MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

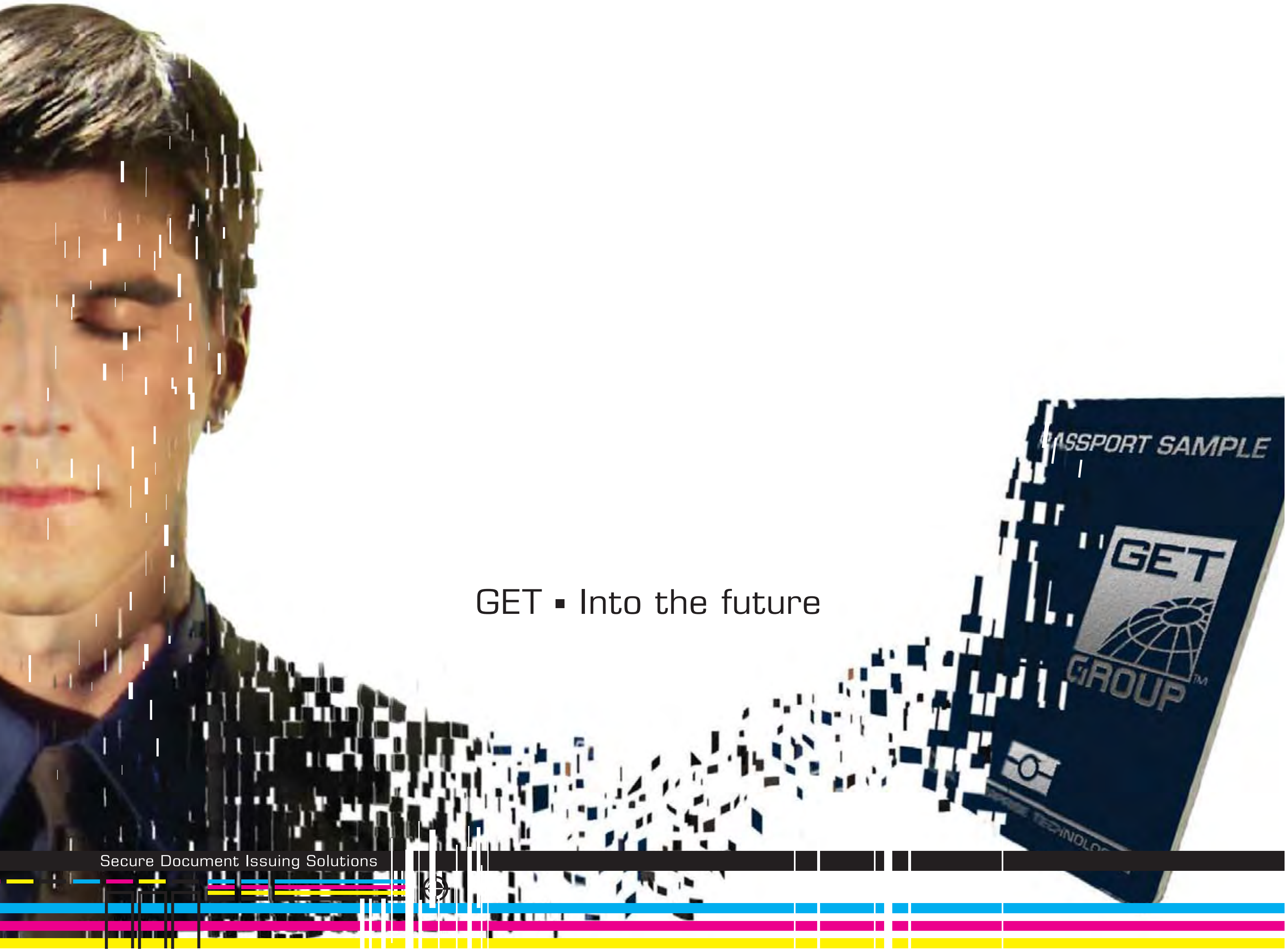
Coordinated Assistance

Reviewing the intensified levels of cooperation being implemented by ICAO SFP and partnering bodies as the Organization continues to provide more effective guidance and resources to its Member States

Also in this issue:
The 'HII' point in our future? • ICAO PKD Update
Tom Kinneging: Simplifying ePassports and the PKD
MRTD Glossary of terms

Vol. 4, N° 1

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



© 2008 Global Enterprise Technologies Corp.

ICAO MRTD REPORT
VOLUME 4, NUMBER 1, 2009

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

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

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

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

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

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

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

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

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

Copyright © 2009
International Civil Aviation Organization

PRINTED BY ICAO

Contents

www.icao.int

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

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

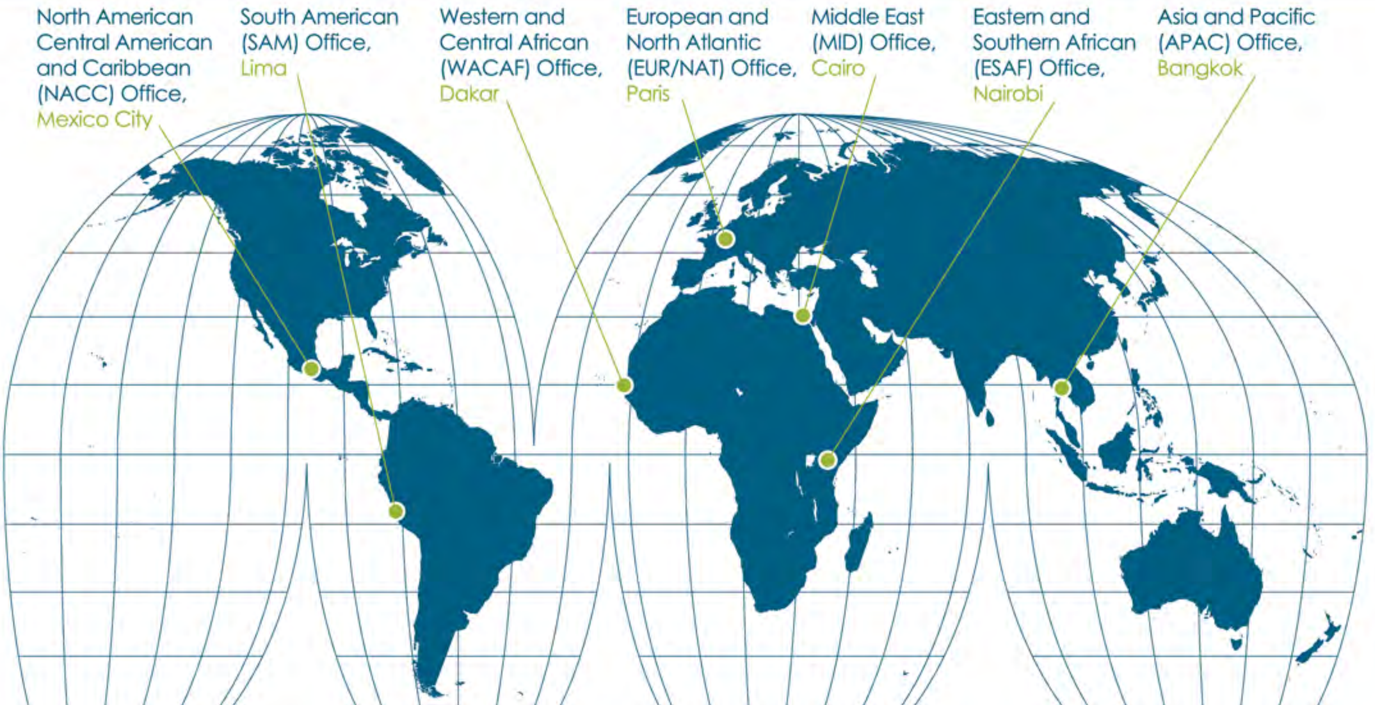
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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

Observer organizations

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

ICAO's Global Presence


North American Central American and Caribbean (NACC) Office, Mexico City
South American (SAM) Office, Lima
Western and Central African (WACAF) Office, Dakar
European and North Atlantic (EUR/NAT) Office, Paris
Middle East (MID) Office, Cairo
Eastern and Southern African (ESAF) Office, Nairobi
Asia and Pacific (APAC) Office, Bangkok

ICAO: the global fulcrum of coordinated MRTD assistance

This issue of the MRTD Report is a special one for me in that it highlights the types of advances that regulators, States and associated international bodies continuously work toward, and yet which often go un-noticed by the millions of travellers who benefit from them every time they take an aircraft or pass through a border check-point. To my mind, it's specifically the seamless and unobtrusive nature of the implementation of these improvements, as well as the satisfaction of the passengers themselves that are our most important benchmarks in measuring MRTD success.

More than this, this issue serves to bring to the forefront the manner in which international cooperation is beginning to reach a truly new and exciting threshold of organization and effectiveness. This is an ambition that has driven regulators at the international level for decades, and we definitely stand on the shoulders of those who have come before us when we look upon our recent accomplishments. As I write to you today I am keenly aware that on a technological, bureaucratic and even a personal level, a truly "global" awareness has begun to take hold and is now manifesting itself in tangible, practical solutions to worldwide challenges.

In all the areas of international cooperation under discussion here, the officials involved could likely point to a key development or event in their domains that revealed itself as a turning point in regard to this new level of cooperative effectiveness. In the area of travel documents and facilitation, I personally look upon the development of the Implementation and Capacity Building Working Group (ICBWG) as our own turning point. Over recent months the ICBWG has revealed itself to be the organizational tool that has permitted the UN and its partners in this area to be able to provide a much higher level of coordinated assistance and guidance to the States and, ultimately, the citizens that we serve.

I need to stress here that this has truly been a cooperative effort. The recent advances in State assistance that have been witnessed were only possible through the determined efforts of ICAO in conjunction with other UN and non-UN bodies. UN partners include the Counter-Terrorism Committee Executive Directorate (UN CTED—the more practical arm of the Security Council's Counter-Terrorism Committee), while key non-UN stakeholders have been comprised of the International Organization for Standardization (ISO), Interpol, the Airports Council International (ACI), the International Air Transport Association (IATA), and more lately the Organization of American States' (OAS) Secretariat of the Inter-American Committee against Terrorism (CICTE), the Organization for Security and Co-operation in Europe (OSCE) and the International Organization for Migration (IOM).

In every case, these organizations, as well as the individuals in them who are constantly working to move cooperation forward, have made invaluable contributions to the new and more effective global conditions we now find ourselves in. The increased level of communication now being enjoyed is leading to less duplication of efforts and a far more harmonized approach to the security and facilitation challenges facing world States and world travellers.

Also included in this edition are some excellent perspectives from the likes of Raymond Wong and Tom Kinneging, which I'm sure readers will find useful as they consider the current situation at hand and the directions and capabilities that new and converging technologies are now beginning to reveal to us.

Last but far from least, there is also an excellent review of the status of ICAO's important work in the area of Document Signer Certificates and the Public Key Directory which distributes these to States. This interview with Dr. Eckhart Brauer is required reading for State officials who are now preparing to sign on to what is essentially the security backbone of the global ePassport effort.

Happy reading. ■

Mauricio Siciliano
Editor

Effective partnerships

As more and more passengers today find themselves travelling through multiple national border control and facilitation systems in the course of just a single business or leisure trip, much of the technological and regulatory backbone that has permitted this highly-effective travel environment to develop and flourish remains, perhaps appropriately, under-recognized and under-appreciated.

Though many felt that the aftermath of 9/11 would evolve into a more-or-less permanent condition of longer passenger wait times and increased difficulties and delays for all travellers and citizens at customs and border control checkpoints, the tremendous efforts of ICAO and several key international partnering bodies has permitted most passenger experiences to improve dramatically in recent years —even as national security requirements have been strengthened.

It may seem remarkable to some that the significant changes to (and ongoing synchronization of) the standards and systems underlying today's border control experience have occurred during a period that has simultaneously witnessed the greatest increase in security-related measures since the dawning of international air transport.

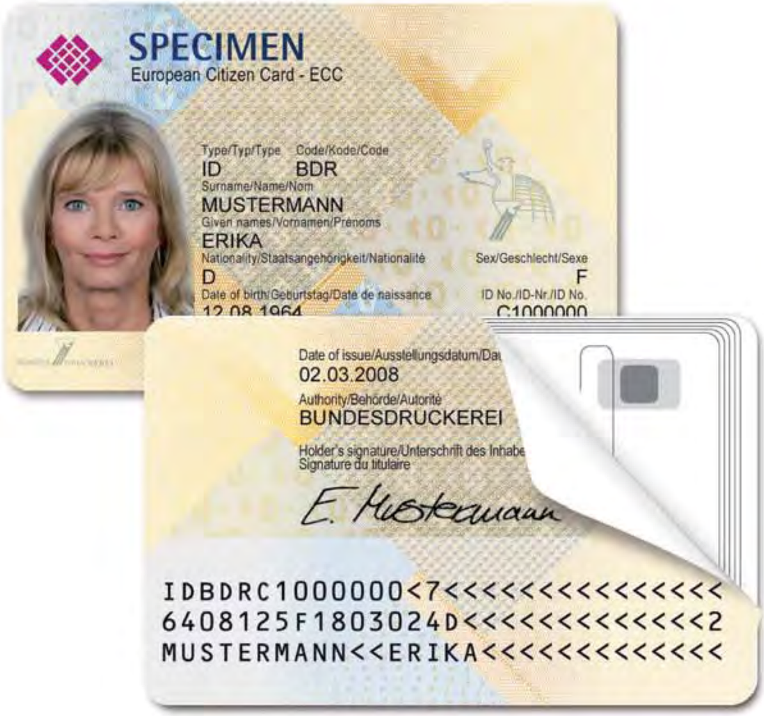
ICAO has contributed in this area primarily through the work of its Aviation Security and Facilitation Policy (SFP) Section, which is responsible for the management of the ICAO Aviation Security (AVSEC) Programme and the Facilitation and Machine Readable Travel Documents (MRTD) Programmes.

Because documents such as passports, visas and national identity cards form such a crucial component of all security-related developments relating to aviation and border control, ICAO's tremendous work in this area has helped to foster

BUNDESDRUCKEREI

▶THE eID CARD

SECURITY IN THE REAL AND DIGITAL WORLD



SPECIMEN
European Citizen Card - ECC

Type/Typ/Type ID
Code/Kode/Code BDR
Surname/Name/Nom MUSTERMANN
Given names/Vornamen/Prénoms ERIKA
Nationality/Staatsangehörigkeit/Nationalité D
Sex/Geschlecht/Sexe F
Date of birth/Geburtstag/Date de naissance 12.08.1964
ID No./ID-Nr./ID No. C1000000

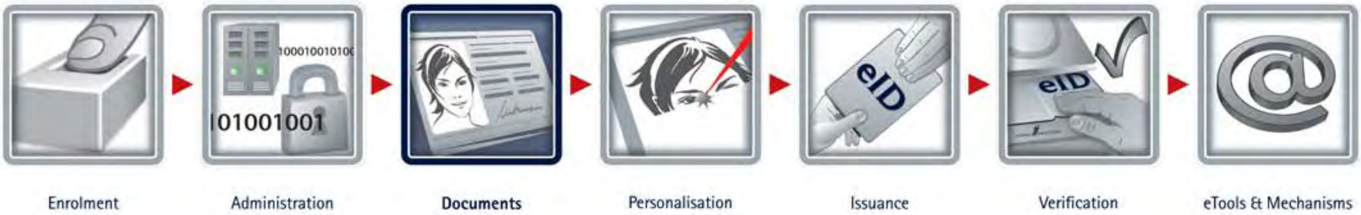
Date of issue/Ausstellungsdatum/Da 02.03.2008
Authority/Behörde/Autorité BUNDESDRUCKEREI
Holder's signature/Unterschrift des Inhabe
Signature du titulaire
E. Mustermann

```
IDBDRC1000000<7<<<<<<<<<<<<<<<
6408125F1803024D<<<<<<<<<<<<<2
MUSTERMANN<<ERIKA<<<<<<<<<<<<<
```

Functionalities	*a) Travel document within EU member states* *b) Authentication for eGovernment and eBusiness applications* *c) Electronic signature (advanced or qualified)*
Specification	• ID-1 card with a contactless chip for electronic storage of personal data and biometric features • Applications according to CENT/TS 15480 European Citizen Card (ECC) • ePassport application according to the EU Directive • High-security design and printing, e.g. guilloches, microtext, DOVD (diffractive optical variable device) with anti-copying / anti-scanning protection • Durable polycarbonate, multi-layer structure
Security processes of the chip	BAC, EAC, Active and Passive Authentication Elliptic Curve Cryptography Terminal Authentication Chip Authentication

▶ Flexible, legally effective and standard-compliant – the innovative ID products from Bundesdruckerei comply with the strict requirements of the German Act on Digital Signature and all current European and international security standards for electronic ID documents. ◀

BUNDESDRUCKEREI SYSTEM PORTFOLIO



closer and more effective partnerships with the International Organization for Standardization (ISO), Interpol, the Airports Council International (ACI) and the International Air Transport Association (IATA).

At the UN level, cooperation between ICAO and the UN Counter-Terrorism Committee Executive Directorate (UN CTED), the more practical arm of the Security Council's Counter-Terrorism Committee (CTC), has also proven very useful.

"The real turning point in how the UN and its partners were able to affect these areas of State activity more coordinatedly came through the development of the Implementation and Capacity Building Working Group (ICBWG)," notes Mauricio Siciliano, ICAO MRTD Officer and Secretary of the ICAO MRTD Technical Advisory Group (TAG).

"Prior to this development, all these Organizations were more focused on their own initiatives. With the ICBWG a new level of coordination was achieved that allowed us to avoid duplication of efforts and truly offer a more harmonized set of programmes and initiatives that touches on virtually every aspect of improved international mobility, security and border control."

As the efforts of these key partners continue to more effectively harmonize the various frameworks and technologies that are now contributing to the safer, more efficient and more globally interoperable systems of travel document processing and passenger throughput being implemented, additional bodies have recently become much more closely integrated into the offering of programmes and initiatives that ICAO participates in to assist and better serve its Member States in this domain.

TABLE 1: ASSISTANCE PROVIDED BY THE ICAO AVIATION SECURITY AND FACILITATION POLICY (SFP) SECTION

Date / Location	Beneficiary	Nature and Purpose
July/August 2008	Bolivia	1) Requested basic information on implementing ICAO Machine Readable Passport (MRP) specifications. Presently, this State is not compliant with Annex 9, SARP 3.10 and the best practices described in Doc 9303. An assistance project was proposed to the Government of Bolivia to assist in the tender process and implementation for a new MRP system compliant with ICAO standards. This project would be established in conjunction with the International Organization for Migration (IOM), which presently has a project management office in La Paz, or with the ICAO Technical Cooperation Bureau. 2) IOM project securing travel documents co-financed with the EU.
October/November 2008	Ecuador	Following a previous mission to Ecuador in August 2007 the government contacted ICAO to request assistance and interpretation on the implementation of ICAO machine-readable visa standards for Ecuadorian consulates around the world. Also, a follow up has been done on the possible implementation project of the Ecuadorian passport modernization as proposed in the ICAO Air Transport Bureau/Technical Co-operation Bureau (ATB-TCB) report that followed the 2007 mission. An invitation was sent to the government to participate in the coming second Best Practices Workshop on MRTD Security to discuss the Ecuadorian mproject and re-launch it.
July/September 2008	Thailand	The Government of Thailand sent a request to the ICAO APAC Regional Office in Bangkok, which then forwarded it to Chief Joint Finance (C/JF). This request was related to the interpretation of specifications contained in Doc 9303, Part 1, Volume 2, and implementation of the ICAO PKD. The questions were addressed and sent back to C/JF for return to the requiring authority.
June/July 2008	Greece	The Delegation of Greece contacted ICAO seeking clarifications regarding the Three-Letter Code list. The issue pertained to the historical origins of the list, and the use of the word "Macedonia" instead of "The former Yugoslav Republic of Macedonia" when describing the State. The same comment was made with respect to denoting the language spoken therein. ICAO provided the Greek Delegation with the relevant explanation and referenced the ISO standards employed by ICAO in this circumstance. This request resulted in an update to Doc 9303 and its Supplement containing the new denomination.
October/November 2008	India	During the TAG/MRTD, the Aviation Security and Facilitation Policy (SFP) Section met with the Indian delegates. They required assistance on the implementation of the ICAO PKD. SFP provided the explanation and the documentation required for the Government of India to proceed with implementation.
December 2008/ January 2009	Kiribati	Kiribati does not yet issue Machine-Readable Passports (MRPs). A joint assessment mission (ICAO, United Nations Counter-Terrorism Executive Directorate (UN CTED) and the International Organization for Migration (IOM)) was performed, focusing on how to upgrade the issuance process to conform to ICAO Standards and specifications.
April/June/July/ September 2008	Mauritius	A request was been received which proposed an assessment mission on how to improve the Mauritian passport issuance process and include biometric information in the State's passport. ICAO has made a proposal and is awaiting a response.
April/May 2008	Mongolia	The Government of Mongolia requested assistance on implementing ICAO Standards for machine-readable visas. SFP Section sent the documentation and additional information required to achieve this.
August/September 2008	Montenegro	The Government of Montenegro requested information on standards and specifications for the issuance of ePassports. ICAO SFP has sent the information requested.
May/June 2008	Pakistan	The Government of Pakistan requested information on applying test methodology to ePassports (durability, reading, etc.). SFP Section provided the technical reports and test methodology they required to implement these tests in their programme.
June/July 2008	Panama	The Passport Office of Panama requested information on capturing facial biometrics for MRTDs according to ICAO's recommendations. SFP provided the respective guideline as published by ICAO.
August/September 2008	Paraguay	A letter from the Paraguayan Embassy in Canada was received requesting an interpretation on implementing Doc 9303 on a Temporary Travel Document for Mercosur (a regional sub-group that includes Argentina, Uruguay, Paraguay and Brazil).
March/May/December 2008	Philippines	The Philippines contacted ICAO SFP regarding the interpretation of Annex 9, SARP 3.10. The interpretation and relevant documentation were sent to the Philippine representatives.

Three organizations now working more closely with ICAO in this area are the Organization of American States' (OAS) Secretariat of the Inter-American Committee against Terrorism (CICTE), the Organization for Security and Co-operation in Europe (OSCE) and the International Organization for Migration (IOM).

High-level cooperation was also on display during last October's 4th ICAO MRTD Symposium. Left-to-right at the head table for this event are: Steven Berti, Chief, ICAO Aviation Security and Facilitation Section (SFP); Dr. Taïeb Chérif, Secretary General of ICAO; Barry Kefauver, ISO; Folasade Odutola, Director of the ICAO Air Transport Bureau; and Roman Vanek, Chief, Identity Documents Section, Swiss Passport Office.

Secretariat of the Inter-American Committee against Terrorism (OAS CICTE)

The main purpose of the CICTE is to promote and develop cooperation among Member States to prevent, combat, and eliminate terrorism. It does this in accordance with the principles of the OAS Charter and the Inter-American Convention against Terrorism, as well as with full respect for the sovereignty of States and the rule of law, including international humanitarian, rights, and refugee-related precedents.

Beginning in 2008, the CICTE joined forces with ICAO's MRTD programme to organize a series of sub-regional workshops on best practices in travel document security through the Americas. In March of that year, the CICTE invited ICAO and INTERPOL to address the annual meeting of CICTE Member States on the topics of MRTDs and the INTERPOL Stolen and Lost Travel Documents (SLTD) database. In June, the CICTE Secretariat and the MRTD Program of ICAO organized a first sub-regional Workshop on Best Practices in Travel Document Security in El Salvador for 44 representatives of Central America (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panama, Mexico, and the Dominican Republic). A second took place in Bogota, Colombia, for 31 representatives of the Andean region (Bolivia, Colombia, Ecuador, Peru, and Venezuela) in November 2008.

The Executive Directorate of the UN Counter Terrorism Committee (UN CTED) joined the partnership for this second event. A third sub-regional workshop will be organized for the Caribbean region in Jamaica in May 2009, and a fourth is planned for the Southern Cone countries of South America in late 2009.

"Experts from North and South America and Europe, as well as from ICAO, INTERPOL, and the OSCE in Europe addressed four main topics at these sub-regional workshops," commented CICTE Secretary, Carol Fuller. "These comprised ICAO's international standards and requirements for travel documents; the integrity of breeder documents and civil registries; travel document handling and issuance procedures; and finally opportunities

info@muhlbauer.com www.muhlbauer.com

Your one-stop-shop equipment & software technology partner for
ID cards and passports/ePassports

Mühlbauer High Tech International

Complete equipment solutions
- Biometric data enrollment & management
- RFID inlay, IC module & ID document production
- Optical, electric and biometric personalization
- Biometric border & access control

Complete software solutions
- Data capturing and processing
- Security document management & PKI
- Integrated production & personalization management
- Automatic border control & authority support

Excellent customer service
- Attractive financing services
- Support services
- Consulting services
- Peace of mind service contracts

Intensively involved in the most ID Card and ePassport projects worldwide

UPCOMING EVENTS CO-ORGANIZED BY ICAO AND THE OAS CICTE:

- Training Course in Document Security and Fraud Prevention for El Salvador, Guatemala and Honduras April 20-24, 2009
- Sub-regional Best Practices Workshop for the Caribbean on Document Security and Fraud Preventions May 4-9, 2009

SHORT-TERM OUTCOMES OF RECENT COLLABORATIONS BETWEEN THE SECRETARIAT OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE) AND ICAO

1) Increased hemispheric compliance with ICAO Doc 9303:

- Greater awareness of Doc 9303, new technologies, MRTDs, eMRTDs, biometrics;
- Greater technical knowledge to improve security of handling and production of documents;
- Greater knowledge for more efficient compliance to security standards;
- Identification of areas of improvement and new tools to assist in the security improvement.

2) The capacity of law enforcement, customs and immigration personnel has been strengthened:

- Greater awareness of INTERPOL's Stolen and Lost Travel Document (SLTD) database and motivation to use it;
- Greater awareness of the need to improve controls on travel and identity documents and detection of fraudulent documents to prevent counterfeiting and fraudulent use;
- Opportunity to exchange information on a sub-regional level;
- Reinforcement of the hemisphere via the participation of various countries of a sub-region.

3) The regional and sub-regional cooperation has been enhanced:

- Networks of international cooperation have been developed via exchanges between the participants and experts;
- Regional strategies to implement ICAO standards and technologies have been promoted and encouraged;
- Data has been shared and has been encouraged to be utilized on a regional basis for inspection operations;
- New impulse to improve the security of manufacturing and issuing identity and travel documents and prevent the alteration or fraudulent use in accordance with the UN Global Counter Terrorism Strategy adopted in 2006.

for international cooperation and several case studies."

Short-term outcomes from the CICTE/ICAO collaborations are shown above.

Organization for Security and Cooperation (OSCE)

With 56 States drawn from Europe, Central Asia and America, the OSCE is the world's largest regional security organization, bringing comprehensive and co-operative security to a region that stretches from Vancouver to Vladivostok. It offers a forum for political negotiations and decision-making in the fields of early warning, conflict prevention, crisis management and post-conflict rehabilitation, and puts the political will of the participating States into practice through its unique network of field missions.

OSCE institutions include negotiating and decision-making as well as operational bodies. They deal with a wide range of OSCE-related issues from arms control to human rights to freedom of the media. In the area of secure travel documents ICAO works primarily with the OSCE's Action against Terrorism Unit (ATU).

At an early stage in the post 9/11 environment, the OSCE recognized the importance of improving travel document security throughout its region to help it succeed in the fight against terrorism. In its Bucharest Plan of Action on Preventing and Combating Terrorism (December 2001), the OSCE participating States committed themselves to:

> *"prevent the movement of terrorist individuals or groups through effective border controls and controls on issuance of identity papers and travel documents, as well as through measures for ensuring the security of identity papers and travel documents and preventing their counterfeiting,* forgery and fraudulent use."
>
> (MC(9).DEC/1).

In 2003, this resolve was further strengthened when the OSCE participating States committed themselves to ICAO's standards for the handling and issuance of passports and other travel documents, including MRTDs and biometric identifiers. Since then, travel document security has formed a major part of the OSCE's counter-terrorism work. Its core task in this respect is facilitating the work of international organizations and major specialized agencies, such as ICAO, and providing a political platform for awareness-raising and pursuing direct technical assistance opportunities for OSCE Participating and Partner States.

Since 2003, the OSCE Action against Terrorism Unit has organized more than 20 capacity building events in co-operation with ICAO and other entities, such as INTERPOL, the ISO, the IOM and the EU.

The contribution of the OSCE in this area has been recognized by national authorities, the international community and the industry alike, and the organization has become a preferred partner in conducting different activities in this field.

"The OSCE has supported the growing partnership between ICAO and OAS/CICTE by providing its knowledge and expertise of project management in the field of travel document security," remarked Dimitar Jalnev, OSCE Programme Coordinator, Action Against Terrorism Unit. "We are convinced that the partnership between global bodies like ICAO and regional organizations like the OSCE and the OAS is mutually beneficial and contributes to the

TABLE 2: ASSISTANCE PROVIDE BY THE OSCE IN COORDINATION WITH ICAO

Date / Location	Beneficiary	Title	Nature and Purpose
February/March 2008 / Podgorica	Montenegro	Forged Document Training	1) Increase operational awareness to detect forged documents. 2) Provide border control officers with the necessary skills to detect, identify and prevent the use of forged documents. 3) Encourage them to disseminate this information in their national structures as national trainers. 4) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 5) Disseminate information on OSCE activities to counter trafficking in human beings.
May 2008 / Berlin July 2008 / Skopje	The former Yugoslav Republic of Macedonia	Expert assessment concerning Extended Access Control and interoperability of data at border control.	1) Fact finding for solutions with the goal of adding interoperable components to the border control system. 2) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 3) Assess Public Key Infrastructure (PKI). 4) Make recommendations on implementation of Extended Access Control.
September 2008 / Bishkek	Kyrgyz Republic	Handling and Issuance Assessment	1) Support vertical integration with SAKS (MoJ) and enrolment (MoI) databases. 2) Improve application process and identity verification. 3) Disseminate international recommendations for breeder documents. 4) Review in-house processing and control mechanisms. 5) Make overall risk assessment and share best practices. 6) Suggest solutions for the digitalization of back records. 7) Facilitate implementation of machine-readable visas. 8) Encourage reporting of lost & stolen document numbers to Interpol.
September 2008 / Ashgabad	Turkmenistan	Forged Document Training	1) Increase operational awareness to detect forged documents. 2) Provide border control officers with the necessary skills to detect, identify and prevent the use of forged documents. 3) Encourage them to disseminate this information in their national structures as national trainers. 4) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database.
November 2007 – March 2009 / Chisinau	Moldova	Deployment of the Mobile Interpol Network Database (MIND) in the Republic of Moldova	1) Assess Moldovan connectivity needs. 2) Raise necessary funds. 3) Deploy relevant technical platforms. 4) Procure related equipment.
February – March 2008 / Podgorica	Montenegro	Forged Document Training	1) Increase operational awareness to detect forged documents. 2) Provide border control officers with the necessary skills to detect, identify and prevent the use of forged documents. 3) Encourage them to disseminate this information in their national structures as national trainers. 4) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 5) Disseminate information on OSCE activities to counter trafficking in human beings.
June 2008 / Banja Luka	Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, The former Yugoslav Republic of Macedonia, Greece, Hungary, Moldova, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, Turkey, UNMIK	I-24/7 Regional Training course for SEE	Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) database and all further law enforcement services and databases accessible via the I-24 network.
May 2008 / Berlin July 2008 / Skopje	The former Yugoslav Republic of Macedonia	Expert assessment concerning Extended Access Control and interoperability of data at border control	1) Fact finding for solutions with the goal of adding interoperable components to the border control system. 2) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 3) Assess Public Key Infrastructure (PKI). 4) Make recommendations on the implementation of Extended Access Control.
September 2008 / Bishkek	Kyrgyz Republic	Handling and Issuance Assessment	1) Support vertical integration with SAKS (MoJ) and enrollment (MoI) databases. 2) Improve application process and identity verification. 3) Disseminate international recommendations for breeder documents. 4) Review in-house processing and control mechanisms. 5) Make overall risk assessment and share best practices. 6) Suggest solutions for the digitalization of back records. 7) Facilitate implementation of machine-readable visa. 8) Encourage reporting of lost & stolen document numbers to Interpol.
September 2008 / Ashgabad	Turkmenistan	Forged Document Training	1) Increase operational awareness to detect forged documents. 2) Provide border control officers with the necessary skills to detect, identify and prevent the use of forged documents. 3) Encourage them to disseminate this information in their national structures as national trainers. 4) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database.
October 2008 / Banja Luka	Bosnia & Herzegovina	Handling & Issuance of Travel Documents in Bosnia & Herzegovina: High-level seminar supporting the introduction of a new travel document.	1) Raise awareness for the recommended ICAO minimum security standards for the handling and issuance of passports as well as other travel documents. 2) Disseminate technical specifications and standards on Machine Readable Travel Documents (MRTDs). 3) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 4) Share best practices on project implementation.

international efforts against terrorism by helping put in place a universal travel document security framework, amplifying important political messages and leveraging resources."

International Organization for Migration (IOM)

The IOM is the leading inter-governmental organization in the field of migration. It works closely with governmental, intergovernmental and non-governmental partners, including ICAO.

With 125 Member States, a further 18 states holding observer status and offices in over 120 countries, the IOM is dedicated to promoting humane and orderly migration for the benefit of all by providing services and advice to governments and migrants. The IOM works to promote international cooperation on migration issues, to assist in the search for practical solutions to migration problems and to provide humanitarian assistance to migrants in need, including refugees and internally displaced people.

Since 2002, the IOM, through its Technical Cooperation on Migration Division, has assisted numerous states in improving their travel document, related issuance processes and identity management. This work has been undertaken with a view to enhancing security in the migration sector, facilitating regional integration and support, and encouraging bilateral initiatives aimed at closer cooperation among countries in the area of migration management.

Recognizing the importance of building support, both technical and financial, from interested partners as well as securing public and private experts, the IOM has resolutely embarked on forging stronger partnership in this field. Supporting the aim of the recently launched ICBWG, the IOM is working closely with the OSCE/ATU in Belarus, and has participated actively in a joint ICAO/IOM travel document assessment in Kiribati at the request of ICAO.

TABLE 3: ASSISTANCE PROVIDE BY THE IOM IN COORDINATION WITH ICAO

Start date	End date	Beneficiary	Title/description
01/Dec/2006	31/Mar/2008	Manila, the Philippines	Workshop Series on Biometric Technology for the Government of the Philippines
01/Jun/2008	01/Jun/2009	Kabul, Afghanistan	Technical Assistance in Passport and Visa Issuance Afghanistan Phase II
18/Jun/2007	18/Jun/2008	Kabul, Afghanistan	Training in Security Standards, Procedures and Fraud Prevention for Afghanistan
01/Oct/2007	31/Dec/2008	Almaty, Kazakhstan	Enhancing Immigration Inspection and Border Control on the Land Border of Kazakhstan
01/Mar/2007	28/Feb/2009	Baghdad, Iraq	Capacity Building in Integrated Border Management at the Southern Borders of Iraq
01/Mar/2007	10/Oct/2008	Jakarta, Indonesia	Capacity Building for Imigrasi in the Field of Migration Management Information Systems
15/Apr/2007	30/Apr/2008	San Jose, Costa Rica	Strengthening of the Passport Issuance Process at the Costa Rican Migration Office
01/May/2007	31/Dec/2008	Kabul, Afghanistan	Afghanistan National ID Card Project
01/Aug/2007	15/Dec/2008	Phnom Penh, Cambodia	International Border Checkpoint (IBC) Project for Improved Border Integrity in the Kingdom of Cambodia
01/Jan/2008	30/Apr/2008	Kinshasa, Congo	Capacity Building in Migration Management at N'Djili Airport, Kinshasa
21/Sep/2007	20/Feb/2008	Nouakchott, Mauritania	Technical Assistance in Securing the Integrity of Travel Documents and ID Issuance Systems in Mauritania
01/Jan/2007	30/Jun/2008	Damascus, Syria	Capacity Building for Border Control Management - Syria
01/Jul/2007	30/Jun/2010	Papua New Guinea	Partnership in Migration Management and Border Control in Papua New Guinea
01/Feb/2008	31/Jul/2009	Amman, Jordan	Capacity Building to Enhance Migration and Border Management in Jordan
01/Dec/2007	31/May/2009	Dushanbe, Tajikistan	Establishment of Training Center for the Border Forces of the Republic of Tajikistan
01/Oct/2007	30/Apr/2009	Kabul, Afghanistan	Capacity Building in Migration Management (IDCU), Afghanistan (Phase III)
14/Jun/2008	12/Jun/2009	Damascus, Syria	Capacity Building for Border Management in Syria - Phase II
01/Jan/2008	31/Dec/2008	Panamá	Equipment and Capacity Building Support for the Department of Migration, Panama
01/Apr/2008	31/Mar/2009	Kinshasa, Congo	Development of the Border Directorate Police National Congolese (PNC) in North and South Kivus
07/Jan/2008	06/Jun/2009	La Paz, Bolivia	Securing Travel Documents, Improving Border Management and Sustaining Return and Reintegration in Bolivia
01/Jan/2008	31/Dec/2008	Dhaka, Bangladesh	Technical Assistance to the Government of Bangladesh for the Introduction of a Machine Readable Passport and Machine Readable Visa Programme
01/Feb/2008	31/Jan/2009	Ankara, Turkey	Supporting Migration and Border Management in Turkey through Capacity Building for Migration and Border Officials at the Local Level
01/Mar/2008	28/Feb/2010	Kiev, Ukraine	Improving Integrated Border Management: Follow-up to the Reinforcing the State Border Guard Service of Ukraine Human Resources Management - HUREMAS 2 (EC)
01/Mar/2008	28/Feb/2009	Kiev, Ukraine	Improving Integrated Border Management: Follow-up to the Reinforcing the State Border Guard Service of Ukraine Human Resources Management - HUREMAS 2 (INL)
26/Mar/2008	31/Jul/2008	Malawi and Namibia	Border Migration Management Assessment for Malawi and Namibia
14/May/2008	31/Aug/2009	Port Moresby, Papua New Guinea	Papua New Guinea Border Management System Project and related Initiatives
01/Oct/2008	30/Sep/2010	Colombo, Sri Lanka	Strengthening Border Management Through Application of Secondary Inspection Regime and Enhanced Data Collection and Sharing – Sri Lanka

"Over recent years we have really welcomed the support and encouragement provided by the ICAO MRTD
team with respect to strengthening cooperation between the various government, international and private sector groups working toward improved travel documentation'" commented David Knight, Head of the IOM Technical Cooperation Division.

"In particular, our recent collaboration with ICAO and the UNCTC, through a joint travel document assessment in Kiribati, represents a model that we can leverage with a wide range of needful States".

With the assistance of the IOM and the additional organizations now participating with ICAO in a wide range of travel document related seminars, symposiums and other cooperative activities, ICAO SFP continues to function as an invaluable instigator and hub for more coordinated international governance and action in the global and common pursuit of more secure and efficient border control and identity management. ■

Fielding questions at the OSCE High-Level Travel Document Security event held last October in Banja Luka. From left to right: Giorgio Blais, OSCE Office in Bosnia and Herzegovina; Sinisa Macan, Director General CIPS, Bosnia & Herzegovina (host); Dimitar Jalnev, Programme Coordinator, Action against Terrorism Unit (ATU), OSCE Secretariat; and Mauricio Siciliano, ICAO MRTD Officer.

TRUSTED WORLDWIDE

SECURE IDENTIFICATION SOLUTIONS FOR A CHANGING WORLD

Datacard Group leads the industry in secure solutions for issuing national IDs, passports, drivers' licenses, smart IDs and e-government applications.

Innovative technologies for ID1 and ID3 documents:

- Color printing and laser engraving technologies
- Custom topcoats with Datacard® Intelligent Supplies Technology™
- Tamper evident features for levels 1, 2 and 3 inspection
- Visual and electronic document verification and authentication

Servicing over 300 government programs in more than 85 countries, governments worldwide trust Datacard Group.

To learn more, visit www.datacard.com/government

©2008 DataCard Corporation. All rights reserved. Names and logos on sample cards are fictitious. Any similarity to actual names, trademarks or tradenames is coincidental.

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

TABLE 4: OTHER EVENTS FEATURING ICAO SFP PARTICIPATION

Dates	Location	Title	Nature and Purpose
Aug-08	El Salvador	Best Practices Workshop on Travel Document Security for the Central American Region (organized by the OAS CICTE and ICAO)	The objective of this workshop was to improve the security related to manufacturing and issuing identity and travel documents, and to increase the State's capacity to prevent and detect alteration or fraudulent use. The workshop served to promote and provide information on issues related to the MRTD Programme. It also helped to: 1) Promote cooperation and the exchange of information. 2) Prevent and control document fraud in accordance with ICAO standards and specifications. 3) Highlight UN Resolution 1373 for universal antiterrorism instruments and the OAS Inter-American Convention against Terrorism.
Oct-08	Montreal	Fourth Symposium on ICAO MRTDs, Biometrics and Security with Exhibition	
Oct-08	Lima, Peru	APEC Business Mobility Group (BMG) Frequent Passenger Programs and Border Facilitation Workshop held in Lima, Peru	The purpose of this mission was to: 1) Make a presentation and promote the MRTD Programme and participate during the Workshop. 2) Establish presence and meaningful partnerships in the region and with the Asia- Pacific Economic Cooperation (APEC). 3) Meet with the Regional Director and professionals of the ICAO Lima Regional Office, and make a presentation of the MRTD Programme to the general office staff.
Nov-08	Bogota, Colombia	Best Practices Workshop on Travel Document Security for the Andean Subregion (organized by the OAS CICTE and ICAO)	The objective of this workshop was to improve the security related to manufacturing and issuing identity and travel documents, and to increase the State's capacity to prevent and detect alteration or fraudulent use. The workshop served to promote and provide information on issues related to the MRTD Programme. It also helped to: 1) Promote cooperation and the exchange of information. 2) Prevent and control document fraud in accordance with ICAO standards and specifications. 3) Highlight UN Resolution 1373 for universal antiterrorism instruments and the OAS Inter-American Convention against Terrorism.
Oct-08	Bosnia & Herzegovina	Seminar on Handling & Issuance of Travel Documents in Bosnia & Herzegovina:High-level seminar supporting the introduction of a new travel documents	1) Raise awareness for the recommended ICAO minimum security standards for the handling and issuance of passports as well as other travel documents. 2) Disseminate technical specifications and Standards on Machine Readable Travel Documents (MRTDs). 3) Raise awareness for INTERPOL's Stolen/Lost Travel Document (SLTD) Database. 4) Share best practices on project implementation.

DILETTA 600i
Inkjet Passport Printer
with integrated RFID Writer

DILETTA ID-Systems
Adam-Opel-Strasse 6
64569 Nauheim
Germany

Tel. +49 / 6152 / 1804 - 20
Fax. +49 / 6152 / 1804 - 22

info@diletta.com
www.diletta.com

Worldwide experience
More than 30000 installations in over 100 countries

Integrated Camera System
for exact positioning of pre-printed passports including OCR and barcode reading (optional)

Integrated RFID Reader / Writer
compliant with the new ICAO specifications and ISO/IEC 14443 type A and B standards for electronic passports (optional)

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

ICAO Regional Seminar

MRTDs, Biometrics and Security Standards

in coordination with the United Nations Counter-Terrorism Executive Directorate (CTED)

6 to 8 April 2009
Abuja, Nigeria

ICAO, in coordination with the United Nations Counter-Terrorism Executive Directorate, will hold its first ICAO MRTD Regional Seminar on Biometrics and Security Standards, April 6-8 at the Transcorp Hilton in Abuja, Nigeria.

An exhibition will complement the Seminar and will serve to highlight important products and services related to MRTDs, biometric identification, security applications and border inspection systems.

Attendees will include officials responsible for national security policies, civil registries, as well as national and other identity issuers and managers. Passport issuing agencies, immigration, customs, police, civil aviation, facilitation and other border control and security authorities will also be in attendance. Officials from airlines and airports involved in passenger service systems, handling of travel documents, facilitation and aviation security should also greatly benefit from the event.

www.icao.int/mrtdseminar/2009

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

www.icao.int

The International Civil Aviation Organization

Answering State concerns: The 2009 Public Key Directory

An interview with 2008 PKD Board Chairman Dr. Eckart Brauer

2009 marks the beginning of a new and more integrated global role for the ICAO Public Key Directory (PKD). The PKD is designed to provide the validation backbone that will assist border control and immigration officials in verifying a given ePassport with respect to issuance, data and holder verification. PKD certificates arguably represent the most essential security-related component in the emerging global ePassport identification and facilitation environment.

As more and more States seek to benefit from the ongoing restructuring of global border control and passenger facilitation infrastructures as a result of recent ePassport implementations, and with a newly-signed operational contract providing new and clearer guidelines related to the PKD's technical, financial and operational objectives, this unique ICAO instrument stands poised in 2009 to assume the full range of its harmonized international verification and validation responsibilities.

The *ICAO MRTD Report* recently spoke to Dr. Eckart Brauer, 2008 PKD Board Chairman, regarding the re-tooling that has been underway to ensure that the ICAO PKD has responded to and continues to reflect the needs of participating ICAO Member States.

***ICAO MRTD Report:* When the ICAO PKD commenced operations in March 2007, it was greeted with little fanfare by the international community. The ICAO PKD Board and other stakeholders within the Organization took a number of steps to address this situation, but it has taken some time for the main issues to be resolved. What is the current status of the programme and what were the major steps taken to address key State concerns?**

Dr. Eckart Brauer: I'd like to begin by addressing the fact that the term "Public Key Directory" may be somewhat misleading for some stakeholders. The current PKD is essentially a distributing body for Document Signer Certificates (C_{DS}) that are included in ePassport chips and not merely the cryptographic keys associated with these certificates.

Secondly, there had been criticism in 2007 that certificates alone would not be sufficient and that the "Master List" concept, which was favoured at that time by European countries such as Germany, would provide additional technical parameters that would improve security and simplify validation. This proposal was endorsed by the ICAO Council at end of 2008 and is to be implemented very soon. Master Lists facilitate the cumbersome diplomatic exchange of root Public Key Information (PKI) certificates between countries. In my opinion this was a crucial concern and with the Council decision it can now be regarded as being resolved in principle.

2008 ICAO Public Key Directory (PKD) Board Chairman Dr. Eckhart Brauer (second from right) receiving Germany's Country Signing Certificate (CSCA or "public key") from ICAO's Air Transport Bureau Director, Folasade Odutola. Dr. Brauer currently holds the position of Senior Officer in Germany's Ministry of the Interior. At left are Christiane DerMarkar, Joint Financing, PKD Officer, and Walter Amaro, Chief Joint Financing and Secretary of the PKD Board. To the far right is Dr. Uwe Seidel, Senior Scientific Officer at the Forensic Institute of the Federal Criminal Police Office of Germany.

A third point of criticism was related to the pricing structure of the PKD. When participation in the PKD programme did not evolve as expected the PKD Board developed a solution which brought improved transparency for State stakeholders. As of now all PKD participants have to pay a specified contribution depending on their activity status. The return on investment which PKD participation ensures is the ability of a participating State's citizens to take full advantage of any ePassport-based streamlining programmes (e.g. border control and passenger facilitation) throughout the world—and without any compromise in overall security levels. The PKD programme is essential to ensure that, in the long term, the ePassport will become the globally interoperable tool that its developers envisaged and not something subject to local variations and proprietary solutions.

What are the cornerstones of the new operational contract that ICAO has signed?

The new operational contract for the PKD was signed at the end of 2008 between ICAO and the PKD operator, Netrust. The major points of interest for all existing and prospective PKD participants are as follows:

1. Participants that are not yet active in the PKD will see their national PKD connection and use periods commence in 2009. This holds true for Germany, the UK, France, Korea and the United States. Canada is also making every effort to meet this 2009 deadline.

2. New PKD participants who sign the PKD Memorandum of Understanding (MoU) in 2009 or later must start their activity in the PKD within 15 months after payment of their one-time registration fee. China and Kazakhstan, who joined in late 2008 after the negotiations with Netrust were concluded, can therefore be expected to commence their PKD activities in 2010 at the latest.

The registration fee is currently $56,000 and covers one-time costs that are required in order to:

- Familiarize newly-joined countries to the Directory's technical requirements.
- Complete the State's registration at ICAO.
- Partially cover the depreciation of assets of the ICAO PKD facilities in Montreal. This contribution will be balanced at the end of the life cycle of those assets—i.e. 2012.

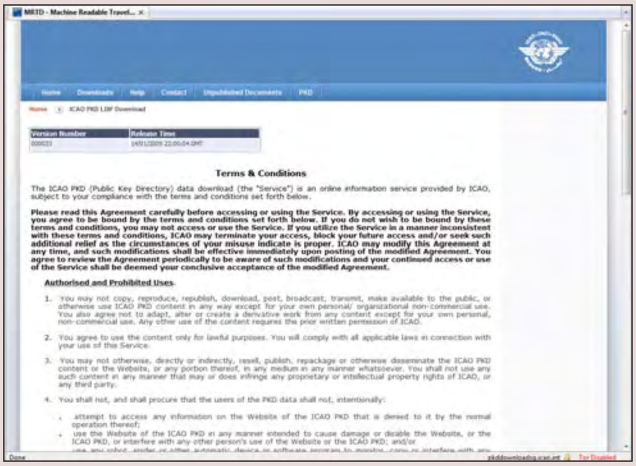
3. The running budgetary contribution or PKD Annual Fee has two major components: ICAO's budget and the PKD operational budget.

4. All PKD Participants contribute equally to the ICAO budget. The ICAO budget covers all administrative costs for the support of the PKD on an institutional level as well as the operation of the ICAO PKD facilities in Montreal. New PKD participants pay a pro rata contribution to the ICAO budget during their first year of PKD participation (calculated on a daily basis). This is then followed by full-year contributions afterwards. For 2009 the budgetary commitment of ICAO is approximately $374,250. With 12 PKD participants at the moment this works out to around $32,000 each for 2009.

DOWNLOADING THE ICAO PKD LDIF FILE

The ICAO Public Key Directory (PKD) can be accessed by anybody to download the Document Signer Certificates (DSCs) and the Certificate Revocation List (CRLs) of the active PKD Participants.

The download URLs are: **https://pkddownloadsg.icao.int** or **https://pkddownloadth.icao.int**



Version Number	Release Time
000023	14/01/2009 22:00:04 GMT

Terms & Conditions

The ICAO PKD (Public Key Directory) data download (the "Service") is an online information service provided by ICAO, subject to your compliance with the terms and conditions set forth below.

Please read this Agreement carefully before accessing or using the Service. By accessing or using the Service, you agree to be bound by the terms and conditions set forth below. If you do not wish to be bound by these terms and conditions, you may not access or use the Service. If you utilize the Service in a manner inconsistent with these terms and conditions, ICAO may terminate your access, block your future access and/or seek such additional relief as the circumstances of your misuse indicate is proper. ICAO may modify this Agreement at any time, and such modifications shall be effective immediately upon posting of the modified Agreement. You agree to review the Agreement periodically to be aware of such modifications and your continued access or use of the Service shall be deemed your conclusive acceptance of the modified Agreement.

Authorised and Prohibited Uses

1. You may not copy, reproduce, republish, download, post, broadcast, transmit, make available to the public, or otherwise use ICAO PKD content in any way except for your own personal/ organizational non-commercial use. You also agree not to adapt, alter or create a derivative work from any content except for your own personal, non-commercial use. Any other use of the content requires the prior written permission of ICAO.
2. You agree to use the content only for lawful purposes. You will comply with all applicable laws in connection with your use of this Service.
3. You may not otherwise, directly or indirectly, resell, publish, repackage or otherwise disseminate the ICAO PKD content or the Website, or any portion thereof, in any medium in any manner whatsoever. You shall not use any such content in any manner that may or does infringe any proprietary or intellectual property rights of ICAO, or any third party.
4. You shall not, and shall procure that the users of the PKD data shall not, intentionally:
   - attempt to access any information on the Website of the ICAO PKD that is denied to it by the normal operation thereof;
   - use the Website of the ICAO PKD in any manner intended to cause damage or disable the Website, or the ICAO PKD, or interfere with any other person's use of the Website or the ICAO PKD; and/or
   - use any robot, spider or other automatic device or software program to monitor, copy or interfere with any

5. All active PKD participants contribute to the PKD operational budget. A full year's activity in the PKD costs $43,000. PKD participants who start their activity during a given year will pay a pro rata contribution (calculated on a daily basis) followed by full-year contributions (for example a half-year contribution would currently be $21,500). It should be noted that the current yearly contribution requirement of $43,000 will be revised downwards once the PKD reaches the 30 participant threshold.

6. The signed PKD operational contract with Netrust is valid for three years.

7. All transitional financial arrangements that came into being during 2008 and earlier are no longer in force.

How are States responding to this new set of financial and operational guidelines?

Though the regulations may seem difficult to understand on first reading they are founded on a rational set of parameters and address concerns which are well-understood by programme participants. I can assure you that these new guidelines provide the necessary transparency and the ability to accommodate all foreseeable financial and technical implications in the medium- and long-term. This is—and I need to underline this point very clearly—exactly what had been sought by the international community. Though there may still be some issues to work through as the programme matures, a State's decision to participate in the PKD can now be taken with the assurance of a sound and predictable return on investment.

How do you respond to the criticism that the 15 month rule, whereby the obligation for a national PKD connection and use implies a contribution to the PKD operational budget, can easily be overlooked by participants and may yet cause unexpected financial consequences?

The 15 month regulation may appear to be a trapdoor of sorts, but any State under that impression needs to take a deeper look at its intentions and consequences. Our top priority is to develop an active global community of responsible PKD participants. It simply wouldn't make sense to go through all the processes and expense related to the introduction of ePassports without at the same time taking proper advantage of the improved security features the ePassport can only deliver with the support of the PKD.

The PKD Board is keen to meet the strategic goals of ICAO with concrete action. Active participation in the PKD is the only way that the promise of ePassport security and facilitation improvements can be fully passed-on by States who have implemented them to the citizens who are paying for them. Last but not least, the 15-month stipulation provided the necessary reassurance that allowed Netrust to feel comfortable about taking on any financial risks related to operating the PKD. ■

> **"Our top priority is to develop an active global community of responsible PKD participants. It simply wouldn't make sense to go through all the processes and expense related to the introduction of ePassports without at the same time taking proper advantage of the improved security features the ePassport can only deliver with the support of the PKD."**
>
> ***Dr. Eckart Brauer***

The HII-point in our future

With almost one-third of its Member States already issuing ePassports, ICAO has begun considering new strategic directions for the future of security and facilitation.

Given the rapid development of information and communication technologies and the rising trend of notification and Automated Border Control systems, a new HII concept that leverages *Hi-tech* deployments (H), *Intelligent* systems (I) and *Integrated* border management (I) is now being contemplated.

Ir. Dr. Raymond Wong, Former Assistant Director and Head of IT Branch of the Immigration Department (HKSAR, China), and Visiting Professor, Jiaotung University (Shanghai), discusses the origins and promise of the HII security and facilitation environment now being envisioned.

Examinations of travelers at the entry and exit points of a State serve important national security and facilitation functions. As the first line of defense, these checkpoint procedures enable the interception of undesirables and individuals with otherwise illicit purposes *before* these unwanted entrants pull attention and resources away from additional state agencies and bureaucracies.

Through professional training and equipped with sophisticated technology, today's border control officers have to decide, within mere moments, whether the person in front of their desks should be allowed to enter their State. An officer's responsibilities during this brief period include the need to check the validity and authenticity of the travel document, verify the identity of the traveler, make sure they're not on the wanted list, input relevant records to the computer system, and reflect the appropriate condition of stay on the travel document.

Most importantly of all, the officer has to establish the purpose of the visit and ascertain if it is a welcome one or possibly a threat to the country. The officer must be allowed sufficient time to accomplish these important tasks effectively.

Unfortunately, the reality is that border control officers are normally not permitted sufficient time to conduct a thorough and prolonged examination over the counter. Globalization, tourism, international trade and business, etc., all account for an ever-rising number of travelers at border check points. This workload surge far outweighs attempts at a commensurate expansion of hardware facilities and human resources that can be deployed to adjust for it. The result is that officers often have to make very quick yet important decisions.

The enduring challenge at border check points therefore is to facilitate

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

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

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

Visit entrust.com/epassport

Entrust® Securing Digital Identities & Information

Entrust and Entrust product names are trademarks or registered trademarks of Entrust, Inc. or its affiliates. All other company and product names are the property of their respective owners. © Copyright 2009 Entrust. All rights reserved.

passenger flow on the one hand while ensuring no compromise of national security on the other. Border control officers have to detect the black sheep from the crowd effectively and efficiently without hampering the swift processing of the vast majority of genuine visitors who bring social, cultural and economic value into the country.

The ICAO doctrine for document security and border control

The ICAO Security and Facilitation Programme (SFP) is committed to a mandate that seeks to maximize facilitation and security at borders. This SFP mission, overseen by ICAO's Member States and facilitated by international cooperation, is implemented in part through the regulations, standards, specifications and recommended practices that it has formulated for this purpose. This guidance helps determine the design and operational requirements relating to travel documents, immigration/ customs systems and procedures, etc.

MRTD and ePassport

Through the concerted effort of Member States of ICAO, significant achievements have been made towards SFP mandate. Specifications for Machine Readable Travel Documents (MRTDs) have been formulated and today almost 90 percent of the member states are issuing a Machine Readable Passport (MRP). Not only enabling the standardisation of document formats, MRTDs facilitate the accurate and efficient input of personal information to computerised systems serving border security and facilitation functions. The ICAO objective of having all Member States issuing MRPs by April 1, 2010, is now very much attainable and not simply a target as it was twenty years ago.

The advancement of technology has accelerated the formulation of MRTD specifications to allow for an even more secure form of travel document: the ePassport. Embedded with a chip containing personal biometrics protected by sophisticated encryption technologies, the ePassport aims at further enhancing document security, in particular the identity of the holder. Moreover, the provision of electronic information also enables more innovative applications for the document under the purview of facilitation and border security.

The commitment of ICAO in promoting the SFP mandate can best be demonstrated by the setting up of the Public Key Directory (PKD) for ePassports now being issued. Not only is this an active operational responsibility, it is also a proactive measure reflecting ICAO's desire to further coordinate international cooperation towards a more efficient and secure SFP environment.

While significant progress has been achieved on the MRTD and ePassport fronts through international cooperation, threats and risks against border security are also transforming to take advantage of new technologies and methods. Globalisation, easy mobility, human trafficking, terrorism, loss and forgery of documents, false identity, etc., are but a few of the factors putting pressure on the ability of States to deliver effective border control.

The rising expectations of travelers for more efficient border examinations that maintain sufficient safeguards for privacy are also compelling authorities to rethink traditional methods.

Initiatives by Member States

Against this background of increased travel volumes and technological progress, ICAO Member States and various Regional organizations have launched a variety of initiatives to cope with their particular situations.

Notification or authorization systems

Australia, which today requires a visa for all visitors, introduced the Electronic Travel Authorization System (ETAS) through which most visitors could acquire travel authorisations in electronic format through local travel agents in a matter of minutes. The system represents a particularly wise application of information and communication technologies and has thus far proven to be very successful.

ETAS has facilitated the Australian visitor experience significantly while maintaining the integrity of the visa regime and broader State security concerns. This model was adapted by Hong Kong, which afterward introduced its iPermit system to facilitate the granting of entry permits (again through travel agents) to Taiwanese residents coming to Hong Kong.

Other States have implemented similar notification systems that enable the early acquisition of arriving passenger information—prior to or immediately after their departure for the destination State. This allows the destination State more time to perform its background check. As of 2008, for example, the U.S. now requires citizens enjoying visa-free status to inform U.S. authorities in advance of any forthcoming visit.

China similarly implemented its Advance Passenger Information System (APIS) in May 2008 to help it prepare for a safer Olympics. Under APIS, information about passengers on board incoming aircraft is sent by the airlines to destination immigration authorities immediately after the departure of the flight. Other Asia-Pacific countries with similar programmes include Japan, Malaysia and Thailand.

Complementing its ETAS system, Australia also utilizes Advance Passenger Processing (APP), through which passenger information is sent to destination authorities during flight check in. Australia-bound passengers are only allowed to board the plane with a green light from Australia in advance. New Zealand, on the other hand, adopted a hybrid system of APIS and APP.

Automated Border Crossing (ABC)

Autogates have become very popular in recent years. Specified travelers or registered users may make use of these installations to streamline immigration formalities through the digital verification of biometric information. This technology was developed in the late 1990s but the Hong Kong implementation in 2004 brought significant enhancements that have since helped to solve its significant border congestion concerns.

Varying ABC applications can now be found in Asia-Pacific countries such as China, Hong Kong, Macau, Singapore, Malaysia, Japan, Thailand, and Australia. In Europe recent installations include the U.K., Netherlands and Portugal. Middle Eastern and in Africa examples can also be found (e.g. Senegal).

ABC increases reliability and efficiency while curtailing the need for increased human resources. It has revolutionized the traditional visual inspection method by officers and, now relieved from their tedious counter work, these officials are able to devote more effort to the observation and supervision of passenger traffic and paying higher attention to possible irregularities.

PASSPORT INLAYS Solutions

Give your Passport the Highest Level of Security

The passive antenna "E-Booster®" is located into the datapage and the module "E-Pastille®" into the coverpage

Solutions including E-Pastille® and E-Booster® into the coverpage also available

Standard : ISO/IEC 14443 A/B, ICAO

Chip Type : Compliant with mains ICAO chips and Operating Systems

Inlay Material : Teslin, PET, PC...

Tel : +33(0)4 42 53 88 36 Mail : contact@s-p-s.com www.s-p-s.com

Smart Packaging Solutions

ABC is particular effective at clearing low risk travelers. It is predicted that there will be significant development of ABC systems in coming years, to tie in with the capabilities and wider application of the ePassport. The experiences so far enjoyed by the RAPID system in Portugal and SmartGate in Australia are good reference models.

The HII concept

With almost one-third of the its Member States already issuing ePassports, it is an opportune time for ICAO to think ahead and begin charting the strategic course for new initiatives relating to its broader security and facilitation mandates. Given the rapid development of information and communications technologies and the rising trend of notification and ABC systems, a concept that focuses on the capabilities relating to Hi-tech deployments **(H)**, intelligent systems **(I)** and Integrated Border Management **(I)** is now being envisaged.

Hi-tech deployments (H)

The ePassport has demonstrated that advanced technology can be employed to help border control authorities perform their tasks more effectively. Hi-tech solutions not only enhance security and facilitation, but additionally their innovative application will revolutionize processes in manners not previously achievable through traditional methods. Let's illustrate with a few examples.

Apart from ABC, the ePassport should have great potential for additional applications. At the moment, its benefits accrue primarily to nationals of the issuing state, and not for foreign visitors. This situation arises because of the legal requirement of endorsing the condition of stay on the passport. It is by no means inconceivable, however, that condition of stay information could be electronically written to and read from an ePassport chip.

Similarly, the ePassport chip could potentially be used to store visa or travel authorizations as well as serving as a boarding pass. With Radio Frequency Identification (RFID) technology, the boarding ePass could provide a unique identifier for the passenger and even facilitate luggage tracking and self service functions inside the airport.

The Netherlands already has an aggressive plan to make use of ePassports as unique identifiers for self-service facilities in the newly-renovated Schiphol airport as of 2012. The self-serve facilities under discussion there include check-in, luggage hold areas, immigration and boarding control.

In general, a wider application of biometric tools is now being envisaged to assist with future challenges. With more accurate and reliable products as

ETAS IN AUSTRALIA

THE PROMISE OF AN INTEGRATED HII OPERATIONAL SYSTEM

The following is a hypothetical description of the type of security and passenger facilitation environment that can be envisaged based on logical evolutions in existing and projected ePassport and border control capabilities:

Before the trip

Once a reservation is made with a travel agent or carrier, the passenger information, preferably an electronic copy of the bio-data page of the travel document, including the holder's facial biometric, will be passed to concerned border control authorities in real-time for information and authorisation, as required. Background and relevant checks, including identity verification, will be conducted to properly categorise the passenger as a welcome or problematic visitor. This allows more time for the border control authorities to prepare for the visit.

During the trip

At the carrier's check-in counter, the travel document of the passenger will be scanned and the personal information that's captured will be used as a unique identifier for luggage check-in, boarding and the compilation of an electronic passenger manifest. The personal information will be verified at each stage against previous stage results and the electronic passenger manifest will be forwarded to relevant parties—the receiving border control authorities in particular—for arrival preparation.

Upon arrival at the destination biometric facial verification will be conducted through images captured by CCTV. Tracking functions of the system would allow sufficient time to provide the verification and categorisation of the passenger.

When arriving at their border check point, the welcome visitors will be channeled to the intelligent ABC system for simple self-service immigration checks while doubtful visitors will be directed to manned counters for careful examination.

After the trip

On completion of the visit—that is, after the departure of the passenger—the system will automatically conduct an evaluation of the whole journey from all sources of information to identify irregularities and inadequacies for assessment and future improvement.

well as rigourous attention to privacy concerns, many future applications for border check points serving security and facilitation purposes are now in much closer reach.

One scenario could see images of disembarking passengers captured by CCTV installations equipped with simultaneous facial recognition capabilities for identity verification. While tracking functions through the CCTV and RFID then help to detect passenger movement irregularities or illicit activities, swifter ABC checking will have already been initiated since the identification process will have started from the moment the passenger disembarked from their aircraft.

One particular application where biometrics should be employed as soon as possible relates to the passenger manifest. Scanners are already commonly installed in immigration counters and airlines could employ this technology for check-in purposes. Digital passenger information could be captured at this stage and then utilized for various purposes, including but not limited to the compilation of a electronic passenger manifest both for green management and more effective verification purposes.

Another of today's loopholes that could be plugged by advanced technology involves the real-time distribution of lost and stolen passport information and wanted lists to all Member States. While Interpol has already been taking proactive action to help make this ability a reality, there remains an obvious and urgent need for this service to help provide border control officers with the most up-to-date national security information.

Lastly, the designs of contemporary auto gate-type systems are not intelligent enough and still require too much human supervision and intervention. Even today, however, technological advances are beginning to address these issues.

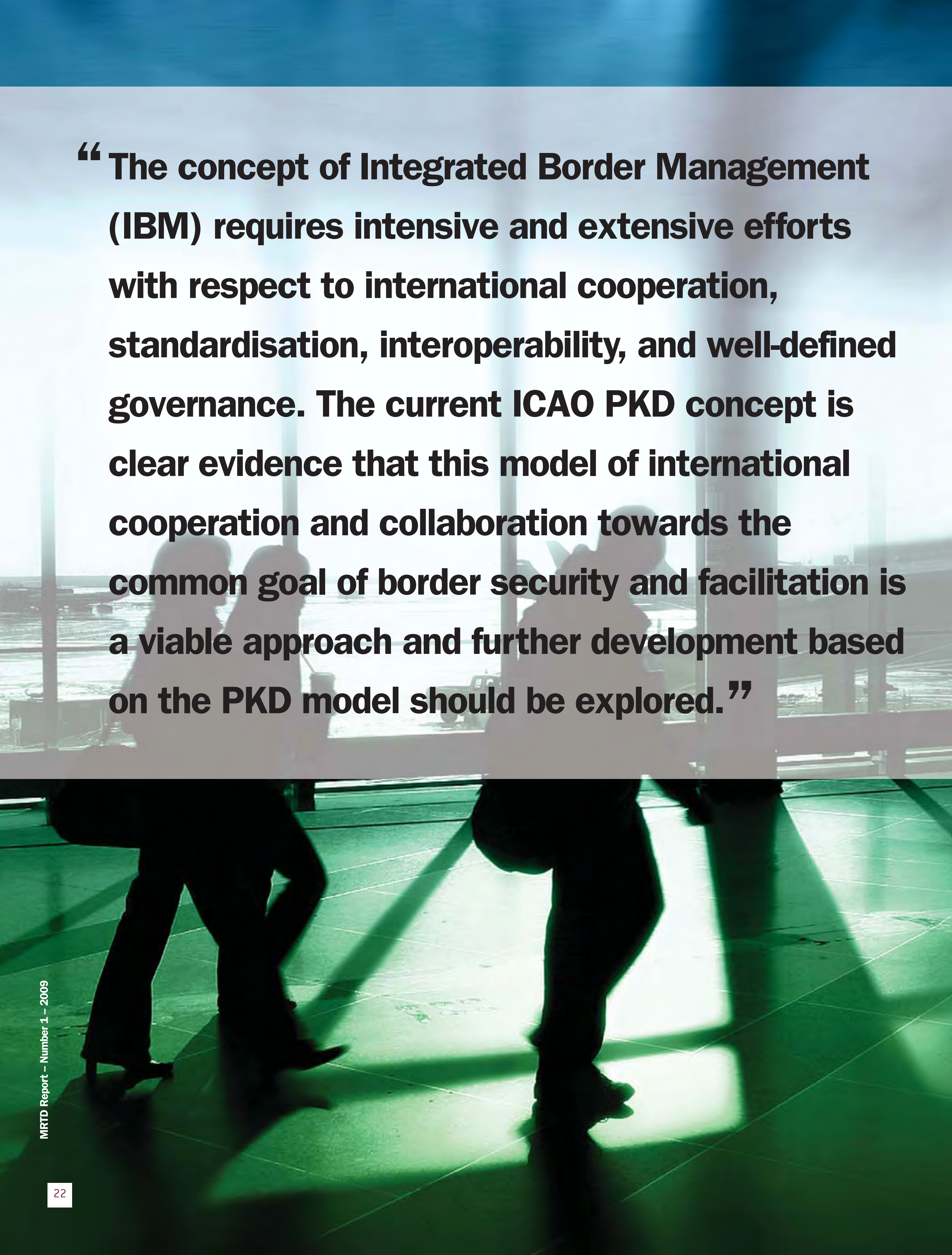
The above examples are offered as humble predictions regarding the future application of advanced technologies to security and facilitation objectives. Though by no means exhaustive or conclusive, it is hoped that they might stimulate further thought in this regard and eventually more innovative designs.

Intelligent Systems (I)

Advanced technologies should be employed intelligently and integrated with existing or new information and communications developments to achieve the broadest possible synergies. With appropriate systems design, for example, an electronic passenger manifest generated by the personal information captured at the airline check-in counter can be sent to respective border control authorities for advance passenger processing, background checking and biometric identification. With ever-increasing digital abilities and lowering costs, intelligent systems can be devised to serve various business and operational needs for States.

An important element of a well-designed intelligent system is that it should have learning capabilities. With artificial intelligence and case learning capability, future systems will become smarter and more powerful with time, thus providing useful functionality and additional services for operators.

The ultimate goal should be the perfect match of the system and the business needs of the authorities. The system, no matter how intelligent it is, should be designed to serve



“The concept of Integrated Border Management (IBM) requires intensive and extensive efforts with respect to international cooperation, standardisation, interoperability, and well-defined governance. The current ICAO PKD concept is clear evidence that this model of international cooperation and collaboration towards the common goal of border security and facilitation is a viable approach and further development based on the PKD model should be explored.”

and not to replace border officials. Wisely devised, it will be an enabling and empowering tool allowing a single border control official to do the work of many. The ABC system is a vivid example already in use. Under traditional visual examination methods, one officer can man just a single counter, whereas with an ABC system an officer is able to supervise five to ten autogates.

Integrated Border Management (I)

Though there is a rising trend in Regional cooperation, border management remains a primarily internal affair of each individual state. Today's challenges, however, have called for a wider and more innovative level of cooperation among States and stakeholders across the entire travel and border control sector. The concept of IBM is therefore proposed as a means to enable the lateral and vertical integration of processes by related stakeholders, with a view to a more rationalized work and information flow geared toward greater border security and facilitation.

Lateral integration calls for full integration and cooperation between travel and border control sectors, including travel agents, carriers and border control authorities. There could be instantaneous sharing of information where there is a common interest so as to enhance efficiency and eliminate redundant processes—all while each stakeholder maintains a high level of autonomy and authority within their core businesses. Needless to say, important privacy, legal, administrative and commercial issues relating to standardization, and greater interoperability will have to be addressed.

Vertical integration requires coordinated action and sharing of information *before, upon* and *after* the passenger journey. Information and data collected before the actual journey by the travel agent or carrier could be transmitted to other stakeholders receiving the passenger; instance; i.e. the destination border control authorities. Feedback after the fact could be sent to all handlers along the route for analysis and evaluation.

The concept of IBM is therefore to integrate the whole world or all Member States of ICAO as one big family or entity under one super system so that any movement of a person within the system entails immediate and automatic transactions like notification, approval, reporting, exception handling, identity verification and identification, etc. Each state would maintain its own autonomy in the design and operation of its own parts of the system, so long as these did not affect the overall interoperability and communications goals of the broader apparatus.

ICAO well-positioned to lead the HII evolution

The concept of IBM requires intensive and extensive efforts with respect to international cooperation, standardisation, interoperability, and well-defined governance. The current ICAO PKD concept is clear evidence that this model of international cooperation and collaboration towards the common goal of border security and facilitation is a viable approach and further development based on the PKD model should be explored.

The need for the leadership of an internationally trusted body in any such endeavour would be absolutely necessary. ICAO is an obvious choice in this regard and its tremendous success with the ePassport thus far indicates that it is well-prepared to assume these responsibilities. ■

Simplifying ePassports and the ICAO PKD

In this overview of the electronic security features of an ICAO-compliant ePassport looked at from an inspection systems perspective, Tom Kinneging, Project Manager at Sagem Identification and Task Forces 2 and 5 Leader at the International Organization for Standardization, looks at how storage technologies offer automated inspection systems the means to verify, through biometric technology, the identity and validity of a passport holder.

In this recap of his presentation to the 2008 MRTD Symposium, Kinneging discusses the ICAO Public Key Infrastructure, certificate chains, certificate distribution mechanisms, and the effective use of keys and certificates in the travel document inspection process.

Tom Kinneging is a Senior Project Manager with Sagem, formally STU Identifications. He is the leader of Task Forces 2 and 5 in the ISO SC-17 Working Group 3, responsible for the development of standards for securing information electronically stored in travel documents. Kinneging also worked as editor of both the Technical Report on Public Key Infrastructures for MRTDs and a supplement to ICAO's Document 9303 as part of his responsibilities with the ICAO New Technologies Working Group (NTWG). He is currently leading the development and certification of Sagem's extended access control solution for the next generation of ePassports.

A new global hub for MRTD suppliers and information!

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

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

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

www2.icao.int/en/MRTD2

I would like to share a little history with you. There is a sketch by a famous painter (and fellow Dutchman), Rembrandt van Rijn. The sketch depicts a scene from the Bible of Isaac, as an old man, blind and in his bed. Before he dies, he needs to fulfill an old tradition, which is to bless his eldest son, who then can become his heir.

Isaac had two sons: the eldest was Esau and the youngest was Jacob. Isaac asked Esau to shoot a deer and prepare a meal from this deer, for which Isaac would give him his blessing. The mother of the two sons, Rebecca, overheard this. She had more love for Jacob than for Esau, and she wanted Jacob to receive the blessing. She secretly sent out Jacob to shoot a deer and bring it to her, so she could prepare the meal for the father.

But how could they fool Isaac? Esau was a big strong guy, with lots of hair on his chest and arms, and Jacob was much smaller, smooth and bald. Their father would definitely recognize the difference, but as Isaac was old and blind Rebecca had an idea.

In Rembrandt's picture, you see Jacob at his father's bed, bringing him the meal prepared by his mother. His mother had the bright idea to stick the deerskin on Jacob's arms to make him appear hairy. His father gave Jacob a hug, felt the deerskin and assumed it was Esau. So Isaac enjoyed the deer and gave his blessing to Jacob. This made Jacob the main heir and the next father in the family.

What do we learn from this story you might ask. First, we learn that Rembrandt was a great painter. Secondly, we learn that, even over 3000 years ago, proper ways of verifying someone's identity were necessary. Over time this resulted in the development of security identity documents and, beginning a few years ago, the introduction of ePassports. We'll now look at some of the security features in our modern passport documents that may have been useful to Isaac all those years ago.

A Kinegram is an optical device used in passports today that changes its appearance depending on the angle from which you view it. Besides being a nice, glittering object to look at and admire, the Kinegram is also a powerful security feature that enables you to detect, for instance, the copying of or attempts to copy a passport page. If, for example, the Kinegram covers a passport's photograph partially, and if one tried to attempt fraud by changing this photograph, the Kinegram would be damaged and the alteration would be discovered.

Border officials are selected and properly trained to carefully inspect the Kinegram. They depend on the Kinegram's features to detect fraud attempts. But if the inspector were not so properly trained or was blindfolded, he would not be able to perform his inspection. In such a case, the Kinegram remains a powerful security feature but is of no use.

The electronic microprocessor in an ePassport stores data and can perform cryptographic calculations. Besides being a nice storage place for biometrics, for instance, the chip is also a powerful security feature enabling you to detect copying. A feature called active authentication in the microchip can detect both copying and attempts at altering the data. These detections use the passport identification mechanism and therefore are fairly similar to the Kinegram.

Current inspection systems are designed to carefully inspect the electronic security features performed by passive and active identification. If the inspection system is not properly designed or lacks necessary information, it becomes unable to carefully inspect the electronic security features. While features such as the Kinegram and chip remain powerful, therefore, they become of no use and fraud would go undetected within the context of a deficient inspection regimen. Therefore it is important to properly design inspection systems so that they can benefit from the latest security features.

But which features must the inspection system check? It must check the features to detect counterfeit and manipulation by performing passive authentication. It must perform active authentication to check for copying or cloning attempts, while also taking care of the bearers' privacy.

A mechanism called basic access control takes care of that. Before you can do anything to check for counterfeit manipulations or copying, you must perform this basic access control process to get access to the chip at all. Within this process, some information that is visually present on the data page, such as document number, date of birth and date of expiry, is used to calculate keys that enable you to access the chip. Before that, you cannot access the chip and, by this means, the system forces you to open the document.

It's worth remarking that you cannot read this information from someone's back pocket. The keys provide access to the chip but also encrypt the communications between the chip and the inspection system. Only upon completion of the basic access control steps can one start reading and inspecting the chip contents.

By putting a so-called electronic signature in the chip, the inspection system can, by verifying the signature, check that the personal data in the chip is authentic. The personal data is stored there by a genuine issuing authority and cannot be changed afterwards. This mechanism is called passive authentication because it does not require the chip to actively perform calculations. The chip merely stores the signature and the inspection system verifies it.

Passive authentication is based on calculations with the cryptographic key pair. The issuer uses the private key to create an electronic signature. By keeping this private key very secret, the issuer takes care that he's the only one who's able to do this. Private keys and public keys belong to each other and enable inspection agencies to verify electronic signatures; therefore the issuer has to distribute these public keys to the relevant inspection systems all over the world.

In the LDS data structure in which the information on the chip is stored, data group 1 is the machine-readable zone, data group 2 is the facial image, and so on. Each data group is represented by a so-called document security object, and this representation is referred to as a hatch number. A hatch number is a unique representation of the contents of such a data group. The security object is digitally signed using the private key of the issuer. This allows the security object to select the perfect table of contents off the chip.

If an inspection system needs to verify which data groups are present, it is highly recommended that it checks this security object and not the so-called EF.com file, which is present on the chip as specified in ISO specifications. EF.com files are not signed and could be altered by an attacker. The security object cannot be altered because of the digital signature.

Principled Secure Solutions Since 1897

cbn
CANADIAN
BANK NOTE
COMPANY, LIMITED

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

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

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

www.cbnco.com
identification@cbnco.com

Let us suppose for a moment that an attacker manipulates the contents of one or more data groups, for instance data group 1 and data group 2. The hatch values in the document security object, also stored on the chip, would not belong to these data groups anymore. By having the data group read and comparing this information with hatch numbers from the security object, an inspection system could easily detect that the data groups had been manipulated.

There are also clever attackers, of course, and a clever attacker would not only alter the data group contents but also the hatch numbers in the security object. Hatch number calculations are public algorithms so it's rather easy to do, but what he cannot do is change the digital signature because he is not in possession of the private key of the issuer, and therefore, a passive authentication check by the system would signal that there's something wrong and the attempt would be discovered.

Of course the use of private keys and public keys requires that the inspection systems trust and use the public keys for verifying these digital signatures. ICAO specifications provide some means to realize this objective.

Suppose that State A issues passports. It would use a private key to create a digital signature in the passport chip. The system that performs this action is called a document signer. It signs the passport. This means that the document signer's public key needs to be distributed in a way that the receiving party can use it and trust it. For this purpose the public key is stored in a so-called certificate computer file. And since the document signer affects a lot of ePassports directly, its lifetime is relatively short—about 3 months—after which time the keys are renewed. Therefore, it is very difficult to distribute these keys. You cannot carry them around and give them to inspection system owners.

Consequently, we need more efficient ways to distribute certificates. We cannot hand them over, so how can the receiving party, if we send them to it, trust the public key? For that purpose, the certificate also has a digital signature, placed there by a higher authority called the Country Signing CA, which uses its own private key for signing the certificate of the document signer. This means that, if we want to verify a certificate, we need the public key of this CSCA.

How then can we effectively distribute this? By storing it in the certificate. The certificate, again, needs to be signed and so on, but the Country Signing Certificate Authority (CSCA) signs its own certificate. The document signer certificates with this public key can be distributed, for instance, by publishing it on the ICAO public key directory and inspection systems can download the certificates from this public key directory. But it could also be stored on the passport chip itself and, in that way, would be carried to an inspection system by the traveler.

In all cases, the inspection system requires the means to verify the authenticity of the certificate, and therefore must obtain, and trust, the CSCA certificates. Trust can be provided in the CSCA certificate by exchanging it bilaterally—handing it over from one person to another. Since the lifetime of the CSCA certificate is 3 to 5 years, this approach seems feasible.

The CSCA certificate must be used by the inspection system to verify the authenticity of the document signer certificate, and the document signer certificate can be used to verify the document's security object in the chip. After this the passport can finally be inspected. So it's all a matter of trust, and trusting the certificates and the public key contained in it is provided by the higher authority signing it. The highest level in the tree is the CSCA certificate which places its trust in its provider through bilateral exchange.

In practice, over the past few years, this bilateral exchange appeared to be problematic and difficult to achieve. Many States encountered problems in receiving the CSCA certificate from other States, but a mechanism has been developed that might help. It is called the CSCA Master List. This is nothing more than a fellow State signing a list of CSCA certificates it has received and validated. Other States may trust the certificates in this list based on the fact that apparently, they are trusted by this fellow country, the issuer of the list.

For example, State W has bilateral exchanges with states X, Y and Z. State W would publish a CSCA Master List and, in this way, inform other states that it uses the certificates from X, Y and Z (as well, of course, as its own certificates). Any other State may use this list to obtain CSCA certificates it didn't obtain bilaterally, and trust it, based on the trust State W places in them. Such a Master List could, for instance, be published on the ICAO Public Key Directory.

In the same way, State Z may have a bilateral exchange with state A, issue a master list containing the certificates of State A, State W and State Z itself, and publish this list. Again, this is away for State W to obtain the certificates of State A. Hopefully this provides a more efficient way to exchange these important certificates than the bilateral exchange.

There are various means available that enable the inspector to verify the authenticity and integrity of the chip's data. To make use of these features, the inspection system needs to be prepared by storing the trusted CSCA certificates, obtained either bilaterally or through a CSCA Master List. The inspection system also has to check certificate revocation lists compiled by issuers of certificates. Such lists are used by an issuer to inform the world of revoked certificates. Certificates you use in your inspection system should not appear on such a list, so check them regularly.

digital identification solutions

Real Secure eID / Driving License Solutions

EDIsecure® LCP 9000 Anti-Conterfeit Security Technologies:

- Tactile Laser Engraving
- Color Retransfer Printing
- High-Res UV Printing
- Custom OVD Lamination
- Smart Chip Encoding
- Multiple and/or Changeable Laser Image
- Allows Flexible Combination of Security Features
- Makes Credential Forgery and Manipulation all but impossible

Digital Identification Solutions also offers the ICAO compliant *EDIsecure*® ePassport and Visa program for secure personalization of MRTDs as well as *IDExpert*® Identity Management Software.

Let us find the perfect secure credential solution for you!

www.digital-identification.com

CARDWARE LAMINATION PASSPORT SOFTWARE CAPTURE PRINTER BIOMETRIC

THERE IS ONE FOR EVERYBODY

The inspection system also needs to have a trusted document signer certificate in it. It can be read from the chip of the traveler or can be downloaded from the ICAO PKD. In both cases, it should be verified using these higher-level CSCA certificates.

The complete inspection process then would proceed as follows:

- Access to the chip should be established with the basic access control mechanism.
- When the document signer certificate has been read from the chip, it should be verified with the CSCA. The digital signature of the document's security object should be verified with the document signer public key.
- Next, a data group of interest can be read, using document security objects as an index to determine which data groups are present.
- The hatch number of the data group should then be calculated in order to compare it with the hatch number of the signed security object.
- Finally, data trust is established and the data can be used in the inspection process.

Although passive authentication enables the inspection system to detect alterations of the data, it is always possible to read the data from the chip and copy it into another chip. The data, including the security object and its digital signature, are static, so copying is in fact possible. Active authentication is the anti-copying mechanism, defined as an option by ICAO.

An inspection system can check that the personal data it has read comes from the genuine chip it was written to by the issuer. In active authentication, we also use a cryptographic key pair.

In this case, both keys, the private key and the public key, are stored on the chip itself. The public key is stored as part of the data in the logical data structure, which is verified through passive authentication, and thereby checked for its integrity and authenticity. It can be trusted. The private key is stored in the chip's secure memory. This memory area cannot be read out or copied; only the chip itself can use it to perform calculations.

In active authentication, the inspection system reads the data from the logical data structure. It can verify the authenticity of this active authentication public key stored in a data group—Data Group 15 (DG 15), in this case—and then the inspection system would send a number, a random number, to the chip, with the request to encrypt this number using the secretly stored private key.

The result of the calculation is returned to the inspection system and, by verifying the result using the corresponding public key (the trusted key), should result in the same number that we generated originally. If this is the case then we know that the chip and the data belong to each other.

But again, the inspection system must perform this. With active authentication no preparation is necessary. Both keys that you need are stored on the chip and once we check the presence of DG 15 (to see if active authentication is supported) the presence of DG 15 can be checked using the document security object.

It requires to be stressed here again that the EF.com file should not be used for this purpose, since an attacker could have removed the DG 15 entry from this file and no one would detect it because it's not digitally signed.

DG 15 should therefore be read out next and passive authentication should be used to verify its integrity. Then the challenge number should be sent to the chip and signed with the private key stored in it. The received response should be verified using the public key from DG 15. And last, but not least, one should compare the printed machine-readable zone on the data page with the machine-readable zone on the chip in DG 1, and then you will know that the data page and the chip also belong to each other.

For the inspection of even newer passports, we all know of so-called computer scientists or security specialists (better known as hackers), who claim they are able to crack ePassports. In all cases, these guys base their claims on assumptions surrounding the inspection process, such as the absence of active authentication or verification of the document signer certificates with the country-signed public key.

Press coverage of these incidents omit any mention of these assumptions, therefore the community reads only half the story based on half-blind inspection systems. The attempts are nothing new. In 2005 and 2006, Dr. Uwe Seidel and I already demonstrated that it is possible and even fairly simple to clone an ePassport chip, but we also showed that measures exist and are sufficient to enable you to detect it, as long as your inspection system is properly designed.

One recent story I heard claimed that the attacker could outwit an inspection system by misleading the famous golden reader tool, which did not verify the country-signed CA certificate. Please note that the golden reader tool is not an inspection system. It is simply a tool to quickly check the basic functionality of an ePassport.

No one has ever made the press by claiming that they were able to crack the security provided by a transparent Kinegram based on the assumption that an attack inspector at the border would not be looking at it. Of course, this will not happen to you. Your inspection systems will perform proper and complete inspections.

Proper and complete ePassport inspection was tested in recent trials at Frankfurt airport in Germany. About 100,000 passports were read, with 25% being ePassports. Most of them were fine. 5,000 passports could not be checked properly because the CSCA certificate was not available in the inspection system.

I recommend that you please exchange your CSCA certificates. Issuers, please take initiatives to distribute your CSCA certificates. Inspectors, please take initiatives to obtain CSCA certificates from the issuers.

About 12 serious red flags came up as a result of these trials. Nine of these showed that there were wrong hatch values in the security objects, which all originated from the same issuer. All nine had the same document signer, therefore it was determined there had been a temporary production problem. In one case, a manipulation of DG 2, the one containing the photograph in the chip, was detected. Since the hatch value in the security object did not match with the hatch value calculated by the inspection system, the comparison failed and the passive authentication mechanism detected this mismatch.

In two cases, there was a complete fake discovered. Probably a complete new self-programmed chip was inserted or glued into the passport and an active authentication key pair was created and stored in that passport. Its own digital signature was created with its own document signer. Upon first look it appeared fine, but the document signer did not verify to the country-signed CA of the issuing state because the attacker could not have done so. Finally, the attempt was detected by passive authentication by performing the complete verification of the chain of certificates up to the CSCA.

The inspection of these ePassports proved to be a success and the fakes were quite easy to detect, but clearly one must perform complete inspections. One must obtain the necessary certificates and regularly check their validity by getting the certificate verifications list.

In summary, use the features provided but note that it is not the 'e' alone which comprises the security aspects of travel documents. The electronic features now available are extremely powerful if handled and checked appropriately, but form only part of the complete concept of the document. ■

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

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

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

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

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

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

Biometric system An automated system capable of:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Laser-perforation A process whereby images (usually personalized images) are created by perforating the substrate with a laser. The images may consist of both text and portrait images and appear as positive images when viewed in reflected light and as negative images when viewed in transmitted light.

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

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

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

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

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

Metallic ink Ink exhibiting a metallic-like appearance.

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

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

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

Multiple biometric The use of more than one biometric.

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

One-to-many Synonym for "Identification."

One-to-one Synonym for "Verification."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UV Ultraviolet light.

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

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

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

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

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

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

Gemalto: the fastest* ePassport

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

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

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

Gemalto's Sealys eTravel operating systems are used in more than 21 national ePassport programs worldwide including Côte d'Ivoire, Estonia, Denmark, France, India (diplomatic), Norway, Poland, Portugal, Qatar, Singapore, Slovenia, Sweden and the United States of America.

Now you know who's behind.

* 2,6 seconds for a full EAC transaction with 48 KB of data, RSA 1024 and extended length (EAC tests in September 2008)

www.gemalto.com

gemalto
security to be free

© 2009 Gemalto. All rights reserved Gemalto, the Gemalto logo are trademarks and service marks of Gemalto NV and are registered in certain countries. Photo credits: Jupiter Images. February 2009 CC

Helping Solve the Global Challenges in Managing Identity

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

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

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

L-1 IDENTITY SOLUTIONS™

SECURE CREDENTIALING DIVISION

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

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

www.L1id.com/ICAO

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