Manager Passports, Identity Services, New Zealand, gave a presentation on *MRTD Issuance and Identity Management*. He presented elements of control processes such as checking persons, databases and lookout checks to ensure that passports are issued to the rightful holder. He presented a comprehensive approach to document security, application, enrolment and issuance to ensure security and identity management.

MRTD Implementation and States Experiences.

John Mercer, Senior Associate Kelly Anderson & Associates moderated this session, and introduced Barry Kefauver, Principal, Fall Hills

Associates, LLC., and Former Deputy Assistant Secretary of State for Passports, representing ISO, who made a presentation on *Recent Developments in eMRP Introduction*. With the publication of the Sixth Edition of Document 9303, Part 1, ICAO has upgraded the world's passports to a new level of travel document security, data integrity and identity management. Now, more than eleven years of hard multilateral work later, deployment has begun for what is considered to be the most secure passport the world has ever known.

Next, Sjef Broekhaar, Research and Development Manager, Personal Records and Travel Documents Agency, Ministry of Interior and Kingdom Relations, The Netherlands, presented the *International Forum for Travel Documents (IF4TD)*. Issuers of travel documents and identity cards now have a new vehicle for exchanging technical information and development news with their peers in other governments worldwide. Called the IF4TD, the International Forum for Travel Documents is an online discussion forum for issuing authorities across all regions of the world, and is accessible only to members.

Dr. Edgar Friedrich, Wissennschaftlicher Direktor, Bundeskriminalamt, Germany, presented the audience with *Germany's Experience in Issuing eMRPs*, and Staffan Tilling, Chief Superintendent, National Police Board, Police Bureau, Sweden, updated *Sweden's experience on Issuance of Official eID Documents*. Both emphasized the importance to their States and their citizens of issuing ICAO-Standard MRTDs in accordance with Doc 9303 for increased security, global interoperability and acceptance.

To conclude this Session, Mr. Chris Lyle, Representative of the World Tourism Organization (UNWTO) to ICAO presented the *Importance of MRTDs to International Tourism*. The UNWTO considers a harmonized world-wide systems approach for the efficient and secured border clearance of arriving international tourism to be essential. It therefore strongly supports ICAO-Standard MRPs, biometrics and eVisas as well as security provisions for improved facilitation and security for rapidly expanding new member of international tourist arrivals.

Border Control, Security and MRTDs

This session was moderated by Mr. Joel Shaw, and began with a presentation from Mr. Michel Oude Veldhuis, Head Expertise Center Identity Fraud and Documents, Royal Marenchausee, The Netherlands, on *Border Control Inspection – Document Verification and Fraud*. The presentation covered border control inspection of passengers travel documents, and the careful and systematic verification procedures implemented to detect document fraud and illegal entry to prevent human trafficking, drugs and terrorism.

Next, a presentation on *Border Control Inspection and Enhanced Identity Confirmation* was made by Mr. Charlie Stevens, Head of the National Document Fraud Unit, UK Immigration Service. He demonstrated the importance of ICAO-Standard MRPs and eMRPs to border control officials and the border crossing process. The new ICAO biometrics standards are a valuable tool in improving the security of the border control process, including airline pre-boarding checks and advance passenger data capture for control authorities (Advanced Passenger Processing - APP and Advanced Passenger Information - API).

Following this, Mr. Bradford Wing, Biometrics Systems and Standards Coordinator, U.S. Department of Homeland Security, gave a presentation on *Using MRPs in Support of Border*

Clearance. He outlined the US experience with the testing, introduction and use of equipment of capable secure and efficient reading of ePassports, basic MRPs and other travel documents in the primary inspection process at ports of entry.

Mr. Robert Davidson, Assistant Director, Facilitation Services, International Air Transport Association (IATA), in his a presentation on *Airline Contribution to Border Control*, stated that airlines are required to verify most passenger's travel documents at check-in, and again at point of boarding. They are also increasingly required to collect, confirm and transmit passenger data in support of governmental border control and security initiatives (APP & API). MRTDs have substantially reduced manual data entry, and new biometric eMRTDs will further increase the efficiency of these processes and border control. Specialized reading equipment is required and airlines must justify incorporating this in their increasingly automated passenger check-in processing systems.

Next, Mr. Yemmi Agdebi, Head of Group Business Development, Manchester Airports Group, United Kingdom, Airports Council International (ACI), made a presentation on *Airport Security and Biometrics*. He highlighted the wide range of security and passenger control measures and system in place at world airports implemented by government agencies, airports and airlines. These can be significantly enhanced by the use of ICAO-Standard MRTD biometrics to confirm personal identity for border control, airport passenger processing and airport access control, to improve security, efficiency and facilitation.

To conclude this session, Mr. Joel Shaw, Convenor of ISO W3, gave a *Concluding Summary Presentation* on the key features, benefits and advantages to States of introducing the MRTD system now as an essential part of national secu-

rity, as well as applying identity management and enhanced identity confirmation to other aviation security related processes in place at world airports and finally, the significant benefits offered to the traveller by the ICAO-Standard eMRPs. Mr Shaw encouraged States to implement the basic ICAO-Standard MRTD or the biometrically enhanced eMRTD now. MRTDs offer much greater levels of security to help deal with the increasing threats of identity theft, illegal migration, trafficking/smuggling and terrorism faced by States today.

Conclusion

Concluding Remarks were presented by Mr. Mohamed Elamiri, at the time of the Symposium, Director, Air Transport Bureau, ICAO, who concluded that the presentations from an outstanding team of experts had been most informative and that the Symposium had been very successful and met its objectives. He invited participants to attend the Workshop prepared for the next day, and thanked moderators, speakers, participants and exhibitors for a great job done. In conclusion, he announced that, following the success of this symposium, ICAO was planning to hold a third event in 2007 as well as two Regional Seminars on the subject.

Workshops

For this Symposium, two workshops were put together to allow participants take part of a round table questions and answers on particular matters.

One session on ePassports (eMRPs) was moderated by Mr. Gary McDonald, and focused on the technical issues of upgrading to ePassports. It provided an in-depth review of the new standard for machine-readable travel documents. This included an overview of the standard, followed by in-depth presentations on the choice of data storage, the type of data that can be stored and review of the biometric application. Two presentations were made: one on *Logical Data Structure* by Mr. Charles Baggeroer, President, FCB IIc, ISO; and another on *Biometric Selection*, made by Mr.Joel Shaw.

The other session was on the ICAO Public Key Directory (PKD), which was moderated by Mr. David Clark. This session explained the functions and usage of the ICAO PKD, which is the ICAO-supervised service for States' eMRPs. It covered what the PKD is about and how it will work, what border inspection authorities and airlines need to know about the PKD, how to sign up as a participant and the interface procedures and specifications. It also explained user procedures, including how to download and use the PKD in an inspection system. This session consisted of two presentations and two commentaries. The two presentations were made by Mr. Daniel Walsh, Managing Director, Total-Trust Solutions Ltd. on *Reading ePassports and the Role of the PKD. What can go Wrong?* The Second presentation was made by Mr. R. Rajeshkumar, Director Business Development, Netrust Pte Ltd. on *Download and distribution of the PKD. Optional re-verification against CA Keys? Applications decisions.*

The commentaries were made by Mr. Mauricio Siciliano, Technical Officer, SGM Section, ICAO on *PKD Registration, Location, Operation and Timetable*; and by Mr. Robert Davidson on *Essential Role of the PKD in Airline's ability to respond to National Border Control Legislation, Future Needs for Effective Global Policy and Enhanced Public-Private Sector Cooperation.*

Information on the ICAO MRTD programme and Standard specifications may be found on the ICAO website: www.mrtd.icao.int MS ◆

Efficient data capture important in implementation of national e-passports in Sweden

In 2003 the Swedish Police Board was given the task by the Swedish government to prepare for the implementation of national passports with biometric information.

An entirely new system demanded new solutions

When the Swedish Police Board was given the task, they decided not only to look at making the passports comply with the new EU directives, but also to make the application process both more efficient and more secure. There were also current international standards to comply with, including ICAO's (International Civil Aviation Organization) standard for photo quality and biometric information in passports. As a result, the Swedish Police Board decided to create a whole new system to manage the entire application process. One important component in the new system was the Capture Station.

After outlining the requirements of the Capture Station, a number of companies were invited to participate in the public purchasing as a supplier according to Swedish law. Included in the requirements from the Swedish Police Board was that the Capture Station had not only to be prepared for facial biometrics, but also for other types of biometric data capture like fingerprints as per forthcoming EU directives. A security requirement was that the passport photo needed to be directly connected to the application and the whole process would be monitored by the administrative official. There was also a strong demand that every applicant should be able to use the Capture Station, meeting the needs of children, adults and people in wheelchairs. The photos also had to be of much higher quality than before.

These features tailored how the Capture Station would operate and the company Speed Identity provided the only solution which met the requirements outlined by the Swedish Police Board. The Capture station, *Speed Capture* provided by Speed Identity is a both that captures the biometric data digitally. Thanks to this method an intact digital chain is created where the image transfers directly from the camera into the system and the process decreases the risk of image manipulation. "Even though it is technically possible to obtain this information when you take a photo and scan it into the system, it is of insufficient quality. The new system is also more secure since the administrative official monitors the whole process", says Lars Karlsand, head of the department at the Swedish Police Board.

The Capture Station supports all of the required standards; ISO-19794-5 for biometric facial recognition and ISO-19794-4 for fingerprints. Thereby the Capture Station complies with all requirements demanded by American authorities in the US Visa Waiver and the new EU directives for travel documents. All the peripheral equipment is maintained inside the Capture Station, which results in a simple IT environment. The Capture Station is easy to connect to different types of systems and at the same time makes updates and support easy to handle.

The result

With more than a year of the new process in place, there has not been any special problems reported except for normal maintenance of the Capture Stations. Because Speed Identity owns the units they control any potential support and maintenance issues. "There are very clear advantages with the use of support and maintenance. We have an optimal deal where Speed Identity is responsible for the entire photo process. In the few cases when we have needed support we have received it quickly", says Thomas Wahlberg, project leader at the Swedish Police Board.

About Speed Identity

Speed Identity AB is an innovative, Swedish family owned technology development company that supplies market leading biometric solutions for data capture to public authorities and companies. All development of hardware and software is made within the company. We are ISO certified (SS-EN ISO 9001) and have worked in the field of passport and identification photography since the company was founded by the Caspar family in 1956. During the past 10 years we have supplied more than 15 million photos used for passports and identification. Speed Identity is part of the Speed Identity Group, which is a rapidly expanding group of international companies with subsidiaries in Norway, Denmark, Finland, Estonia and Latvia. Speed Identity's customers: The Swedish National Police Board, Swedish National Road Administration, Swedish Migration Board and Estonian Road Authorities.

SPEED IDENTITY®
www.speed-identity.com

Why ICAO Selected the Face as Primary Biometric Identifier specified to ePassports

by ICAO Secretariat

It has long been recognized that names and honour are not sufficient to guarantee that the holder of an identity document (such as a Machine Readable Passport - MRP) assigned to that person by the issuing State is guaranteed to be the person purporting, at a receiving State, to be the same person to whom that document was issued.

The only method of relating a person irrevocably to his travel document is to have a physiological characteristic of that person associated with the travel document in a tamper-proof manner. This physiological characteristic is a biometric.

After a five-year investigation into the operational needs for a biometric identifier which combines suitability for use in the MRP issuance procedure and in the various processes in cross-border travel consistent with the privacy laws of various States, ICAO has specified that facial recognition shall become the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

In reaching this conclusion, ICAO observed that for the majority of States the following advantages applied to facial images:

- Facial photographs do not disclose information that the person does not routinely disclose to the general public.
- The photograph (facial image) is already socially and culturally accepted internationally.
- The facial image is already collected and verified routinely as part of the MRP application form process in order to produce a passport to Doc 9303 standards.
- The public is already aware of the capture of a facial image and its use for identity verification purposes.
- The capture of a facial image is non-intrusive. The end user does not have to touch or interact with any physical device for a substantial timeframe to be enrolled.
- Facial image capture does not require new and costly enrollment procedures to be introduced.

- Capture of a facial image can be deployed relatively immediately, and the opportunity to capture facial images retrospectively is also available.

- Many States have a legacy database of facial images captured as part of the digitized production of passport photographs which can be encoded into facial templates and verified for identity comparison purposes.

- In appropriate circumstances, as decided by the issuing State, a facial image can be captured from an endorsed photograph, not requiring the person to be physically present.

- For watch lists, a photograph of the face is generally the only biometric available for comparison.

- Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.

Optional additional biometrics

States can optionally provide additional data input to their (and other States) identity verification processes by including multiple biometrics in travel documents, i.e. a combination of face and/or fingerprint and/or iris. This is especially relevant where States may have existing fingerprint or iris databases in place against which they can verify the biometrics proffered to them; for example, as part of an ID card system.

Storage of an optional fingerprint biometric

There are three classes of fingerprint biometric technology: finger image-based systems, finger minutiae-based systems, and finger pattern-based systems. Whilst standards have been developed within these classes to make most systems interoperable amongst their class, they are not interoperable between classes. Three standards for fingerprint interoperability are therefore emerging: storage of the image data, storage of the minutiae data and storage of the pattern data. Where an issuing State elects to provide fingerprint data in its ePassport, the storage of the fingerprint image is mandatory to permit global interoperability between the classes. The storage of an associated template is optional at the discretion of the issuing State.

Storage of an optional iris biometric

Iris biometrics are complicated by the dearth of proven vendors. A de facto standard for iris biometrics has therefore emerged based on the methodology of the one recognized vendor. Other vendors may in future provide iris technology, but it is likely they will need the image of the iris as their starting point, rather than the template created by the current vendor. Where an issuing State elects to provide iris data in its ePassport, the storage of the iris image is mandatory to permit global interoperability. The storage of an associated template is optional at the discretion of the issuing State.

For more on this issue, please see ICAO Doc 9303 Part 1, Volume 2 sixth edition. ◆

The Biometric Identification for use with ICAO-Compliant Machine Readable Travel Documents

by ICAO Secretariat

"Biometric identification" is a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.

A "biometric template" is a machine-encoded representation of the trait created by a computer software algorithm and enables comparisons (matches) to be performed to score the degree of confidence that separately recorded traits identify (or do not identify) the same person.

Key considerations when applying biometric specifications in MRPs

- *Global Interoperability* — the crucial need to specify a system for biometrics deployment that is universally interoperable;
- *Uniformity* — the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States;
- *Technical reliability* — the need to provide guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them are of sufficient quality and integrity to enable accurate verification in their own systems;
- *Practicality* — the need to ensure that specifications can be operationally and implemented by States without having to introduce a plethora of disparate systems and equipment to ensure that all possible variations and interpretations of the standards are met;
- *Durability* — the requirement that the systems introduced will last the maximum 10-year life of a travel document, and that future updates will be retroactively compatible.

Typically, a biometric template is of relatively small data size; however, each manufacturer of a biometric system uses a unique template format, and templates are not interchangeable between systems.

Doc 9303 Part 1, Volume 2 (Sixth Edition) considers only three types of biometric identification systems. These are the physiological ones of:

- facial recognition (mandatory)
- fingerprint (optional)
- iris recognition (optional)

An international standard, ISO/IEC 19794 composed of several parts, provides specifications for these types of biometric identification. Issuing States shall conform to these specifications. For more information on ISO standards, please visit the ISO web site: http://www.iso.org.

The following terms are used in relation to biometric identification:

- *"verify"* means to perform a one-to-one match between proffered biometric data obtained from the Machine Readable Passport (MRP) holder now and a biometric template created when the holder enrolled in the system;
- *"identify"* means to perform a *one-to-many* search between proffered biometric data and a collection of templates representing all of the subjects who have enrolled in the system.

Biometrics can be used in the *identification function* to improve the quality of the background checking performed as part of the passport, visa or other travel document application process. In the *verification function*, they can be used to establish a positive match between the travel document and the person who presents it.

State applications for a biometrics solution

The key applications of a biometrics solution are the identity verification of relating an MRP holder to the MRP he is carrying.

There are typical applications for biometrics during the enrolment process of applying for an MRP, and in performing border control functions.

The typical applications for biometrics during the enrolment process of applying for an MRP are:

- The end user's biometric data generated by the enrollment process can be used in a search of one or more biometric databases (identification) to determine whether the end user is known to any of the corresponding systems (for example, holding a passport under a different identity, having a criminal record, holding a passport from another State).
- When the end user collects the passport or visa (or presents himself for any step in the issuance process after the initial application is made and the biometric data are captured) his biometric data can be taken again and verified against the initially captured biometric data.
- The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

There are also several typical applications for biometrics at the border.

- Each time a traveller (i.e. MRP holder) enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any advance passenger information (API) system. Ideally, the biometric template or templates should be stored on the travel document along with the

image, so that a traveler's identity can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.

- *Two-way check* — The traveller's current captured biometric image data, and the biometric template from his travel document (or from a central database), can be matched to confirm that the travel document has not been altered.

ICAO vision on biometrics

The ICAO vision for the application of biometrics technology encompasses:

— specification of a primary interoperable form of biometrics technology for use at border control (verification, watch lists) as well as by carriers and document issuers and specification of agreed supplementary biometric technologies;

— specification of the biometrics technologies for use by document issuers (identification, verification and watch lists);

— capability of data retrieval for a maximum ten-year validity, as specified in Doc 9303;

— having a no proprietary element to ensure that any States investing in biometrics are protected against changing infrastructure or suppliers.

- *Three-way check* — The traveller's current biometric image data, the image from his travel document, and the image stored in a central database can be matched (by constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person with his passport and with the database recording the data that were put in that passport at the time it was issued.

- *Four-way check* — A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the three-way check with the digitized photograph on the data page of the traveller's passport.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States should also set their own criteria in regard to:

— Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint or iris biometrics on the MRP as per LDS specifications. (It may also be stored on a database accessible to the receiving State). Given an ICAO-standardized biometric image, receiving States must select their own biometric verification software and determine their own biometric scoring thresholds for identity verification acceptance rates — and referral of impostors.

— Throughput (e.g. travellers per minute) of either the biometric system or the border-crossing system as a whole.

— Suitability of a particular biometric technology (face or finger or eye) to the border-crossing application.

Key processes with respect to biometrics

The major components of a biometric system are:

Capture — acquisition of a raw biometric sample
Extract — conversion of the raw biometric sample data to an intermediate form
Create template — conversion of the intermediate data into a template for storage
Compare — comparison with the information in a stored reference template.

These processes involve:

- The *enrolment* process is the capture of a raw biometric sample. It is used for each new person (potential MRP holder) taking biometric samples to establish a new template. This capture process is the automatic acquisition of the biometric via a capture device such as a fingerprint scanner, photograph scanner, live-

Facial recognition vendors all use proprietary algorithms to generate their biometric templates. These algorithms are kept secret by the vendors as their intellectual property and cannot be reverse-engineered to create a recognizable facial image. Therefore, facial recognition templates are not interoperable between vendors — the only way to achieve interoperability is for the "original" captured photograph to be passed to the receiving State. The receiving State then uses its own vendor algorithm (which may or may not be the same vendor/version as used by the issuing State) to compare a facial image captured in real time of the MRP holder with the facial image read from the data storage technology in itsr MRP.

capture digital image camera, or live-capture iris zooming camera. Each capture device will need certain criteria and procedures defined for the capture process — for example, standard pose facing the camera straight-on for a facial recognition capture; whether fingerprints are captured flat or rolled; eyes fully open for iris capture.

- The *template creation* process preserves the distinct and repeatable biometric features from the captured biometric sample and is generally done with a proprietary software algorithm to extract a template from the captured image, which defines that image in a way that it can subsequently be compared with another captured image and a comparative score determined. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. Quality standards need to be as high as possible since all future checks are dependent on the quality of the originally captured image. If the quality is not acceptable, the capture process should be repeated.

- The *identification* process takes new samples and compares them to saved templates of enrolled end users to determine whether they have been enrolled in the system before and, if so, whether under the same identity.

- The *verification* process takes new samples of an ePassport holder and compares them to previously saved templates of that holder, to determine whether the holder is presenting himself/herself under the same identity.

Constraints on biometrics solutions

It is recognized that implementation of most biometrics technologies is subject to further (rapid) development. Given the rapidity of technological change, any specifications (including those herein) must recognize and allow for changes resulting from technology improvements.

The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State.

For more on this issue, please see ICAO Doc 9303 Part 1, Volume 2 (sixth edition).◆

Facial Biometric Digital Images to be stored in a Radio Frequency Integrated Circuit (RFIC)

by ICAO Secretariat

The ICAO Blueprint contemplates the use of digital images of the biometric features, the primary being the face, with the fingerprint or iris being the secondary, and that such images be "on-board," i.e. electronically stored in the travel document. Such image or images, depending on the number of biometric features chosen, will have to be placed in the Radio Frequency Integrated Circuit (RFIC) or chip, which is the variable size data item that has the most impact on the Logical Data Structure (LDS) size. However, the next question becomes "to what level can the image be compressed by the issuing State without degrading the results of biometric comparison by the receiving State?"

Biometric systems reduce the raw acquired image (face/fingerprint/iris) to a feature space that is used for matching — it follows that as long as compression does not compromise this feature space, it can be undertaken to reduce the storage requirements of the images retained.

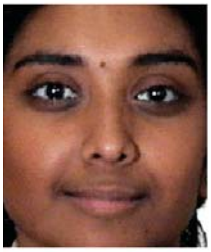
Facial image data size

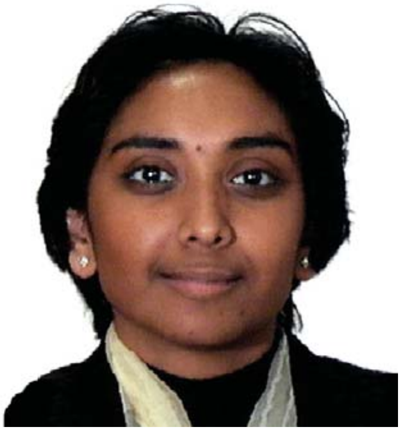
An ICAO standard-size portrait colour-scanned at 300 dpi results in a facial image with approximately 90 pixels between the eyes and a size of approximately 643 K (kilobytes). This can be reduced to 112 Kb with very minimal compression.

Studies undertaken using standard photograph images but with different vendor algorithms and JPEG and or JPEG2000 compression, showed the minimum practical image size for an ICAO standard passport photo image to be approximately 12 Kb of data. The studies showed higher compression beyond this size results in significantly less reliable facial recognition results. Twelve kilobytes cannot always be achieved as some images compress more than others at the same compression ratio — depending on factors such as clothes, colouring and hair style. In practice, facial image average compressed sizes in the 15 K – 20 K range is the optimum for use in ePassports.

Cropping

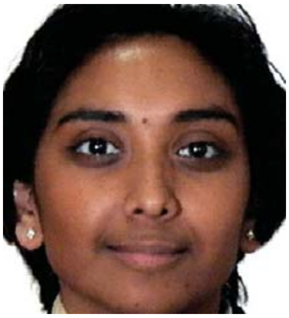
While images can be cropped to save storage and show just the eye/nose/mouth features, the ability for a person to easily verify that image as being the same person who is in front of him/her, or appearing in the photograph in the data page of the passport, is diminished significantly. For example, the image to the left provides a greater challenge in recognition than that on the right.





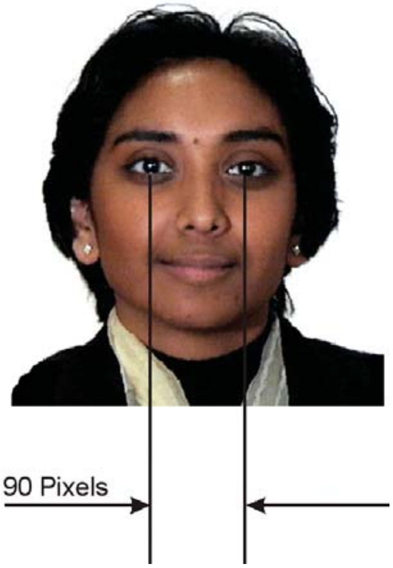
It is therefore recommended that images stored in the LDS are to be either:

- not cropped, i.e. identical to the portrait printed on the data page; or
- cropped from chin to crown and edge-to-edge as a minimum, as shown below.



To assist in the facial recognition process, the facial image shall be stored either as a full frontal image or as a token image in accordance with the specifications established in ISO/IEC 19794-5. A token image is a facial image in which the image is rotated if necessary to ensure that an imaginary horizontal line drawn between the centers of the eyes is parallel to the top edge of the picture and the size adjusted. ICAO recommends that the centres of the eyes be approximately 90 pixels apart as in the following illustration.

Original image



Token image (angled and resized)

The Logical Data Structure (see Section III Doc 9303 Part 1, Volume 2) can accommodate the storage of the eye coordinates.

Finally, regarding *facial ornaments,* the issuing State shall decide to what extent it permits them to appear in stored (and displayed) portraits. In general, if such ornaments are permanently worn, they should appear in the stored image.

For more information, please see Doc 9303 Part 1, Volume 2 (sixth edition). ◆

EDAPS

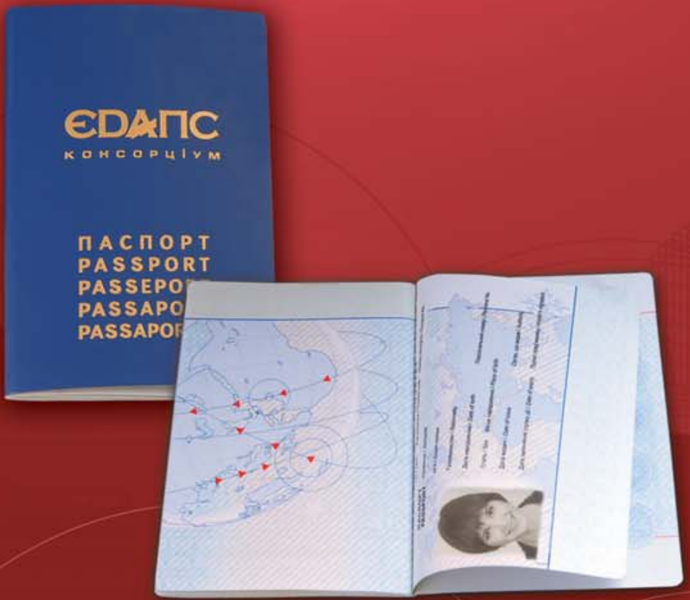
CONSORTIUM

PASSPORT

Passport differentiated by various booklet construction approaches.
Centralized personalization utilizing laser engraving and perforation insures maximum protection against counterfeiting and falsification.
The combination of contemporary materials and new technology, utilized during document personalization, insures that all of today's standards set for travel documents are fully met.

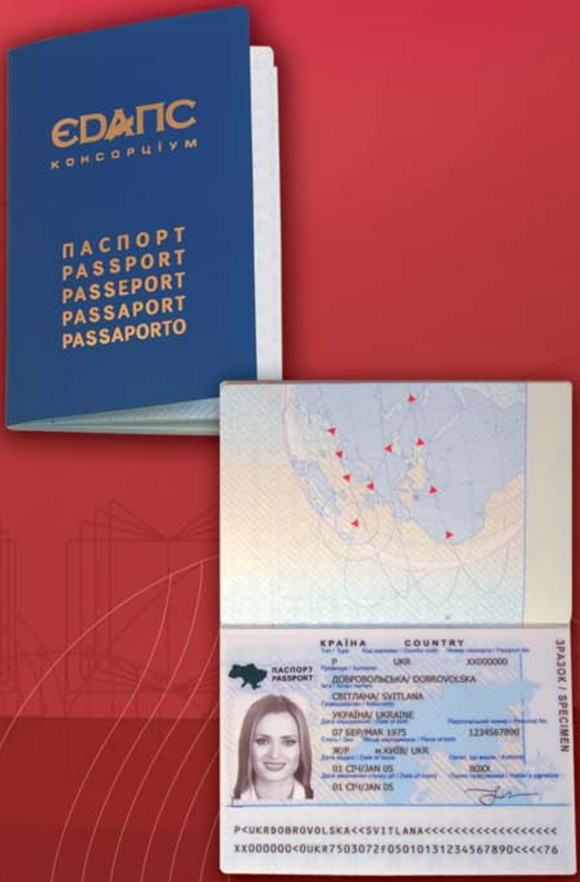
PASSPORT WITH A DATA PAGE INSIDE THE PASSPORT BOOKLET

A machine readable passport, where the data page is located on the first paper page of the booklet. After the data is entered by printer, both sides of the page are laminated by a special security film, preventing its separation from the surface of the material that contains the information.



PASSPORT WITH A DATA PAGE COMPRISED OF MANY - LAYERED POLYCARBONATE

A machine-readable passport, with a polycarbonate data page, placed between the inside left cover and the first paper page of the passport. Data is laser engraved on a polycarbonate sheet on the inside of the sandwich. The facial image of the holder is duplicated on the data page by laser perforation.



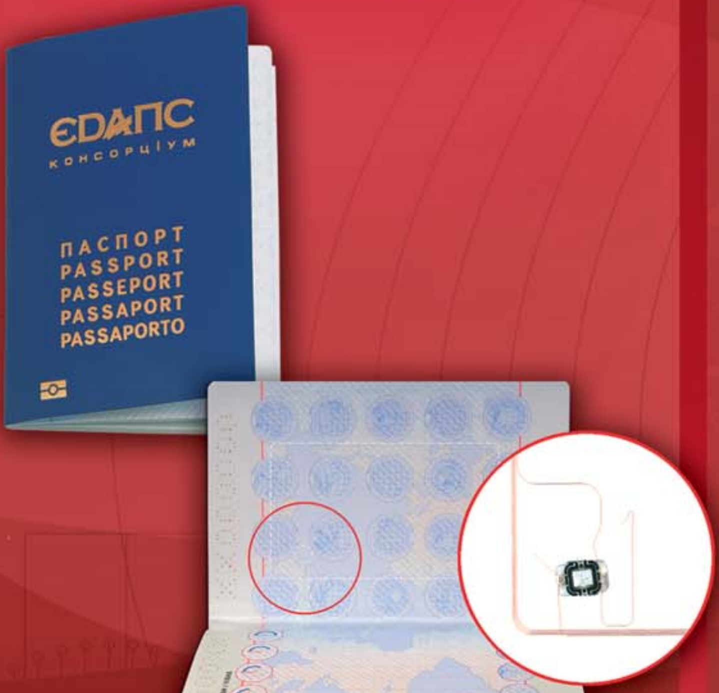
EDAPS CONSORTIUM - PROVIDING A COMPLETE SELECTION OF IDENTIFICATION DOCUMENTS UTILIZING THE LATEST TECHNOLOGY. DEVELOPMENT AND IMPLEMENTATION OF INTEGRATED SYSTEMS FOR PRODUCTION OF IDENTIFICATION DOCUMENTS, INCLUDING PASSPORTS, UTILIZING STATE OF THE ART TECHNOLOGY. DELIVERING THOSE SYSTEMS TO CLIENTS ON A «TURNKEY» BASIS.

The EDAPS Consortium:

Development and manufacturing of passport and other identity documents utilizing the most advanced technologies.

ELECTRONIC PASSPORT WITH A DATA PAGE COMPRISED OF MANY - LAYERED POLYCARBONATE

A machine-readable passport, with a polycarbonate data page, placed between the inside left cover and the first paper page of the passport. The passport contains a contactless microchip with a capacity of 72 kb, embedded into the lower part of the cover.



PASSPORT WITH A DATA PAGE ON THE INSIDE OF THE COVER

A machine readable passport where the data page is located on the left inside of the cover. After the required data about the passport holder is entered by printer, the page is laminated with a special security film, preventing its separation from the surface of the material containing the information.

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

CONTACT US TO LEARN MORE!

Address:
64, Lenina Str.
Kiev, Ukraine, 02088

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

Fax:
+38 (044) 561 2585

E-Mail:
edaps@edaps.biz

WWW:
http://www.edaps.biz

Illustrative Guidelines for Portraits in a Machine Readable Travel Document (MRTD)

by ICAO Secretariat

The main biometric feature in Machine Readable Passports (MRPs) is the portrait of the holder. Taking a good picture or acquiring a good image that could serve the purpose of identifying the holder is required. In view of standardizing the production of quality picture or images, ICAO has included the following Illustrative Guidelines for Portraits to be used in an MRP or any other Machine Readable Travel Document (MRTD).

The illustrations on the following pages provide guidance for the taking of photographs to be used as the portrait of the holder in an MRP contained in Appendix 11 to Section IV of Doc 9303 Part 1, Volume 1 sixth edition), and should be viewed in relation to Section IV, 7 – Displayed Identification Feature(s) of the Holder.

Finally, in the pages that follow, you will find examples of portrait quality, style and lighting, the use of glasses and head covers, and the expression and how to frame an image.

1. Pose

1.1. The photograph shall be less than six months old.

1.2. It should show a close up of the head and shoulders.

1.3. The photograph should be taken so that an imaginary horizontal line between the centres of the eyes is parallel to the top edge of the picture.

1.4. The face should be in sharp focus and clear with no blemishes such as ink marks or creases.

1.5. The photograph should show the subject facing square on and looking directly at the camera with a neutral expression and the mouth closed.

1.6. The chin to crown (crown is the position of the top of the head if there were no hair) shall be 70 to 80 per cent of the vertical height of the picture.

1.7. The eyes must be open with no hair obscuring them.

1.8. If the subject wears glasses, the photograph must show the eyes clearly with no lights reflected in the glasses. The glasses shall not have tinted lenses. Avoid heavy frames if possible and ensure that the frames do not cover any part of the eyes.

1.9. Coverings, hair, headdress or facial ornamentation which obscure the face are not permitted.

1.10. The photograph must have a plain, light-coloured background.

1.11. There must be no other people or objects in the photograph.

PORTRAIT QUALITY

The portrait shall be not more than 6 months old.

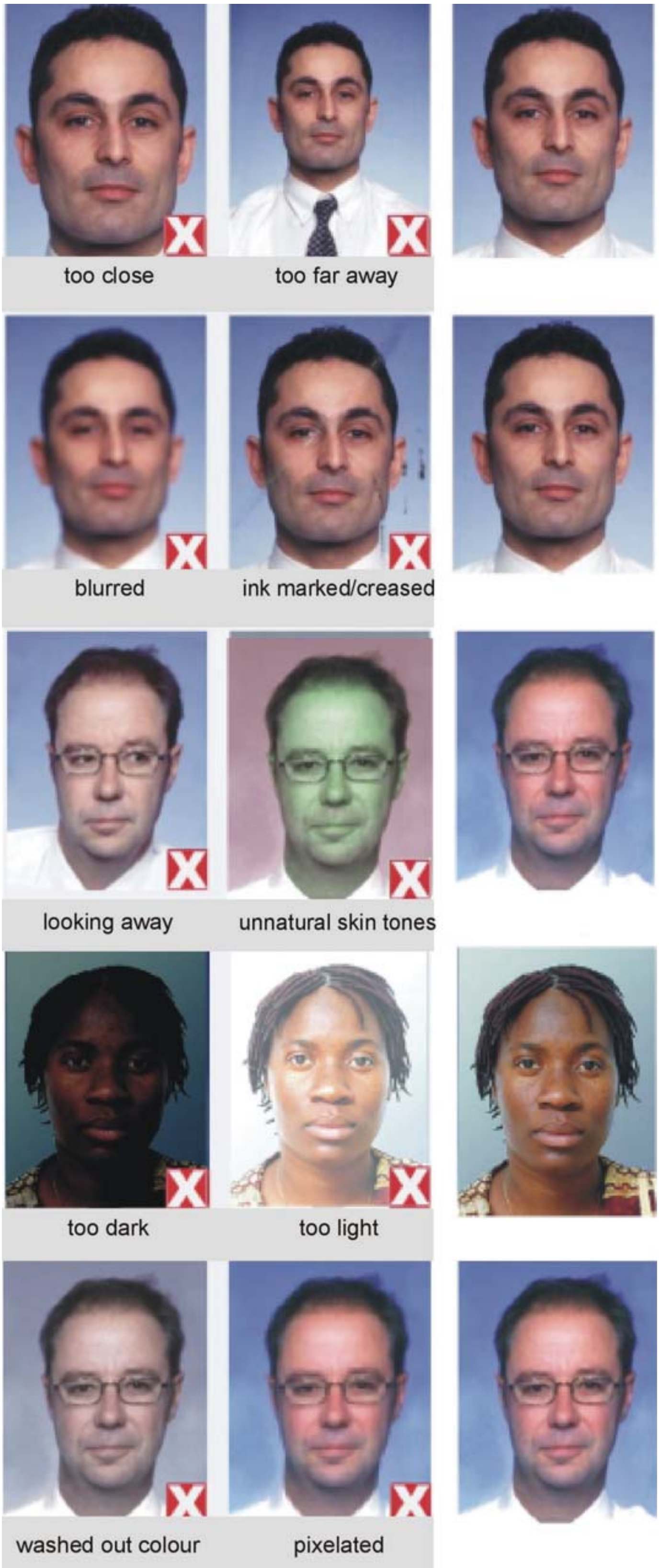
It shall not be larger than 45 x 35mm (1.77 x 1.38 in) nor smaller than 32 x 26 mm (1.26 x 1.02 in) in height and width and show a close-up of the applicant's head and the top of the shoulders. The face shall take up 70-80 per cent of the vertical dimension of the picture.

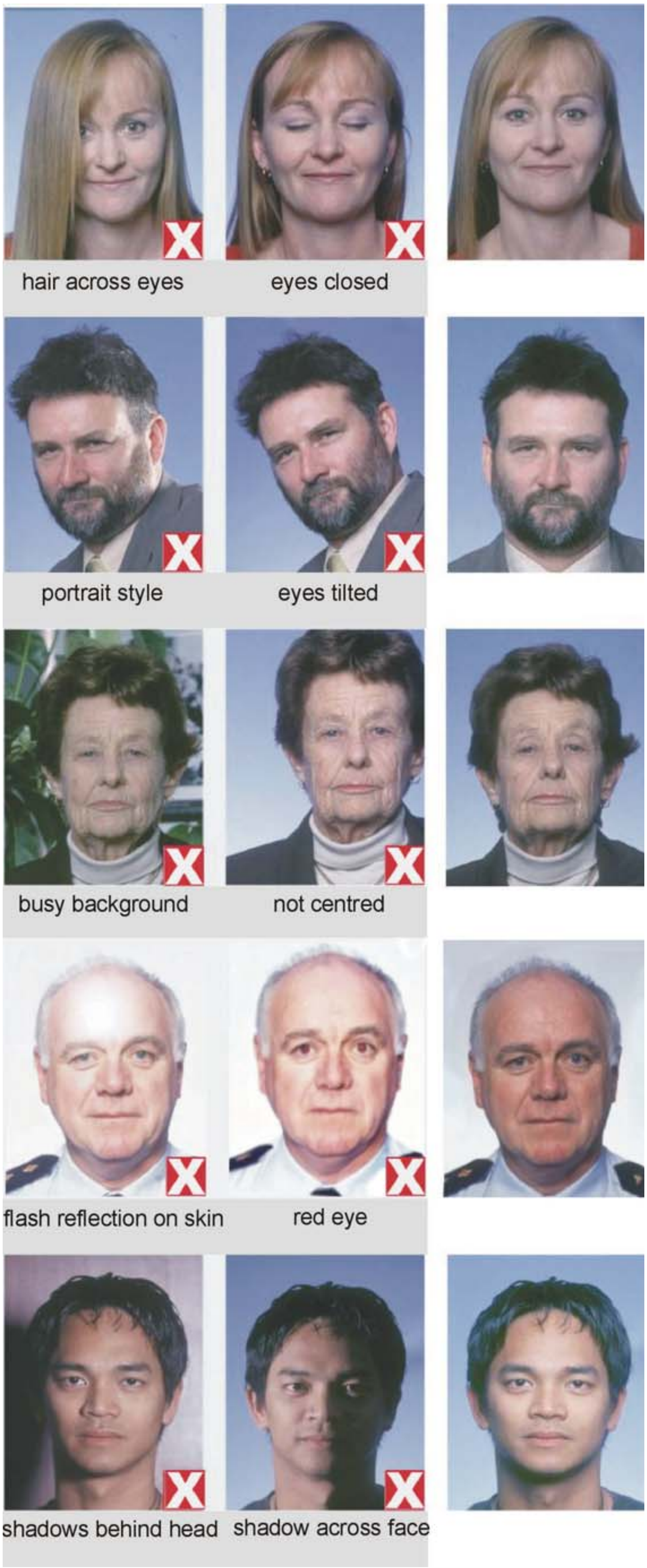
The portrait shall be in sharp focus, of high quality with no creases or ink marks.

The portrait shall show the applicant looking directly at the camera. It should have appropriate brightness and contrast. If in colour, it should show skin tones naturally.

If submitted as a print, it should be on high quality paper with high resolution.

Portraits taken with a digital camera should be at high quality and resolution and be printed on photo-quality paper.





hair across eyes

eyes closed

portrait style

eyes tilted

busy background

not centred

flash reflection on skin

red eye

shadows behind head

shadow across face

2. Lighting, exposure and colour balance

2.1 The lighting must be uniform with no shadows or reflections on the face or in the background.

2.2 The subject's eyes must not show red eye.

2.3 The photograph must have appropriate brightness and contrast.

2.4 Where the picture is in colour, the lighting and photographic process must be colour balanced to render skin tones faithfully.

STYLE AND LIGHTING

The portrait shall be colour neutral showing the applicant with the eyes open and clearly visible; there shall be no hair obscuring the eyes. The applicant shall be shown facing square to the camera, not looking over one shoulder (portrait style).

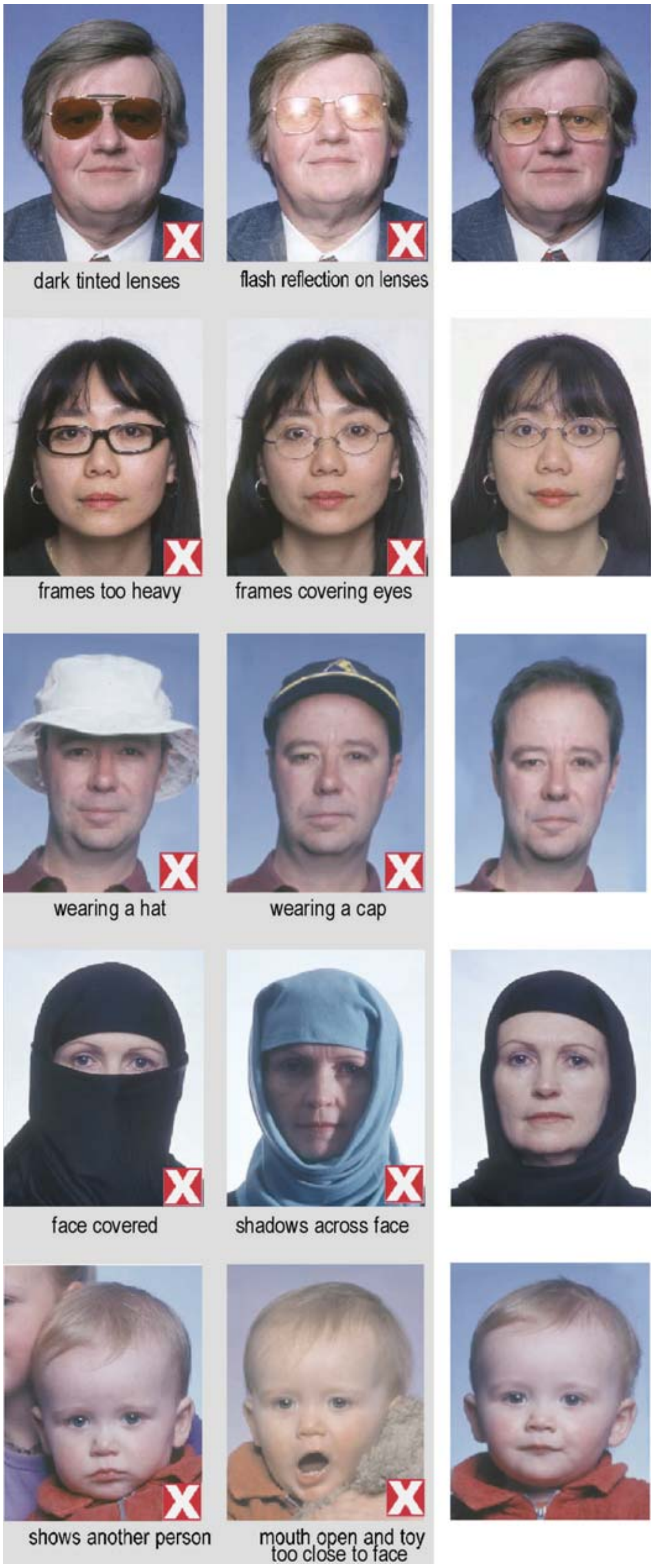
The head should be upright so that an imaginary horizontal line drawn between the centres of the eyes is parallel to the top edge of the picture.

Both edges of the face shall be clearly visible.

The background shall be plain and light coloured.

The lighting shall be uniform with no shadows and no reflections on the face.

There shall be no red eye.



3. Submission of portrait to the issuing authority

3.1 Where the portrait is supplied to the issuing authority in the form of a print, the photograph, whether produced using conventional photographic techniques or digital techniques, should be on good or photo-quality paper and should be of the maximum specified dimensions.

3.2 Where the portrait is supplied to the issuing authority in digital form, the requirements specified by the issuing authority must be adhered to.

4. Compliance with international standards

4.1 The photograph shall comply with the appropriate definitions set out in ISO/IEC 19794-5.

GLASSES AND HEAD COVERS

Glasses:
The portrait shall show the eyes clearly with no light reflection off the glasses and no tinted lenses. If possible, avoid heavy frames. The frames shall not cover any part of the eyes.

Head Coverings:
Head coverings shall not be accepted except in circumstances which the competent State authority specifically approves. Such circumstances may be religious, medical or cultural.

EXPRESSION AND FRAME

The portrait shall show the applicant alone with no other people, chair backs or toys visible. The applicant shall be looking at the camera with a neutral expression and the mouth closed. ◆

Extended Access Control: the impact of the EU implementation

by Peter Buck,
Temporal S. Limited

The next generation of ePassports issued in compliance with ICAO specifications will include biometric data to which access needs to be controlled. While the ICAO specifications[1] define authentication mechanisms and *Basic Access Control* (BAC) to protect the privacy of embedded data, *Extended Access Control* (EAC), intended to protect sensitive biometric data, is undefined. As a result, it is left to individual States or regions to produce their own specification for an implementation of EAC.

The European Union (EU) has developed a set of protocols[2] to implement EAC which extend the underlying inter-operable Public Key Infrastructure (PKI) that participating States must employ. The design of the protocols and the PKI elements upon which they are predicated has significant operational implications for EU States and any other States that wish to be able to obtain access to the EAC-protected data on an ePassport issued by an EU State. All EU States' Issuing Authorities are required[3] to issue ePassports using EAC to protect fingerprint images by 28th June 2009. The EU specification may be adopted by some non-EU States, while other States or regional groups of States may specify their own EAC mechanisms using similar processes and protocols or significantly different alternatives.

Authentication

There are two mechanisms for authenticating an ePassport when it is being inspected. *Passive Authentication* is mandatory and authenticates the data that is read from the ePassport by validating the signature of that data, using the appropriate Public Key certificates from the Issuing State.; to this end some elements of an inter-operable Public Key Infrastructure must be in place. *Active Authentication* is optional and may be used to verify that the chip itself is genuine. In either case the data read optically from the Machine Readable Zone (MRZ) is compared with the data read from the chip to ensure that they match, confirming that it is the correct chip for that passport.

Access Control

Access control is intended to protect the privacy of data stored on the ePassport chip. *Basic Access Control* is recommended for all access to the ePassport, while *Extended Access Control* is intended to protect sensitive biometric data. Both can be enforced by the chip.

Basic Access Control

Basic Access Control enables an inspection system to read the data from the chip only if it proves it has physical access to the Passport, using a challenge-response protocol including data from the optically read MRZ, thus preventing skimming; cryptographic session keys are generated enabling subsequent data communications between the chip and the inspection system to be encrypted by *Secure Messaging* to protect against eavesdropping.

Extended Access Control

Extended Access Control is intended to restrict access to sensitive data to inspection systems that can prove they know the specific key for that particular passport in a challenge-response protocol. Unlike BAC the key cannot be derived solely from the MRZ and requires prior knowledge of other information. ICAO also suggests that instead of EAC, States can choose to encrypt the sensitive data.

The EU implementation of EAC

The EU specified Extended Access Control mechanism adopts an approach that entails each inspection system being specifically authorized to have access to EAC-protected passports from each State and being able to prove its authorization to the ePassport itself. It introduces additional certificates and another hierarchy of Certification Authorities over and above those defined in the ICAO specifications to support Passive Authentication. This enables the ePassport to authenticate an Inspection System and determine that the system is authorized to read its sensitive data.

There are two distinct steps, *Chip Authentication* which is mandatory for all access to EU EAC-protected ePassports from EAC authorized inspection systems; and *Terminal Authentication* which is mandatory when the inspection system requires access to the sensitive data. Where an ePassport containing EAC-protected sensitive data is read by a non-authorized Inspection System, Basic Access Control may be enforced by the chip but sensitive data cannot be read.

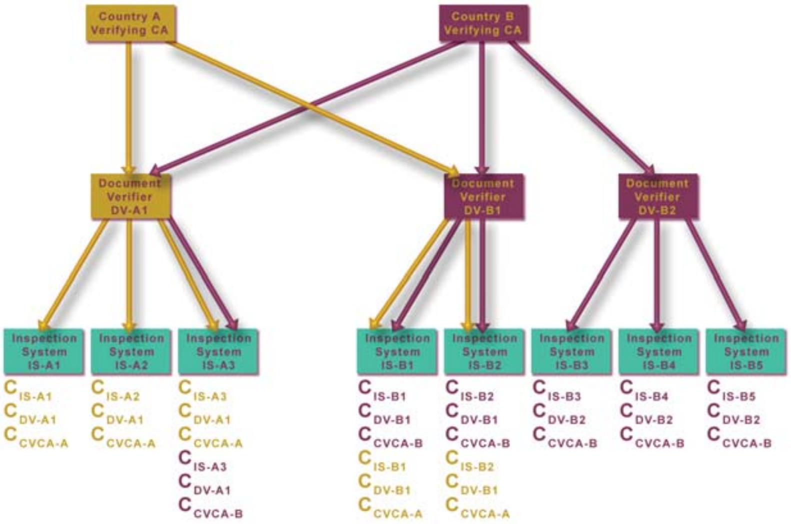
Chip Authentication

Chip Authentication is an alternative to Active Authentication and the Secure Messaging implemented as part of Basic Access Control. It is performed after Basic Access Control and provides both a means of authenticating the chip and of generating session keys for secure communications between the chip and the inspection system. It is immediately followed by Passive Authentication.

The chip has a key pair stored in it, specifically for use during Chip Authentication, to generate a shared secret that is used to derive the session key. The inspection system generates a dynamic key pair for the same purpose. Using a key agreement algorithm such as Diffie-Hellman both the chip and the inspection system can generate the same shared secret without compromising information in their communications. In the process the chip sends its public key to the inspection system. In the subsequent Passive Authentication that public key is verified along with the rest of the embedded data. The ability of the chip to successfully generate the shared secret and hence perform the encrypted communications verifies that it has knowledge of the private key that matches the public key, while the Passive Authentication verifies that the public key is genuine.

Terminal Authentication

This is the protocol that enables the chip to confirm that the inspection system is authorized to read the sensitive data. It is used if the inspection


Country A Verifying CA
Country B Verifying CA
Document Verifier DV-A1
Document Verifier DV-B1
Document Verifier DV-B2
Inspection System IS-A1
Inspection System IS-A2
Inspection System IS-A3
Inspection System IS-B1
Inspection System IS-B2
Inspection System IS-B3
Inspection System IS-B4
Inspection System IS-B5
C_{IS-A1} C_{DV-A1} C_{CVCA-A}
C_{IS-A2} C_{DV-A1} C_{CVCA-A}
C_{IS-A3} C_{DV-A1} C_{CVCA-A} C_{IS-A3} C_{DV-A1} C_{CVCA-B}
C_{IS-B1} C_{DV-B1} C_{CVCA-B} C_{IS-B1} C_{DV-B1} C_{CVCA-A}
C_{IS-B2} C_{DV-B1} C_{CVCA-B} C_{IS-B2} C_{DV-B1} C_{CVCA-A}
C_{IS-B3} C_{DV-B2} C_{CVCA-B}
C_{IS-B4} C_{DV-B2} C_{CVCA-B}
C_{IS-B5} C_{DV-B2} C_{CVCA-B}

system wishes to read the sensitive data and must have been preceded by successful Chip Authentication and Passive Authentication.

Each Issuing State that requires protection for sensitive data on its ePassports using EAC must operate a Country Verifying Certification Authority (CVCA). The public key of the CVCA is stored as a *trustpoint* in the chips embedded in the ePassports issued by that State. As the keys are renewed over time, the CVCA issues a link certificate, CCVCA, that enables the previous public key to be used to validate a certificate identifying the new public key.

Each Receiving State that requires to be authorized to read the sensitive data from EAC-protected ePassports must reach an agreement with the Issuing State. The State will operate a Document Verifier (DV) which is a Certification Authority that is responsible for issuing certificates to authorised Inspection Systems. A CVCA issues a Certificate, C_{DV}, to each DV, both domestic and foreign, that has been authorized to view the protected data. The DV issues an Inspection System certificate, C_{IS}, to each authorized Inspection System in that State.

Thus an inspection system will have a certificate chain consisting of the system's C_{IS}, the C_{DV} of its certifying DV and, if necessary, the Passport Issuer's link certificate C_{CVCA}. For each Issuing State for which it is authorized to read sensitive data from EAC protected ePassports, the inspection system will have a separate certificate chain.

During Terminal Authentication the inspection system sends the appropriate certificate chain to the chip, which validates the certificates. If a link certificate has been supplied and it relates to a more recent key than the trustpoint already stored in the chip, the chip will validate the certificate using the stored key and, if valid, store the new public key from the certificate as its most recent trustpoint. This is used to validate the C_{DV}, which is then used to validate the C_{IS}. The chip also stores the effective date of the most recent of the C_{CVCA}, C_{DV} or domestic C_{IS} as its *current date*. Subsequently any certificate presented by an inspection system, with an expiration date before the stored current date will not be accepted by the chip, causing Terminal Authentication to fail on the grounds that the inspection system is no longer authorized for that passport. This type of failure may occur for a number of reasons, ranging from the use of a bogus inspection system to ineffective certification or certificate management within the State.

Once the chip has validated the certificate chain sent by the inspection system it extracts the public key from the C_{IS}. It sends a randomly chosen challenge to the inspection system, which returns a response that has been signed with the associated private key. The chip verifies the signature thus confirming that the inspection system has knowledge of the private key. If successful the chip allows the inspection system access to the sensitive data.

Each of the certificates in the chain identifies the access rights (essentially iris, fingerprint, or both) granted by the issuer – thus the CDV may restrict the rights granted to a DV by the CVCA and the C_{IS} may further restrict the rights granted to an Inspection System by the DV. The chip will permit only the rights that are granted in all certificates in the chain.

Implications for EU Issuing States

The implications of implementing EAC for an Issuing State relate to the choice of chip to be used in the ePassports and the establishment of additional Public Key Infrastructure and associated processes within the State and cross-border.

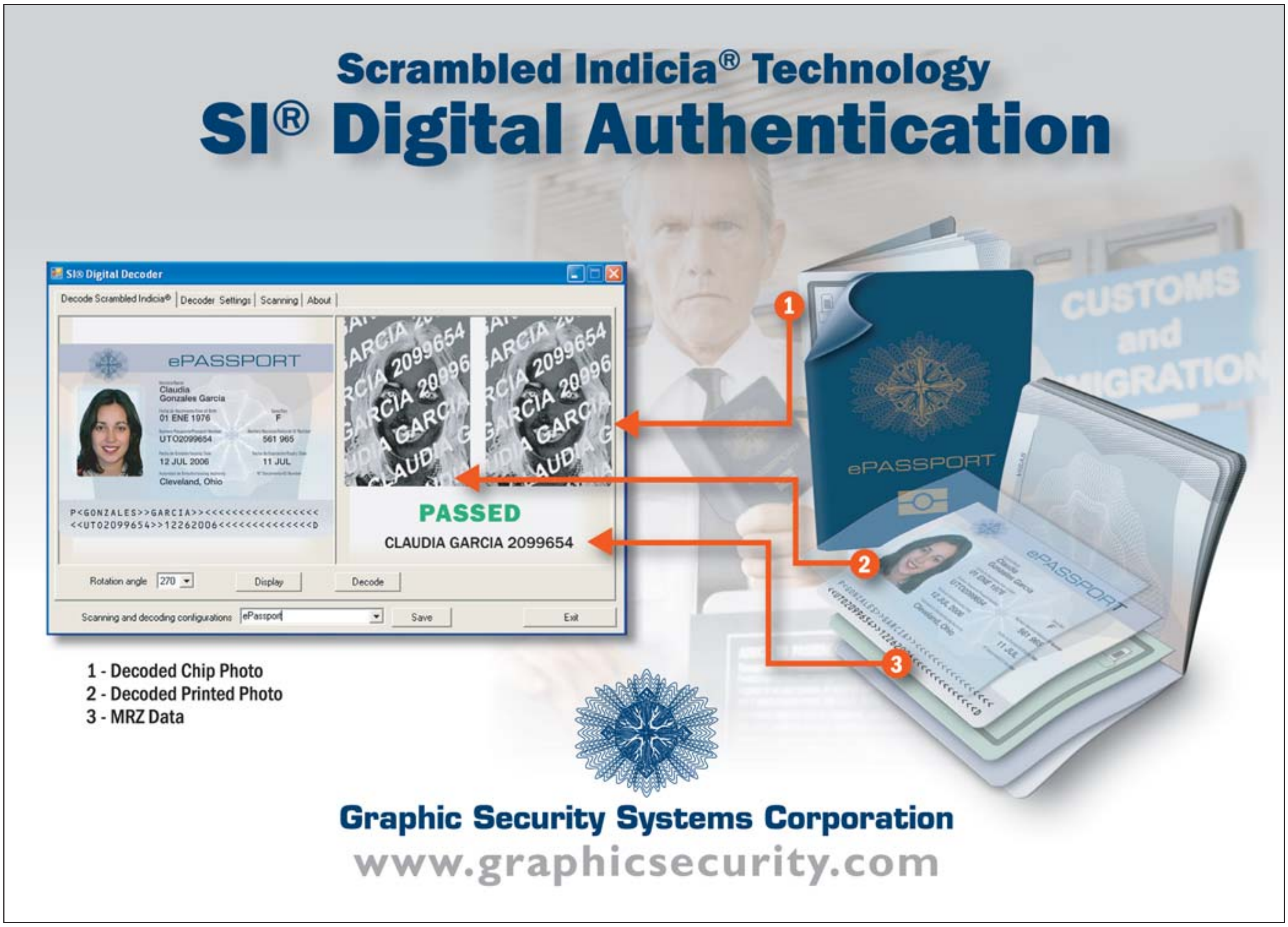
Certification of chips

The chip needs to be capable of performing the cryptographic operations required to validate the certificate chain and verify the response during terminal authentication. The chip will also need to be able to store additional secure data (keys, trustpoint and current date). ICAO recommends that the chips used should be certified against a suitable Common Criteria (CC) protection profile. The EU decision[3] to adopt EAC mandates the use of CC certified chips, for which a protection profile now exists[4]. This is likely to significantly increase the development cost of any chip that implements the EU EAC specification, leading not only to higher costs but probably to a limited choice of suppliers.

Infrastructure

A State issuing ePassports must have in place the basic PKI entities required to sign the embedded data, i.e. the Country Signing Certification Authority (CSCA) and at least one Document Signer (DS). It will also need to have mechanisms in place to issue a Certificate Revocation List (CRL) on a regular basis, and to distribute the certificates and CRLs to ICAO and other participating States[1].

The EU implementation of EAC will require the establishment of the CVCA to issue certificates to any authorised DV (domestic or other States). The validity periods of certificates issued for EAC are shorter than CSCA and DS certificates and will require significantly more management — a C_{DV} will have a validity period between two weeks and three months, while a C_{IS} will have a validity between one day and one month. The


Scrambled Indicia® Technology
SI® Digital Authentication
SI® Digital Decoder
Decode Scrambled Indicia® | Decoder Settings | Scanning | About
ePASSPORT
Claudia
Gonzales Garcia
01 ENE 1976
F
UTO2099654
561 965
12 JUL 2006
11 JUL
Cleveland, Ohio
P<GONZALES>>GARCIA>><<<<<<<<<<<<<<<<<
<<UTO2099654>>12262006<<<<<<<<<<<<<<D
PASSED
CLAUDIA GARCIA 2099654
Rotation angle 270
Display
Decode
Scanning and decoding configurations ePassport
Save
Exit
1
2
3
ePASSPORT
CUSTOMS and IMMIGRATION
1 - Decoded Chip Photo
2 - Decoded Printed Photo
3 - MRZ Data
Graphic Security Systems Corporation
www.graphicsecurity.com

certificates are to be distributed via email so a suitable mechanism should be implemented to manage and handle the receipt of certification requests and the subsequent issue and delivery of certificates.

While the technology for the CVCA and DV is substantially the same as for the CSCA and DS (except that the certificates are in Card Verifiable format rather than the standard X.509), the short validity periods will result in a significantly higher volume and will potentially necessitate more operational and management complexity.

The protocols for inter-State certification requests and certificate distribution have not yet been formulated. The Brussels Interoperability Group is tasked with considering the operational aspects of EAC certificate management and the impact upon border control inspection of ePassports within EU and non-EU States.

The EU decision to adopt EAC also mandates the publication of a Certificate Policy by each State's CVCA but makes a Certification Practice Statement optional.

Implications for EU Receiving States

Receiving States who wish to inspect EAC protected ePassports and access the sensitive data therein will need to operate inspection systems that are EAC compliant, and the concomitant Public Key Infrastructure.

Inspection System

An EAC compliant inspection system will require additional components over and above those needed for a basic inspection system; most significantly the means to securely generate, store and use a key pair in a device such as a Hardware Security Module (HSM). It will also need biometric devices to capture images to be validated against the data on the ePassport.

A State will need to determine how this can be effectively implemented, which will depend on the number of borders control points and other places where the inspection systems will be deployed. There are two alternate approaches. A *centralized* approach where there is one authorized Inspection System Server that maintains keys securely, and all terminals pass their transactions to the server for cryptographic operations; this reduces the cost and complexity of securing the keys as well as the volume of certificates (and key pairs) that must be managed, but at the expense of performance, as the inspection of every EAC passport must endure the inevitable communications delays arising from the remote operation. A *distributed* model where each inspection terminal is a separately authorizsed inspection system with its own keys and certificates that it must manage; this significantly increases the cost and complexity of securing the keys and managing the increased volume of certificates, but enables the best performance to be obtained. Inevitably hybrid solutions, such as distributed servers handling a local network of terminals (say all those at a particular port) will be a suitable compromise.

Infrastructure

Any State inspecting ePassports must already have in place the basic PKI entities required to validate the signature in the embedded data, i.e. a Public Key Directory (PKD) from which to retrieve the relevant C_{CSCA} and C_{DS} certificates. It will also need to have mechanisms in place to action in a timely manner any CRLs that are received.

The EU implementation of EAC will also require the establishment of at least one Document Verifier CA to issue certificates to authorised inspection systems, having itself been certificated by the CVCA of each Issuing State. Thus a DV may have 27 currently valid C_{DV} certificates which may need to be renewed as often as every two weeks. The DV will need to issue a C_{IS} for each of its dependent EAC compliant inspection systems relating to each State (and chained to the relevant C_{DV}), potentially every day.

Sdu Identification's passport concept ready for the future

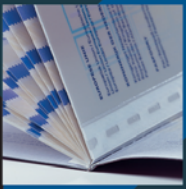
Dutch passport

Finnish passport

Irish passport

Swiss passport data page

Integrated transparent Kinegram®


Binding technology®

ImagePerf/TLI®

Enrolment device

Sdu Identification is one of the leading developers of physical and digital high-end national identity documents world-wide. By means of system integration we realise secured end-to-end solutions to process the issuing of ID documents.

Research & Development has always been high on our list of priorities. We have developed a high-end passport concept in which the data page with integrated contact less chip technology is finished as a polycarbonate document that is incorporated into the passport booklet using a durable binding technology invented by Sdu Identification.

Moreover, our company has developed the concept for the current Dutch identity card. Also made from polycarbonate, it enables contact and contact less chip technology to be integrated. In addition to the graphic laser-engraved personalisation, ImagePerf/TLI® and a transparent Kinegram® are applied in the identity cards as well as in the passport data page.

Also the Dutch EU Residence Permits and the new Dutch driver licences are produced following this high end identity card concept.

Integration of biometrics
Concerning the durability of a biometric passport, the most important requirement is that chip and antenna must function correctly during the lifetime of the passport. The best solution for security and durability is the ICAO compliant integration of a contact less crypto processor chip with an antenna into the polycarbonate data page. Biometrical information about the document owner is saved digitally and secured electronically in the contact less crypto processor chip.

Sdu Identification developed a biometric passport solution that is already in full scale operation in three European countries. The Dutch government as well as the Finnish successfully implemented this since August and the Irish government successfully implemented this since October 2006. Next to that Sdu Identification has been awarded with a contract for the production of biometric passports for Slovakia. Sdu Identification is also the supplier of polycarbonate data pages for the Swiss passport.

Secured storage of biometric data
The authenticity, integrity and contents of the chip are guaranteed by the use of a digital certificate and asymmetric keys. The retrieval of this information and the biometric identification of the identity of the document owner can take place at border crossings.

The Sdu Identification ePassport solution, consisting of a Philips 72 kB Smart MX micro crypto processor chip, operating system and Sdu ID_Applet, allows the storage of two types of biometric data, i.e. facial recognition and fingerprints and the following functionalities as far as specified by ICAO:
- Passive Authentication;
- Basic Access Control;
- Active Authentication;
- Extended Access Control.

Enrolment device for recording of biometric data
For the collection of biometric characteristics (such as face or finger) of the applicant in an electronic way Sdu Identification developed an enrolment device and software. The enrolment device can be integrated as a front office device in every process where applications are digitised and plays an essential role at issuance of the travel documents.

Sdu IDENTIFICATION

PO Box 5300
2000 GH Haarlem
The Netherlands

Telephone +31 23 799 51 46
Fax +31 23 799 51 80
www.sdu-identification.nl
sales@sdu-identification.nl

Implications for Non-EU Receiving States

Although the EU implementation is intended for use by EU States, there are likely to be some non-EU States that will wish to inspect sensitive data in EU passports. In the event that agreement is reached with an EU Issuing State to authorize access, any such Receiving State will need to implement an EAC compliant inspection system and Public Key Infrastructure as described above for EU Receiving States. If such agreements are made on a reciprocal basis there is likely to be additional complexity introduced if the State has implemented an alternative mechanism for protecting sensitive data on its own passports.

Compromised inspection systems

In the current specifications there are no mechanisms for revoking the C_{CSCA}, C_{DV} or C_{IS} certificates, only replacing them. Thus, the robustness of the PKI solution, including the PKD, that supports EAC-enabled inspection systems, is critical to ensure prompt recovery from failures or compromises and allow normal operations to continue.

If an inspection system is compromised the implications are that it can read passports for which it is authorized until the C_{IS} expires (one to 30 days) and thus whoever has access to it can use it to read sensitive data from passports. The chain within the terminal is valid and consistent and so the chip has no way of knowing it has been compromised. Replacing the IS certificates for all of the State's other inspection systems would have no effect, even domestic inspection systems which could cause the chip in a passport to update *current date* to the effective date of the new IS certificate(s). The compromised inspection system will still have a certificate with an expiry date after the new *current date* so it makes no difference. Replacing the DV certificates is similarly ineffective. In all cases, there is nothing the Issuing States can do to reduce the time that the compromised inspection system will work. Hence the need for a short validity period for inspection systems that are vulnerable to attack.

It is worth noting that the centralized approach to inspection systems described earlier would reduce the risks from a compromised terminal.

Alternatives

What alternative approaches might be used by other States? Details of protocols could be changed, but the best target for replacement is the EU implementation's dependence on an operationally complex hierarchy of certificate issuing and management processes and entities, in place purely to ensure that only authorized inspection systems can access the sensitive data from the passport in order to compare it with real-time biometric sensor data being captured from the passport holder. The most radical alternative would therefore be for a State to choose to perform the biometric validation on the chip itself thus obviating the need for any sensitive data to leave its secure environment and hence removing the need for authorization of terminals. As long as the chip has been authenticated by the terminal and Secure Messaging is in place, the result of the biometric validation can be verifiably communicated to the terminal. This would obviously require the chip to have suitable processing capability to perform the biometric validation.

Temporal S. (www.temporals.com) is a specialist provider of products and services to the ePassport market, and it has developed specific EAC functionality that can be used to support the development and implementation of EAC-based ePassport solutions. For more information contact: Gillian@temporals.com

References

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

2 *Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control*, TR-03110, Version 1.01, 2 November 2006, Bundesamt für Sicherheit in der Informationstechnik

3 *Commission Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States*, C(2006) 2909, 28 June 2006, Commission of the European Union

4 *Common Criteria Protection Profile, Machine Readable Travel Document with "ICAO Application" Extended Access Control*, BSI-PP-0026, Version 1.1, 7 September 2006, Bundesamt für Sicherheit in der Informationstechnik ◆

Australia Hands Over First Participation Notice to ICAO PKD MoU

Australia becomes the first Participant to the "*Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory*" (the ICAO PKD MoU) during a brief ceremony at ICAO headquarters on 6 March 2006. The ICAO PKD MoU has been effective since 8 March 2007 when the fifth Notice of Participation was received by ICAO Secretary General. Shown on the occasion are (l-r) ICAO Council President Roberto Kobeh Gonzalez; Haile Belai, Chief Security and Facilitation Branch; ICAO Secretary General Dr. Taïeb Chérif; John Begin, Acting Director Air Transport Bureau; Mauricio Siciliano, Technical Officer, MRTD Programme; and Simon Clegg, Representative of Australia on Council. ◆

Events to come

As part of the **MigraMacau** project, the Macao SAR China Immigration Department will organize, in partnership with the Portuguese Immigration Service (SEF), the "***I. Pan-Asian Seminar on Security Documents***", from 28 May to 8 June 2007.

This Seminar will be technically and financially assisted by the European Union under the **AENEAS PROGRAMME** and will be conducted by highly qualified trainers from Portugal, Germany, Ireland, Hong Kong SAR China, the Netherlands and the United Kingdom.

Faced with rapidly growing technological development and demands for high security standards in biometrics, identity and travel documents are becoming extra secure, more synthetic-based and demand knowledge on electronic issues. The consequences of this on the identity chain are immense. Therefore, the need for updating information and availing ourselves of new teaching materials to focus on this aspect is crucial to implement a higher level in document examination worldwide and to combat document fraud.

The purpose of this course, genuine-oriented and based on the principle "***Train the trainer*** " which allows the participants to deepen their knowledge and build up specific networks, is to provide the participants with up-to-date training on security documents as well as with the latest tools for their work in detecting fraudulent documents.

To accomplish those goals, the training will provide the *opportunity*, to all participants to:

- get in touch with samples of all materials, fabrics, substance and in some cases, objects that come into the production chain of a security document;
- be familiar with the most recent fraud on security documents on both substrates: paper and polymer;
- deal with the most up-to-date analyzing technical equipment;
- visit some security document issuing authorities, such as the Portuguese Consulate, the Macao Identification Department (DSI) and the Macao Government Printing Bureau;
- exchange information so that the use of fraudulent travel documents at the borders and within the region can be adequately combated.

Consequently, this training is oriented for mid to senior level officers *involved in document inspection/examination*, mainly: **I**) Police officers who have to deal with document investigation; **II**) Investigation officers at border checkpoints and **III**) Immigration or Police services, with experience in developing new concepts for security documentation.

Keeping the focus on the detection of fraudulent documents as well as on the need to have equivalent training structures and harmonized procedures in this regard, the intention of this initiative is to encourage the participation of Asian countries, and to set a starting point for a training structure on security documents and document fraud . ◆

Third Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

Montreal, 1-3 October 2007

ICAO will hold its Third Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards from 1 to 3 October. The Symposium, which will be complemented by an Exhibition focusing on products and services related to Machine Readable Travel Documents (MRTDs), biometric identification, airport security biometric and border control inspection systems is paticularly addressed to the representatives of Border Control Agencies, Airports and Airlines.

The 2007 Symposium follows last year's successful event, attended by over 550 participants from 65 States, 12 international organizations and more than 80 companies and institutions. It will again take place at ICAO Headquarters, 999 University Street, Montreal, Quebec, Canada.

THE SYMPOSIUM WILL FOCUS ON:

- *The main features and benefits of globally interoperable and ICAO-compliant MRTDs, including biometric enabled versions with enhanced ID confirmation;*
- *Benefits and challenges in the integration of biometrics into an airport security system – access control, passengers and crew identification;*
- *Airport and airline experience in the implementation of biometrics in an airport security system;*
- *Biometrics and supporting document reading systems;*
- *Essential security measures to address identity theft, illegal migration and trans-border crime;*
- *The use of biometric technology in MRTDs and eMRTDs to enhance security in enrolment, issuance and border control inspection systems;*
- *The use of MRTDs and eMRTDs in airline passenger service systems;*
- *Importance of travel document security measures, MRTDs and biometrics implementation in national security programmes;*
- *Benefits of biometric-enabled travel documents for travellers.*

The Symposium will be of particular interest to officials of passport and ID document issuing agencies, immigration, customs and other border control and security authorities.

Representatives of airlines and airports especially those involved in passenger service systems, handling travel documents, facilitation and aviation airport security should greatly benefit from attendance.

We encourage your participation. For further information, please visit the Symposium website, which will be updated on a regular basis:

http:// www.mrtd.icao.int

The Benefits of Using ICAO Standards for Travel Documents from a Border Control Perspective

by Bradford J. Wing, Chief Biometrics Engineer,
US-VISIT/Department of Homeland Security

The International Civil Aviation Organization (ICAO) has been actively working to develop and promote the standardization of travel documents since 1980. The major benefit of these standards is that they provide the foundation for global interoperability so that documents produced in one country can be read and inspected by all other countries using compliant hardware, software and infrastructure.

The use of standards has several other advantages, including the increased ability for border control officials to examine and recognize legitimate documents. Additionally, the introduction of special security features into travel documents deters counterfeiting and alteration.

With the increased use of technology, standardization becomes even more critical for effective border inspection. With a uniform approach adopted by travel document issuing authorities around the world, nations checking the documents of travellers do not have to adapt their technology to accept multiple interpretations of travel documents.

One example of standardization is the information contained on the data page and in the Machine Readable Zone (MRZ), which is printed in a standard position, with specified locations in the zone for particular information, and with the characters placed on the page in a specified font and size and with specified ink characteristics. This standardization, adopted by ICAO in the 1980s and to be mandatory by 1 April 2010 for all ICAO-compliant passports, allows automated scanning of the MRZ. This dramatically reduces errors that are caused by human data entry of the information, which would otherwise be necessary.

ICAO adopted the blueprint for e-passports in 2004. E-passports are passports that conform to all of the basic ICAO standardization requirements (size, composition, contents, appearance), including an MRZ on the data page, as well as having an electronic data chip (and small antenna) contained within the passport itself. This data chip must conform to ICAO specifications in its physical and operational characteristics. A key element is the specification of the format of information to be contained on the chip itself.

Only if a passport meets all of the physical, operational, and data requirements associated with the ICAO e-passport standards can that passport be branded with the ICAO e-passport logo. This standardization ensures that the data on the e-passports can actually be read and used by the receiving state, as well as allowing verification that the biographic data stored on the chip matches that printed on the data page, through the use of electronic signatures and data security measures developed specifically for e-passports.

The biometric data on the chip is also protected against alteration or counterfeiting through the use of these data security and protection measures that likewise can be checked by the receiving state. Standardization of content on the chips means that the information will have a consistent definition (for biographic data) and that an automated comparison is possible of biometric data stored on the chip against a live biometric data sample provided by the traveller, thereby confirming that the person using the travel document is the person to whom it was legitimately issued.

The process of standardization for e-passports was extensive and thorough. Building upon general standards for electronic chips and biometrics, as established by the International Organization for Standardization, a particular set of options allowed under those standards was selected for adoption by ICAO. A crucial step involved testing of this set to ensure that they would truly allow global interoperability. This was essential, since prior to the e-passport project, most chip applications had used "closed systems" (i.e systems in which the chip's manufacturer provided the reading equipment and used a proprietary data format). E-passports might have been produced that met general technical specifications, but that would have been ineffective, since they most likely would not have been readable by a receiving State's equipment (also meeting only general technical standards). In other words, the basic purpose of having ePassports would have been defeated.

With the adoption of strong and clear standards by ICAO, travel document issuing authorities have been able to produce e-passports that are readable by all receiving states, regardless of the manufacturer of the chip or of the passport reader equipment. This is a major milestone in travel security and facilitation –- principal goals of ICAO MRTD standards and specifications. ◆

190 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
Montenegro
Netherlands
Norway
Poland
Portugal
Republic of Moldova
Romania
Russian Federation
San Marino
Serbia
Slovakia
Slovenia
Spain
Sweden
Switzerland
Tajikistan
The former Yugoslav Republic of Macedonia
Turkey
Turkmenistan
Ukraine
United Kingdom
Uzbekistan

MIDDLE EAST

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
Republic of Korea
Samoa
Singapore
Solomon Island
Sri Lanka
Thailand
Timor-Leste
Tonga
Vanuatu
Viet Nam

The importance of Machine Readable Travel Documents to tourism

by Chris Lyle, Representative of the World Tourism Organization to ICAO

The World Tourism Organization (UNWTO) is the United Nations Specialized Agency with a central and decisive role in promoting the development of responsible, sustainable and universally accessible tourism. Concerned with the continued threat of terrorism to tourists, on the ground as well as in the air, and the costs and irritation of security measures, in 2004 the Organization consolidated its work on tourism safety, security and facilitation into a strategy known as S.A.F.E, Security and Facilitation Enhancement. S.A.F.E. applies a systems approach to facilitation and security, to tourism and air transport, and to rich and developing countries.

Chris Lyle, Representative of the World Tourism Organization to ICAO.

Over 40 per cent of the 842 million international tourist arrivals in 2006 reached their destination by air, with much higher percentages being recorded for long-haul destinations and for those not readily accessible by other means of transport, including island and landlocked developing countries. Conversely, the vast majority of the 931 million international passengers (including 91 million on non-scheduled operations) estimated by ICAO for the same year are defined as international tourists (which include those on business-related travel). UNWTO therefore strongly supports ICAO Annexes 9 and 17 as well as the ICAO MRTD programme, and participates in the industry's Simplifying Passenger Travel programme.

UNWTO supports the rapid introduction of ePassports as an added security measure, urging governments to move rapidly and cohesively, but to take account of:

- the need to reflect tourism requirements in the historically focussed aviation approaches – including eVisas, land border crossings, cruise ships, large hotels, major events and key tourism sites
- the importance of using common technical languages and interoperable systems in tourism and aviation
- the pressing case for parallel enhancements in security and facilitation
- the critical shortfalls in developing countries of technologies, human skills and finance, and the need to rectify these both for total system security and equitable participation of those countries in tourism benefits
- the need to reconcile the fact that more than 60 States have yet to issue passports in a basic

machine-readable form, against an ICAO Standard deadline of April 2010, while issuance of ePassports remains a Recommended Practice rather than a Standard, with no deadline.

UNWTO is involved in some parallel activity to that of ICAO. For example, in 2006 UNWTO signed a strategic cooperation agreement with Microsoft on new information and communication technologies, with priority for Africa. In addition to establishing a new portal called "Windows on Africa", this includes improving access for tourists though electronic border clearance. UNWTO is also working with Microsoft and WISeKey, the internet security company, on expanding the use of traveller identification and authentication technologies, including biometrics. There is a need for ICAO and UNWTO to work closely to ensure interoperability between their respective initiatives and to assist the communities that they represent in benefiting from potential synergy.

A recent survey of National Tourism Administrations shows that the application of new technology should benefit all modes of transport, not just air; all aspects of travel, not just air transport; all travellers, not just frequent trippers; and all countries and communities, not just rich ones. ◆

Worldwide overview introduction of ePassports

Introduction dates and technical specifications

Country	Introduction date	Face ICAO compliant	IMAGE format
Belgium	24 November 2004	Yes	JPEG
Thailand	26 May 2005	Yes	
Sweden	3 October 2005	Yes	JPEG 2000
Norway	3 October 2005	Yes	JPEG
Australia	24 October 2005	Yes	JPEG
Germany	1 November 2005	Yes	JPEG 2000
New Zealand	4 November 2005	Yes	JPEG
United Kingdom	6 March 2006	Yes	JPEG
Japan	20 March 2006	Yes	JPEG
France	12 April 2006	Yes	JPEG 2000
Singapore	29 April 2006	Yes	JPEG 2000
Iceland	23 May 2006	Yes	JPEG 2000
Austria	16 June 2006	Yes	JPEG
Portugal	31 July 2006	Yes	JPEG 2000
United States	14 August 2006	Yes	JPEG
Denmark	1 August 2006	Yes	JPEG
Spain	14 August 2006	Yes	JPEG 2000
Finland	21 August 2006	Yes	JPEG
Netherlands	26 august 2006	Yes	JPEG 2000
Greece	26 August 2006	Yes	JPEG
Lithuania	28 August 2006	Yes	JPEG 2000
Luxembourg	28 August 2006	Yes	JPEG
Slovenia	28 August 2006	Yes	JPEG 2000
Poland	28 August 2006	Yes	JPEG
Hungary	29 August 2006	Yes	JPEG
Czech Republic	1 September 2006	Yes	JPEG
Switzerland	4 September 2006	Yes	JPEG 2000
Andorra	1 September 2006	N/A	N/A
San Marino	12 October 2006	N/A	N/A
Ireland	16 October 2006	Yes	JPEG 2000
Liechtenstein	26 October 2006	Yes	JPEG
Italy	26 October 2006	Yes	JPEG
Hong Kong - SAR China	5 February 2007	Yes	JPEG 2000

Source: IF4TD Web Site.

States that have announced the issuance of ePassports for 2007 are:

Brazil, Bulgaria, Chad, Egypt, Estonia, India, Latvia, Moldova, Nigeria, Russia, Somalia, Turkey, United Arab Emirates and Venezuela.

Definitions and Terms Related to Biometrics

(Excerpts of Section III Doc 9303 Part 1, Volume 2 - sixth edition.)

Terms related to biometrics are defined as follows:

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 an 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.

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.

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.

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

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

End User. A person who interacts with a biometric system to enroll or have his[1] 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.

[1] Throughout this document, the use of the male gender should be understood to include male and female persons.

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 his 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 his 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.

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.

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

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

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

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

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

Impostor. A person who submits a biometric sample in either an intentional or inadvertent attempt to pass for another person.

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

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.

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.

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.

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.

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

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

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.

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.

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).

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.

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 II, 13 in this volume of Doc 9303, Part 1.)

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

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*".

WSQ (Wavelet Scalar Quantization). A means of compressing data used particularly in relation to the storage of fingerprint images. ◆

PASSPO