MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Also in this issue:
OSCE Collaborative Efforts with ICAO, INTERPOL and the IOM
Argentine Identity and Passport Advances • e-MRTD Project Contract Development
39 Myths About e-Passports: Part II • MRTD Glossary of Terms

Vol. 5, No. 2

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

GET. Faster

The new eP600 from GET Group is the fastest retransfer printer ever introduced for personalizing ICAO compliant ePassports. With high print resolution, fully automatic book processing, and biometric interface, the **eP600** continues the Toppan legend of state-of-the-art printers for both centralized and decentralized passport issuance.

GET. Into the future

ICAO MRTD REPORT
VOLUME 5, NUMBER 2, 2010

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: +1 (514) 886-7746
E-mail: info@philbin.ca
Web Site: www.philbin.ca

Production and Design
Bang Marketing
Stéphanie Kennan
Tel: +1 (514) 849-2264
E-mail: info@bang-marketing.com
Web Site: www.bang-marketing.com

Advertising
Keith Miller, Advertising Representative
Tel: +1 (514) 954 8219, ext. 6293
Fax: +1 (514) 954 6769
E-mail: kmiller@icao.int
Web: www2.icao.int/en/mrtd2

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

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

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

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

Printed by ICAO

Contents

Identity Management for Safer, More Secure Travel

Government agencies depend on L-1 Identity Solutions to provide complete secure ID issuance and authentication, and to help protect citizens against crime perpetrated by fraudulent identities. Ensuring that travelers are who they claim to be — and assuring the legitimacy of IDs presented at ticket counters, airport delivery gates, and border crossings — is a matter of global security affecting the entire travel industry.

L-1 Identity Solutions produces millions of secure government-issued IDs each year, including ID solutions around the world. Our solutions and services include:

- Enrollment Services including ICAO-Compliant Biometric Images
- ID Authentication for Airport Employment, Passenger Screening, and ID Workflow
- Multi-Biometric Identification
- ICAO-Compliant ID and Passport Book Production
- e-Gate Border Management Solutions

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

Visit us at the 2010 ICAO Symposium and CARTES!

Protecting and Securing Personal Identities and Assets

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

L-1 IDENTITY SOLUTIONS™

SECURE CREDENTIALING DIVISION

978-215-2400 / SCDinfo@L1ID.com

April 2010:

A Deadline Achieved and new Challenges Identified

Around the world today, ICAO Doc 9303 is continuing to have a transformative effect on the scope and substance of border security and passenger facilitation advances.

As of the ICAO Machine-readable Passport (MRP) compliance deadline of 01 April 2010, only 20 of ICAO's 190 Member States were not yet issuing MRPs, and 12 of these were projected to have fully functioning MRP programmes in place before the end of the year. This latter figure is based on ICBWG research which has confirmed that the 12 States in question have either engaged in tendering processes or are implementing the required technology to issue MRPs according to ICAO Standards and Specifications.

As we move past the April compliance deadline, I would be remiss not to acknowledge the many individuals and organizations that have played such an important part in helping to realize this remarkable achievement. They are too many to mention here individually, but it is clear to me and to anyone familiar with the MRTD field that without the extraordinary collaborative contributions of the past few years there would be a far greater number of States still outstanding with respect to basic MRP compliance.

As with all accomplishments, the achievement of almost universal global MRP compliance has only served to reveal the next great challenges ahead. As I write to you today, I look out towards the even more interoperable and seamlessly secure border control and passenger facilitation scenario that advances in MRTDs and e-Passports are now making possible, with ICAO and its MRTD programme remaining at the forefront of the comprehensive collaborative frameworks that will enable this new era in international travel.

This realization of the promise inherent in new e-Passport and biometric technologies is precisely the purpose and objective of our next decade in the MRTD field. It is why ICAO launched the Vision2020 initiative at last year's Fifth Symposium and it is why now, more than ever, stakeholders must continue to reach out to one another and create the links that will enable our seamlessly secure future.

A good example of how ICAO is continuing to lead in this area was in evidence at the recent ICAO Regional Seminar on Machine Readable Travel Documents (MRTDs), Biometrics and Security Standards in Montevideo, Uruguay. ICAO and the Latin American Civil Aviation Commission (LACAC), with the support of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) and the United Nations Counter-Terrorism Committee Executive Directorate (CTED), organized and contributed to this excellent example of outreach and assistance.

Though designed to highlight the relevance of ICAO's MRTD Programme to a key provision [2(g)] in Security Council Resolution 1373 (2001), the Montevideo event and other capacity-building efforts of this nature are also allowing States to become much better informed about newer passenger facilitation technologies being enabled in our new MRTD era. These are dramatically improving cross-border travel experiences for passengers even as they make borders more secure.

Other feature stories in this issue, most notably the overview of Argentine identity tools and travel documents, as well as the OSCE review of some of its 2009 collaborative outreach efforts, clearly reference the Standards contained in Doc 9303 in addition to ICAO's new Vision 2020 initiative—which has laid out a number of strategic, policy level goals to take full advantage of, and put fully at State disposal, the newest technologies driving travel document, border control and identity management processes.

ICAO's work in this area, however, does not begin and end with the development of appropriate Standards. The Organization is also closely involved in many efforts aimed at improving the ability of States to implement new MRTD or e-Passport programmes, and the next instalment in the article series on this topic from HJP Consulting continues in its objective to provide very useful MRTD-related project management advice to States.

As we approach the Sixth Symposium on ICAO MRTDs, Biometrics and Security Standards, to be held this coming November in Montreal, I look forward to the new insights and reports of even further progress being made in our domain that will undoubtedly be featured in the many practical and provocative presentations we have in store for you.

Happy reading.

Mauricio Siciliano
Editor ■

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	Ms. I.O. Sosina	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		

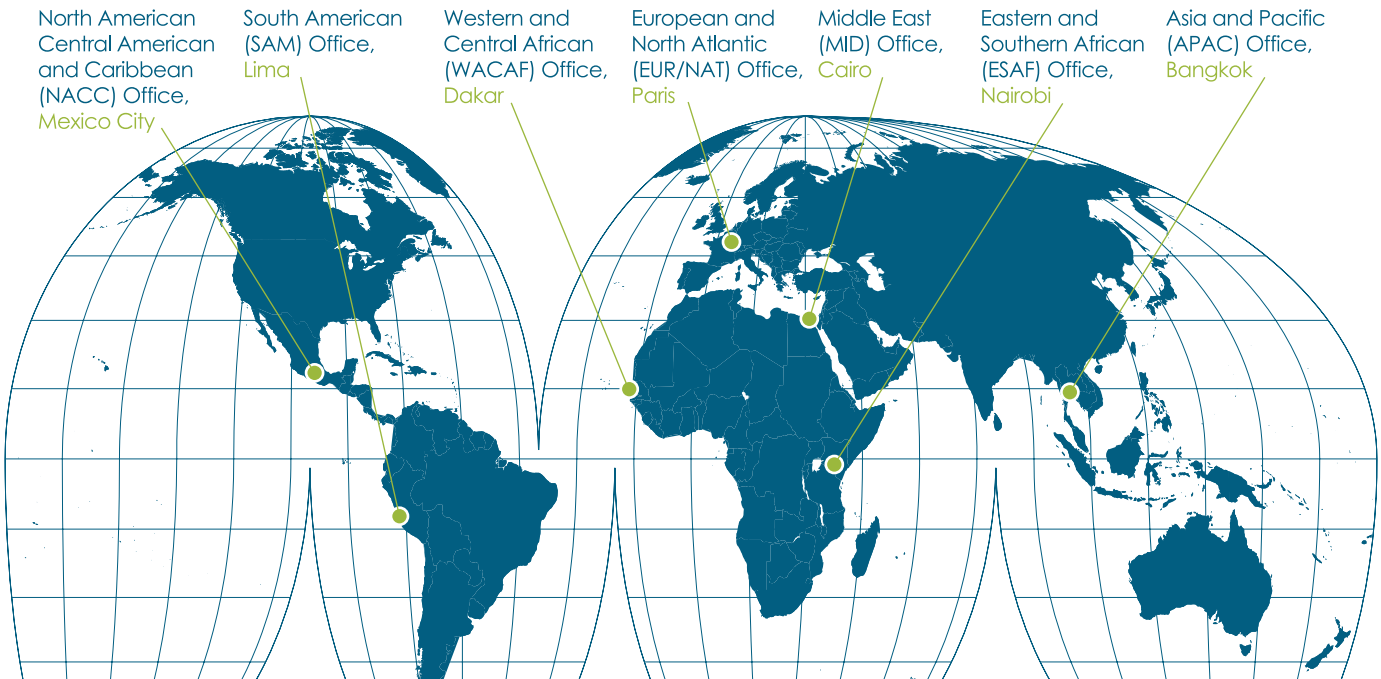
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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)
International Organization for Migration (IOM)
United Nations (UN)

ICAO's Global Presence



Staying in contact?

Global e-Passport and MRTD advances are happening all around you at the speed of travel. 24/7. To keep current and stay in touch with the decision makers who matter most, post a new listing or renew your existing value offering on **ICAO's MRTD Community Web Site,** the world's most succesful hub for MRTD professionals and the States who need them most.

For more information regarding listing your company on our site, or to enquire about new advertising opportunities for the MRTD Web Site or ICAO's widely-read *MRTD Report*, contact:

Carmen Kasrelevitz • ckasrelevitz@icao.int • +1.514.954.8219 ext.7090
Keith Miller • kmiller@icao.int • +1.514.954.8219 ext.6293

ICAO • OACI • ИКАО
国际民航组织 • ايكاو

www2.icao.int/en/MRTD2

Argentine Identity Documents

Seeing the Benefits of ICAO Standards

In the last few years, Argentina has introduced various types of new travel identification for its citizens in accordance with ICAO Standards. These Standards have provided the basis for the design, programming, production, issuance and international acceptance of all Argentine travel and identity products.

As Counselor Julio Ferrari Freyre, Argentina's Director of Travel Documents in its General Directorate of Consular Affairs for the Ministry of Foreign Affairs, International Trade and Worship reports, the standardization of Argentine travel document design and information has aided in the facilitation of travel, from check-in through immigration and customs checks. This is valid during departure from a citizen's country of residence or upon their arrival at, or transit through, destination and third countries.

Since November 2009, Julio C. Ferrari Freyre has been Director of Travel Documents in the General Directorate of Consular Affairs of the Argentine Ministry of Foreign Affairs, International Trade and Worship. He is also a member of the Argentine Inter-ministerial Commission for the Facilitation of Commercial Air Transport. Freyre originally entered the Argentine Foreign Service in 1984, serving at the State's Consulate in Bilbao (Spain) and its Embassy in Beijing (P.R. China).

▶GOT A TEENAGER? THEN YOU PROBABLY KNOW THIS EXPRESSION.

www.bundesdruckerei.de

SORRY, BUT FOR US IT'S PERFECT.

▶ Please do not smile. Seriously. No smiles please, because the passport with biometric data requires a neutral facial expression. That way the document is safe from forgeries and abuse. Sorry about that – but you probably wanted to look cool anyway. ◀

BUNDESDRUCKEREI
We are family

Travel document guidelines from ICAO relating to their production, personalization and issuance assures document trustworthiness and aids in reducing the risk of these identity tools falling into the wrong hands.

A travel document is only valid so long as the personal information that it reflects has been subject to due diligence and adequate systems of authentication. Officials who approve these measures must therefore be absolutely certain that the person to whom the document is being issued really exists, and that the information being attributed to them has a clear chain of custody and authenticity.

Ensuring all of these steps on the path to document issuance is of tremendous value to the development and maintenance of proper civil registry files. Accordingly, the insistence on this point cannot be more strongly emphasized: a document is only as trustworthy and useful as the veracity of the information it contains.

The first machine-readable passport was introduced by the Argentine Federal Police in 1995. This document was prepared following the directives and recommendations of the ICAO MRTD programme and was, in many respects, the model which many countries subsequently emulated.

The same company which produced this 'MERCOSUR' passport, as it is now commonly referred to, also produced travel documents for several other countries in addition to establishing a joint venture with the Ministry of Public Security of the People's Republic of China for its citizen's passports.

In 2009, the contract between the supplier of the MERCOSUR passport and the Argentine Federal Police ended, partially due to financial considerations. This contract included the supply of passport booklets and the necessary software for the personalization and registration of the documents.

The possibility of this happening had been considered in advance by the Argentine authorities and, accordingly, preparations had been put in place so that a new document could be designed incorporating newer technology, improved security and improved methods of capturing user data while maintaining centralized production.

The new document was aptly called the 'Contingency' passport since, along with the cancelation of the old contract, a new electronic passport was by that time already on the drawing board. The Contingency version was seen as a way of closing the gap between both.

Accordingly, in October 2009, the Federal Police started issuing the new Argentine Contingency passport—not without the occasional difficulties which a new document and new software can sometimes bring about. The fact that these issues were quickly rectified, and that production and issuance got underway at relatively short notice, speaks greatly of the persons involved and the vision they had from the start. This quick adaptation and response was also assured in part by new technological developments and by the practical, forward-looking framework which ICAO Standards and Recommended Practices (SARPs) continue to provide regarding all travel documents.

Specimen copies of this new Argentine document, together with a CD describing the security measures and other information contained in it, were also sent to foreign governments as an additional measure helping to ensure its acceptance by foreign border control officials.

Additionally in 2009, the Argentine Ministry of Foreign Affairs started to issue new Diplomatic, Official and Military Mission Passports. These were also designed on the basis of ICAO Standards. The new documents use modern technology and security elements which make forgeries or adulterations very difficult, featuring integrated photographs, data pages printed on foil and a variety of other security elements.

Similar to the standard Argentine documents, centralized personalization processes decrease the possibility of blank Diplomatic, Official or Military documents falling into the wrong hands.

"The unending work carried out by ICAO in this field has helped standardize many important aspects of Passport and identity documents, simplifying international travel and establishing a Standard which—when met—aids the passenger, government authorities and transport agents. In short, ICAO-Standard travel documents serve as the great facilitators of international travel and border security."

Additional Argentine Identification Tools

As previously noted, the security of any type of travel Document depends on the veracity of the breeder documents which a citizen presents to their State. While the most common document used as a basis for a Passport is a birth certificate, Argentina also has a second internal document which can serve this purpose: its National Identification Document or *Documento Nacional de Identidad* (DNI).

The origin of the DNI goes back to 1901, when military conscription was introduced in Argentina. In 1912, the same document, then called the *Libreta de Enrolamiento* (Enrolment Document), was modified to incorporate proof that a citizen bearing it had voted in elections (voting in Argentina has been obligatory since the adoption of its 1853 Constitution).

"The first machine-readable passport was introduced by the Argentine Federal Police in 1995. This document was prepared following the directives and recommendations of the ICAO MRTD programme and was, in many respects, the model which many countries subsequently emulated."

Later, women were eventually permitted to register for elections and the *Libreta Cívica* (Civic Document) was created for them. Fortunately, women did not have to worry about military service. In 1968, both of the Civic and Enrolment documents where amalgamated into the DNI.

The end result of the DNI process is that all Argentine citizens are registered by authorities at the national level for identification and voting purposes. The process of issuance of the DNI (and also the two older identification documents mentioned) includes photographs, fingerprints, and other personal information which is obtained from the holder's birth certificate.

The DNI number is assigned to a person at birth and it is used for all official documents including identification cards, driver's licenses, passports and, with a slight modification, for tax registration purposes. Accordingly, the same number appears on a variety of documents which facilitates identification, registration and probing for police or criminal records.

The presentation of the DNI is obligatory for all official business by citizens, including school registration, opening bank accounts or obtaining credit cards, and—especially—requesting a passport.

The DNI has recently received a facelift and now meets the ICAO Standards for identification documents in addition to its local purposes. The new DNI has an integrated photograph printed on foil and several additional types of security measures. What is more, the document has now changed colour, from dark green to light blue.

The new look has been accompanied by remote capturing of photographs, fingerprints and personal data which can be compared with existing records—including those only accessible via older, paper-based formats. Personalization is also centralized which improves the obvious security factors.

As a final point, it should be mentioned that foreigners who are temporary (more than six months) or permanent residents of Argentina are also registered and have DNI's in a dark red shade numbered from 92.000.000. These have not changed as yet, although the method of issuance has been simplified.

It is possible to carry out the verification of data and identity quickly, which is regularly done by government authorities for a variety of purposes.

The Federal Police also issues an *Cédula de Identidad* (Identity Card), similarly designed to Doc. 9303 Standards, a process which has furnished the added advantage of providing photograph and fingerprint files for approximately 21 million Argentines and other permanent residents since the 1920s (all persons, that is, who at one time or another have sought an Argentine Passport or Identity Card).

The insistence of Argentine authorities on the use of fingerprints for identification purposes is due to the work carried out in this area by Juan Vucetich. His method has been in use since 1891 and, when Military Service was introduced in 1911, all males had to be fingerprinted. Later, when women were registered, they also had to go through the same process.

Today it is possible to travel between the MERCOSUR and Associated countries with national identification documents, such as the DNI and the different identity documents used by

Argentina's National Identity Document as well as its Police, Official and Diplomatic Passports.

Argentina's modern 'Contingency' passport, its Diplomatic variant, and the older 'Mercosur' travel document (blue).

each country. The quality of the documents that may be used must provide certainty and have a high degree of security. Compliance with applicable ICAO Standards greatly aids with the acceptance, practicality and security of these documents.

Consular Security Page

A final point which may be of interest to MRTD Report readers is the *Folio de Seguridad* (Security folio or page) used by the Argentine Consular Service since 2001 to legalize and certify documents. Although this is not a document per se, it serves the very important purpose of insuring that any identity documents are legally acceptable and have been certified as such in an Argentine Consulate by an authorized officer.

This foil used for the Consular Security folios/pages has a very finely offset printed background, special security features, and carries the signature and stamp of the Consular official. They can be easily traced and electronic recording of their sending, reception and use at a Consular office can be monitored. This simple tool has helped to effectively reduce the use of false certifications regarding immigration and customs functions in the Consular Service.

Conclusion

Travel Documents have the dual function of identifying a person and allowing him or her to cross frontiers. Their security and trustworthiness is of fundamental importance for the citizen who travels for pleasure or work in a world that is beset

The consular Security folio/page eliminates the need for further certification of documents and the associated costs. This form of consular intervention is accepted by all national and provincial authorities for the securing of all personal documents leading to the holder's eventual resident status.

The Security page also makes it very easy to verify any documents that have been processed by Consular officials. This has helped to greatly reduce fraud and the related counterfeiting of documents used by immigrants and travellers. The Security folios also have an important incidence in documents used in international trade, such as invoices, certificates of origin, etc.

by illegal activities, of which international crime, terrorism and drug smuggling are but a few.

The unending work carried out by ICAO in this field has helped standardize many important aspects of Passport and identity documents, simplifying international travel and establishing a standard which—when met—aids the passenger, government authorities and transport agents.

In short, ICAO-Standard travel documents serve as the great facilitators of international travel and border security. ■

OSCE Travel Document Security

Advancing Global Border Control Effectiveness and Collaboration

The OSCE has, for a number of years, been actively promoting the implementation of ICAO travel document Standards to its stakeholders. In 2009, assistance requests to the OSCE increased considerably and, in cooperation with ICAO, the OSCE responded by conducting awareness-raising workshops, training courses and technical assessments.

As Christopher Hornek, Ben Hiller and Dimitar Dimitrov of the OSCE Action against Terrorism Unit (ATU) explain in this report, their organization has recently expanded the scope of its collaborative efforts by intensifying important capacity-building efforts with ICAO and other organizations, such as INTERPOL and the IOM. They report here on the progress achieved thus far and on the OSCE's near-term ambitions for further advancing global border control effectiveness and collaboration.

Christopher Hornek joined the OSCE Action against Terrorism Unit (ATU) in 2003 and is the Assistant Programme Officer for Travel Document Security, the OSCE's largest counter-terrorism programme.

Ben Hiller, Assistant Programme Officer, joined the ATU in 2007 and is jointly responsible for the portfolios on Travel Document Security, Cyber Security and Counter-Terrorism Network.

Dimitar Dimitrov worked on Travel Document Security as an intern in the ATU in 2009.

The OSCE Travel Document Security Programme is guided by the OSCE's principle of comprehensive and cooperative security.

OSCE participating States have agreed on a comprehensive travel document mandate that includes the standards and specifications of new documents, the issuance process and the ramifications of these factors on effective border control. In providing assistance across these areas, the OSCE provides a platform where standards, expertise and financial contributions come together to provide capacity-building opportunities. The OSCE Action against Terrorism Unit's (ATU's) core tasks of facilitating the work of standard-setting organizations and major specialized agencies, such as ICAO and INTERPOL, are reflected prominently in such endeavours.

OSCE cooperation with INTERPOL, established to promote improved connectivity between INTERPOL's databases and national border control operations, has similarly been growing steadily since 2004. This work has resulted in the development of joint technical assistance projects for Moldova, Kyrgyzstan and Tajikistan that provide border control officers with integrated real-time access to INTERPOL's databases through a machine-assisted travel document check.

In the last two years, the OSCE also has partnered with the International Organization for Migration (IOM) in joint assistance efforts undertaken in Belarus and Armenia.

Electronic Documents and the ICAO PKD

Since the 2003 Maastricht Ministerial Council Decision on Travel Document Security *(see sidebar, below),*, numerous OSCE participating States have introduced and subsequently enhanced MRTD issuing systems. To date, the majority of these MRTD upgrades have focused on electronic passports, though the benefits of using a chip are also applicable to identity cards when issued as machine readable official travel documents, in line with the standards and specifications of ICAO Doc 9303, Part 3, Volume 2.

THE 2003 MAASTRICHT MINISTERIAL COUNCIL DECISION ON TRAVEL DOCUMENT SECURITY

In 2003, the Maastricht Ministerial Council decided that all OSCE participating States should aim to comply fully, by December 2004, with the minimum security standards for the handling and issuance of passports and other travel documents as elaborated by the International Civil Aviation Organization (ICAO). Additionally, all OSCE participating States were expected to begin issuing machine readable travel documents (MRTDs), if possible with digitized photographs, by December 2005. Moreover, the Decision envisages the standard issuing of passports with one or more biometric identifiers.

The ICAO Implementation and Capacity Building Working Group (ICBWG) estimates that, by the end of 2009, 54 OSCE participating and Partner States will be issuing e-MRPs. On a global scale, the ICBWG calculates that more than 65 million e-Passports are now being issued annually, a fact which only underscores the need to participate in and use the ICAO Public Key Directory (PKD).

In 2009, the OSCE participating States recognized the need to promote the ICAO PKD as *the* globally interoperable validation system for e-MRTDs. The OSCE initiative began in July, 2009, with a food-for-thought paper and a presentation by the Chairman of the PKD Board, Dr. Eckart Brauer, to the OSCE Security Committee. Discussions in Vienna continued until the 2009 OSCE Ministerial Council in Athens that December, where the participating States adopted a ministerial commitment to participate in the ICAO PKD.

Human Element of Border Control

Despite the growing volume of electronic passports in circulation, inspection processes around the world still depend in large part on the physical security features of the travel document. On numerous occasions, the OSCE has received feedback that border control officers cannot keep track of newly-designed document security features and/or new forgery methods.

In response to such feedback and following on assistance requests from participating States, the ATU, together with the

2009 OSCE MINISTERIAL COUNCIL DECISION:
TRAVEL DOCUMENT SECURITY – ICAO PUBLIC KEY DIRECTORY

Key Points:

Recalling the OSCE commitments to counter terrorism, in particular to enhance travel document security… and acknowledging the significant contribution by the OSCE in the area of travel document security,

Recognizing the need to enable relevant national authorities to effectively validate the authenticity of electronic security features and biometric data stored in e-MRTDs as a precondition for the verification of the identity of the bearer of an e-MRTD on the basis of the aforesaid features and data,

Taking note of the work by ICAO in developing the ICAO PKD to promote a globally interoperable validation system for eMRTDs in order to significantly improve border security measures and thereby to contribute to counter terrorism and to the prevention of illegal cross-border activities,

Calls on the participating States to consider becoming participants in the ICAO PKD, subject to administrative and financial resources, and thereby to contribute to enabling border control and other relevant national authorities to validate digital signatures of electronic e-MRTDs.

Tasks the Secretary General to organize, within available resources, in coordination with the Chairmanship-in-Office and in co-operation with ICAO an OSCE expert workshop in 2010 in Vienna, designed to raise awareness and to facilitate the participation in and the use of the ICAO PKD by the participating States.

Borders Team of the OSCE Secretariat, have developed a training course designed to provide participants with the necessary skills to detect forged documents. Through a competitive examination, the course also helps to identify promising students who are in a position to further disseminate these skills as national trainers.

To this end, the OSCE, using a training programme developed by the Austrian Federal Ministry of the Interior, created a project template entitled: *Increasing Operational Awareness to Detect Forged Documents*. The template is typically implemented as a two-week course, but can be tailored to the needs of the beneficiary. This course comprises modules such as document printing, document security features, and document forgery methods as well as the means of identifying them. To enhance interaction between the trainers and the students, the OSCE donates basic forensic equipment which can be used to help participants identify forgeries during case studies.

Since September 2007, 11 such training courses have been organized by the OSCE Secretariat and OSCE field missions. In 2009 and 2010, training courses for border control officers were held for:

- Turkmenistan in the Turkmenbashi Province.
- Turkmenistan in the Dashgouz Province.
- Belarus in Minsk (organized within the framework of the IOM MIGRABEL project).
- Tajikistan in Dushanbe.
- Turkmenistan in the Lebar Province.
- Turkmenistan in the Mary Province.

OSCE Cooperation with INTERPOL

To promote the use of INTERPOL databases, the ATU organizes regular training sessions to inform about the use and benefits of real-time access to INTERPOL's Stolen/Lost Travel Document Database (SLTD), Stolen Motor Vehicles database (SMV) and Wanted Individuals database (Nominals).

In coordination with the Norwegian Police, the OSCE and the Interpol General Secretariat (IPSG) also have launched technical assistance projects

Photos courtesy Guncha Nepesova.

Gerold Glechner, a consultant with the Austrian Ministry of the Interior, discusses travel document concerns with officials from Turkmenistan.

"The recently established OSCE PKD mandate will launch a new area of capacity-building focused on increasing the participation and use of the ICAO PKD throughout the OSCE area. The OSCE's focus on handling and issuance predominantly encompasses implementing ICAO minimum security standards, which place a solid and enduring emphasis on the traditional aspects of document issuance."

that provide hardware, software, web services and the capacity-building needed to connect to INTERPOL databases. This can be achieved through a multitude of technical solutions for a wide cross-section of a country's law enforcement community.

The OSCE, however, specifically focuses on bringing real-time INTERPOL access to border control inspection officers. In order to promote both security and facilitation, the OSCE's current goal is to integrate INTERPOL database queries into the machine-assisted check of any given MRTD. The following is a review of two recent projects in this regard.

Moldova

The first of these INTERPOL-related technical assistance projects was developed for Moldova in November 2007, after a needs-assessment mission attended by the ATU, IPSG, Norway and Lithuania on the one hand, and the Moldovan National Central Bureau Chisinau (NCB), Border Service, Customs Service, and Ministry of Information Development (travel document issuing authority) on the other.

The resulting project equipped 51 border control lanes and 11 police stations with the hardware required to realize

Photos courtesy Guncha Nepesova

Juergen Duftschmied and Gerold Glechner of the Austrian Ministry of the Interior consult with local officials during the OSCE's recent Forged Document Training event in Turkmenistan.

2010 OSCE EVENT SUPPORTS ICAO PKD

From 27–28 May 2010, the OSCE Action against Terrorism Unit (ATU), jointly with the ICAO Secretariat and the ICAO Public Key Directory (PKD) Board, organized the OSCE Workshop on *Promoting the ICAO PKD*, in Vienna, Austria.

Over 200 participants from 53 OSCE participating States and partner States, the private sector and other international organizations discussed the technical, financial and administrative details related to participating in the ICAO PKD.

The workshop was the first step towards implementing an OSCE Ministerial Council Decision from 2009, in which OSCE States committed to consider participating in the ICAO PKD as part of their ongoing efforts to further enhance travel document security in the OSCE region.

Currently, 54 OSCE participating States and partner States are issuing e-Passports. The workshop sought to close the gap between e-Passport issuers and PKD participants by outlining the inseparable link between the two programmes and the advantages of the PKD through national case studies and expert presentations.

The workshop built on the comprehensive OSCE mandate in the area of travel document security. The OSCE ATU, in co-operation with ICAO and INTERPOL, currently assists OSCE participating States with upgrading electronic travel document security features, enhancing handling and issuance procedures, facilitating connection to INTERPOL databases, and improving the detection of forged documents.

real-time queries against the INTERPOL databases. The project also provided web services for the NCB to analyze, develop, test and implement the database interface and to define a national workflow so that hits are resolved quickly and efficiently. The project was funded by Norway, the Czech Republic and Lithuania.

Kyrgyzstan and Tajikistan

Building on the momentum developed in Moldova, the OSCE and INTERPOL designed a similar project for Kyrgyzstan and Tajikistan to connect 10 border control points in each country to INTERPOL's databases and to support the building of databases for travel document issuance and border control purposes. The project is being funded by Norway.

The OSCE/INTERPOL project in Kyrgyzstan and Tajikistan will complement another INTERPOL project for all five Central Asian States funded by the European Commission, which will focus on connecting law enforcement headquarters throughout all five Central Asian countries to INTERPOL's Global Police Communications System I-24/7.

Cooperation with the IOM: Leveraging Resources and Expertise

Since 2008, the OSCE has strengthened its co-operation with the IOM, a move which produced new synergies and

reinvigorated a valuable partnership. Cooperation between the two organizations has been fortified by mutual participation in ICAO's ICBWG, an arena where new initiatives can be coordinated to provide timely and effective responses.

The partnership with IOM's Technical Co-operation Division supports one of the ATU's guiding principles: to implement assistance activities through the effective utilization of resources while avoiding duplication.

WHAT IS THE OSCE?

With 56 participating States from Europe, Central Asia and North America, the Organization for Security and Co-operation in Europe (OSCE) forms the largest regional security organization in the world.

The OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation. It has 18 missions or field operations in South-Eastern Europe, Eastern Europe, South Caucasus and Central Asia.

The Organization deals with three dimensions of security: the politico-military; the economic and environmental and the human dimension. It addresses a wide range of security-related concerns, including arms control, confidence- and security-building measures, human rights, national minorities, democratization, policing strategies, counter-terrorism and economic and environmental activities. All 56 participating OSCE States enjoy equal status and decisions are taken by consensus on a politically, but not legally binding basis.

Belarus

In Belarus, the IOM invited the OSCE to join a project it had developed with the European Commission entitled: *Strengthening Migration Management in the Republic of Belarus (MIGRABEL)*. Subsequently, the Belarusian Ministry of Internal Affairs invited the OSCE to formally participate in the MIGRABEL project platform.

Within the MIGRABEL framework, the OSCE in 2009 helped co-organize two capacity-building events with the IOM in Belarus. In addition to the aforementioned training course on identifying forged documents, the OSCE and IOM co-organized a Travel Document Security Conference for Belarus entitled: *Biometric Applications in Electronic Machine-Readable Travel Documents and Issuance Systems*. The 75 participants included international experts from Lithuania, the Netherlands, Sweden, United Kingdom, United States, the Commonwealth of Independent States, the European Commission, IOM, INTERPOL, ISO, OSCE, the UN Counter-Terrorism Committee Executive Directorate (UN CTED) and United Nations Development Programme (UNDP). Domestic participants came from a number of the government's

"In order to promote both security and facilitation, the OSCE's current goal is to integrate INTERPOL database queries into the machine-assisted check of any given MRTD. The following is a review of two recent projects in this regard."

Ministries and agencies, in particular from the Ministry of Internal Affairs—the Belarusian travel document issuing authority.

Armenia

In Armenia, the IOM invited the OSCE to contribute to a project called: Support to the Armenian Government in Introduction of Identity and Travel Documents with Biometrical Parameters, which was developed by the IOM at the request of the Armenian Police.

The primary goal of OSCE and IOM cooperation was to deliver a National Action Plan for the introduction of an e-Passport and ID Card in Armenia. To achieve this outcome, the OSCE, IOM and an ICAO expert conducted a needs-assessment mission in Yerevan that focused on the main government stakeholders: the police; Ministry of Economy; Central Bank, and Ministry of Foreign Affairs. The joint report provided recommendations and guidance on technical issues, policy and procedures related to both the e-Passport and the ID card. The OSCE/IOM National Action Plan was recently presented to a cross-section of the government's subject matter professionals, convened under the auspices of the Prime Minister's Office.

To complement the plans for an MRTD/biometrics upgrade in Armenia, the IOM and OSCE also co-organized a training course for Armenian travel document security officials dealing with all aspects of professional identity infrastructure and management from a strategic and tactical perspective.

A Turkmenistan travel document official reviews recent developments in forged document analysis.

Looking Ahead: The OSCE and ICAO's Vision 2020 and PKD Programmes

Over the last decade, travel document security and commensurate border controls in the OSCE area have markedly improved. Nonetheless, much remains to be done. Accordingly, ICAO's Vision 2020 has set out a number of strategic policy level goals to take full advantage of and put fully at State disposal the newest technologies driving travel document, border control and identity management processes.

Within its geographic remit, the OSCE will continue its efforts on the cutting edge of travel document security by developing existing programmes and projects and by identifying innovative responses for important growth areas such as the PKD and Identity Breeder Documentation. The basis for this lies in the OSCE's role as a force multiplier to provide a platform where standards, expertise and donor contributions come together to build capacity.

The recently established OSCE PKD mandate will launch a new area of capacity-building focused on increasing the participation and use of the ICAO PKD throughout the OSCE area. The OSCE's focus on handling and issuance predominantly encompasses implementing ICAO minimum security standards, which place a solid and enduring emphasis on the traditional aspects of document issuance. Complementing focal concerns for handling the document itself, the OSCE continues to actively promote robust issuance systems that secure the identity chain (birth, name changes, death, etc.)

In the coming years it is expected that work in this area will turn to the attuning of handling and issuance systems to the various breeder documents in circulation, particularly birth certificates, as well as greater focus on the standardization and security of those documents. ■

Implementing e-MRTD Part II-B: Procurement and Implementation

In this continuation of the second instalment on this topic, Markus Hartmann of HJP Consulting GmbH focuses on the execution of a professional procurement process—one that allows for the transfer of technical and commercial requirements into a professional legal agreement that will help keep State authorities in full control during the implementation of their e-MRTD projects.

The legal aspects involved have been detailed here with the assistance of article co-author Chris Coulter, of the law firm Morrision & Foerster.

The third and final instalment in this series on implementing e-MRTD projects will be included in the last *MRTD Report* issue of 2010, later this fall.

After your e-MRTD project planning is completed and the invitation to tender has been prepared, it is of utmost importance to design a professional procurement contract so that the issuing authority retains full control over their rights and the project's deliverables, both during implementation and beyond.

e-MRTD Project Contract Management

Contracts in e-MRTD projects perform many essential functions. The contract itself should set out, in clear, unambiguous detail, the entire commercial understanding between customer and supplier. Within this structure will sit the technical and operational specifications which underpin e-MRTD delivery, including the rules relating to relationship governance and logistics.

The e-MRTD project contract is also an essential tool in transferring ownership of key assets and establishing the scope of licences and rights covering core technologies which may be embedded within your e-MRTD.

Finally, as well as providing the structure for project delivery, the contract will also address future risk mitigation and liability issues so that the parties can achieve their commercial objectives.

To achieve these multiple objectives, the contract needs to be properly developed with due and timely consideration given to key issues.

Preparation: Understanding your own "Must-haves"

The contract most likely to underpin a successful e-MRTD project is that which represents a "win-win" scenario for customer and supplier. This requires reasonableness and may require compromise on both sides. Both the customer and the supplier will typically have different starting points and different external pressures, however, and each side of the table will have issues which they "must-have" addressed in the relationship.

Sometimes these "must-haves" only come to light once the e-MRTD project is underway. Rectifying late realizations of this nature can often be costly for the customer. It is therefore essential that, before engaging with one another, both customer and supplier establish a clear understanding of their own positions on key issues. Invariably, suppliers will already have established their own "must-haves" through prior project experience, whereas for the customer this may be its first e-MRTD project. With this in mind, we believe that preparation of contract terms is a key issue for all customers.

Briefing lawyers

Economic, political and other pressures can quickly combine to cause an e-MRTD project to be moved forward before the customer has managed to establish and agree its own "must-haves" with the supplier. Under these conditions, some projects will start with a technical requirement that gradually evolves into one or more supplier price proposals and then, without a formal or adequate contract in place, preliminary aspects of the project get underway.

These preliminary aspects may be superficially minor but there are significant risks in this approach, most of which are borne by the customer who could lose commercial leverage when contracts are finally introduced. An incumbent supplier has many advantages over any potential competitors.

For these reasons, it is preferable for the customer to negotiate technical and commercial matters in the context of a well-developed draft contract. In order to achieve this, it is advisable to engage and brief legal teams in the early stages of an e-MRTD project.

"As a bare minimum, the e-MRTD implementation contract should include a robust change control mechanism detailing what should be included in each change control note, impact analysis requirements, turnaround times, etc. Anticipating the need for change and establishing rules around pricing changes (and the cost of change implementation) are key cost and quality control issues which the contract needs to address."

Key Legal Issues

Each e-MRTD project will reveal its own complexities depending upon the regulatory environment of the customer, legacy systems, existing MRTD infrastructure, existing commercial relationships and other commercial as well as political factors.

Each of these aspects may lead to important contractual must-haves. We have therefore identified here a number of key issues which are common to most e-MRTD projects and which should be considered prior to engagement with suppliers.

Development and Change Management

It is essential to specify clear parameters (time, location, etc.) for all aspects of e-MRTD delivery and, frequently, a significant requirement in this respect will be the development of all or part of the e-MRTD package, including software, design features, etc.

e-MRTD development requires rigorous and phased testing and acceptance in order for components and entire packages to

Sixth ICAO Symposium on

ICAO MRTDs, Biometrics and Security Standards

1–4 November 2010
ICAO HQ, Montreal, Canada

ICAO will hold its Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards from 1–4 November 2010. An Exhibition will complement the Symposium and highlight important products and services related to MRTDs, biometric identification and border inspection systems.

The 2010 Symposium follows last year's successful event, attended by over 500 participants from States, international organizations, companies and institutions. It will be of particular interest to officials of passport and official ID document issuing agencies, immigration, customs, and other border control and security authorities. Officials from airlines and airports involved in passenger service systems, handling of travel documents, facilitation and aviation security would also benefit by attending.

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

www.icao.int/MRTDsymposium/2010

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

qualify as suitable for large-scale production. The contract should therefore specify testing methodology, the criteria for success and the consequences of failure.

It is additionally essential that the customer retain control of the definition of each of these project aspects. Appropriate testing stipulations in the contract require effective cooperation between technical, operational and legal work-streams.

In addition to defining and controlling development, the contract should also provide a clear method to implement changes once it has been signed. In the fast-moving field of e-MRTD projects, technical and regulatory advances make it essential for any customer/supplier relationship to be able to accommodate any externally-mandated changes to proposed requirements or solutions.

As a bare minimum, the e-MRTD implementation contract should include a robust change control mechanism detailing what should be included in each change control note, impact analysis requirements, turnaround times, etc. Anticipating the need for change and establishing rules around pricing changes (and the cost of change implementation) are key cost and quality control issues which the contract needs to address.

Warranty & Liability

e-MRTD products are often composite in nature and include components of different types (papers, plastics, hardware, software, etc.) from more than one supplier. Furthermore, a single defective component is likely to render other non-defective parts non-reusable. This component diversity raises challenges for customers seeking to harmonize warranty protection; different component suppliers may offer varying periods of warranty and varying remedies if the warranty is breached.

As a result, this is one of the more complex contractual areas and the cost consequences of defects can be significant.

One method of reducing this complexity is to engage a prime contractor as integrator. However, this approach means that it is essential that price and legal risk, in relation to third party components, are established early in the negotiations and set out clearly in the contract prior to short listing or contract award.

If an integrator is not used, and the customer uses a multi-sourcing model while bearing the integration risk itself, it is essential for each supplier contract

to be constructed so as to mitigate the integration cost risk. This requires contract structure planning prior to engagement with suppliers.

In addition to contract structuring issues, the details of the warranty protection is also important. In this manner, software embedded on silicon may be supported by legacy operating systems, for example, and while it may be possible to test output functions it is not always so simple to test other aspects of the operating system. This carries the risk of failure in live-use of e-MRTD products, which may not be detected until products are in the field, which in turn carries the risk of expensive recall issues.

Naturally, suppliers are keen to limit their risk to "tested" failures and to avoid liability for unknown or "untested" failures. Rigorous testing procedures can mitigate this risk, however there are also approaches to drafting contractual warranties and related language which can also improve the customer's remedies in the case of untested software failure. These precautions can have the effect of reducing financial impact of material batch failure.

Intellectual Property Rights and Related Know-how

The commercial market for e-MRTD products is in rapid development and suppliers are hastily seeking to establish defensive and aggressive Intellectual Property Rights (IPR) strategies to secure patents, etc. Against this backdrop, it is essential that customers have as strong an IPR position as possible in their arrangements with suppliers. This means setting out in the contract suitable IPR licences and, where appropriate, detailing ownership transfers of embedded technologies and related systems.

Given the expense of defending patent litigation, customers should also ensure that the contract is clear as to the financial consequences of IPR infringements.

Where an e-MRTD project is expected to have a transformative effect on current practices, it is essential for the customer to ensure that (once all development has been completed) it has the internal skills and know how to use IPR as well as the required IP rights. This skill-base helps reduce supplier-dependency and maintains commercial leverage for system upgrades and ongoing support.

There are certain critical areas to address to ensure a customer is able to maintain such a knowledge base. For example, the customer should ensure that it obtains, by express contractual provision, the freedom to use project documentation, appropriate access to software source code (which may need to be delivered-up during the development phase or placed into escrow on reasonable terms), and lastly adequate training—if necessary for specified personnel.

Key Contract Negotiation Success Factors

There are varying approaches to negotiation strategy but certain factors, specifically those relating to contract negotiations, remain constant, namely:

- Issues introduced late may be lost in the rush to close. Or even if they are successfully forced into the contract at a late stage, such issues can cause additional cost, delays and create mistrust. It is essential to enter into an e-MRTD project with a well developed contract which addresses all key issues, especially those which may have cost impact.

- Customers lose leverage once suppliers are embedded. A well-run competitive procurement process should outline supplier issues at an early stage by including a detailed and well-developed contract in the tender documentation.

"...it is preferable for the customer to negotiate technical and commercial matters in the context of a well-developed draft contract. In order to achieve this, it is advisable to engage and brief legal teams in the early stages of an e-MRTD project."

- A comprehensive contract start point enables informed compromise and is good preparation for the unexpected.

- All significant contracts take time to conclude but a reasonable "win-win" approach should deliver the most successful long term relationship between customer and supplier.

Implemention:
Joint Project Management with Clear Responsibilities

After having concluded their tough contract negotiations, the buying issuing authority and the awarded supplier shake hands, wishing one another all the best for completing the project successfully. In this manner both parties become partners even though the roles and responsibilities of each remain different.

First and foremost, the issuing authority is responsible for keeping the requirements specifications up to date. There is no doubt that, during the implementation phase, changes to the

initial planning will become necessary. In order to retain the legal position agreed upon in the procurement contract, however, it is essential to process any change within a formal change control management procedure. In the event that any of the requirements or specifications are affected, these need to be updated by the issuing authority prior to acceptance of the change.

The authority's project management needs to be very accurate in recording and controlling all communications, actions and deliveries on behalf of the supplier. When problems occur, every communication will become legally relevant. Only when the supplier realizes that their client is in full control over the project implementation phase will it be fully committed to delivering what it has promised within its proposal.

Issuing authorities should be aware that suppliers often develop the proposed e-MRTD products only after they have been awarded—despite the fact that fancy product collaterals may well have given a different impression.

The second main responsibility of the authorities is the management of those tasks and sub-projects which have not been put out for tender. Sites for installing equipment for personalization machines and enrolment IT need to be prepared. Business processes in enrolment and delivery need to be adapted. National rules and regulations about new e-passport issuance and related acts such as Data Privacy Acts need to be investigated. Later issues tackling logistics and quality assurance of e-MRTDs should be addressed. Finally the authority's HR department needs to check if new personnel should be hired and how existing staff should be trained. It is paramount that the project schedule of the authority's tasks is fully in line with the supplier's project schedule. For example, when the personalisation site is not ready, the supplier will hold back delivery. Sometimes suppliers even use the authority's delays for hiding their own delays. Authorities should not allow suppliers playing hide and seek with them.

The Importance of Competency-based Training Approaches

It is the issuing authority who will operate the new e-MRTD issuance system. Hence their staff must become e-MRTD experts in the same way as they are required to be MRTD experts today. New chip technology will require very different skill sets from IT officers, personalization bureau operators, forensic experts and all other staff members involved.

Instead of expertise in security printing, expertise in IT and cryptography will be required. A well designed and targeted group-oriented training course will be paramount for managing the new e-MRTD solution successfully. It is also common that the supplier be asked to provide relevant training as part of its delivery, but the issuing authority might also consider engaging independent trainers in order to gain more fundamental knowledge about the new technologies and processes in place. This type of training is offered by various international organizations, the most important of which are reflected in Table 1 *(below)*.

International e-MRTD Training Organizations*
ICAO Implementation and Capacity Building Working Group (ICBWG)
International Organization of Migration (IOM)
Organization of American States (OAS)
Organization for Security and Co-operation in Europe (OSCE)
FRONTEX

*Many of these organizations support joint, collaborative programmes to support States.

Regardless of which organization provides the training, the issuing authorities should only select trainers who are not only expert in the requested subject, but also provide training based on a proven training methodology. A competency based training approach is recommended in this regard.

Competency-based training approaches ensure that the trainee fully learns the practical aspects of working with e-MRTD issuance systems. These courses are designed towards a specific target group's needs. A mix of practical and theoretical tests should be conducted rather than simply firing hundreds of slides at the trainees.

One of the better known competency-based training methodologies has been developed by R. Mager, based on his Criterion Referenced Instruction (CRI) and Instructional Module Development (IMD) training tools. The ICAO TRAINAIR programme also employs and recommends competency-based training approaches.

Conclusion

Procurement is by far the most crucial component of implementing an effective e-MRTD system. It connects technical requirements with the commercial and legal frameworks, making it essential for a successful implementation phase.

In order to keep an arm's length relationship with the supplier, an independent legal and commercial advisor may help you to avoid legal pitfalls and unnecessarily high costs. It is essential not to bind your project too early to one supplier only. A thoroughly planned tender process must take precedence and this article has, we hope, provided an overview of the most critical and most important aspects that issuing authorities should consider before they sign their contracts.

After having ordered a solution from a supplier, the issuing authority must lastly take proper care before approving the delivered solution. We will cover this final aspect in the third article in the "Implementing e-MRTD" series, which will be included in ICAO MRTD Report 03/2010. ■

HIGHLIGHTS

ICAO AIR TRANSPORT DATA AND ANALYSES

All information in one place.

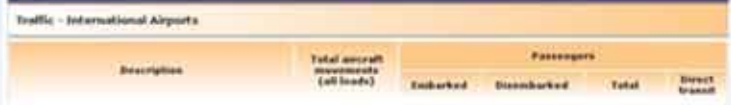
For more information, contact: Tel: + 1 514-954-8136, Fax: + 1 514-954-6744, E-mail: eap@icao.int

AIR CARRIERS
Including Low Cost Carriers Traffic

Traffic & Financials — On-Flight Origin and Destination

Fleet / Personnel — Traffic by Flight Stage

AIRPORTS



Traffic & Financials

ECONOMIC STUDIES AND DATABASES

- Regional Differences in International Airline Operating Economics
- Regional and Global Traffic Forecasts
- Statistical Reports
- Tariffs for Airports and Air Navigation Services
- World's Air Service Agreements

And much more ...

ICAO DATA AND ANALYSES ... THE ESSENTIAL TOOLS FOR:

- Route Development and Planning
- Air Traffic Flow Analyses and Forecasting
- Market Analyses and Strategy Development (e.g. market share, flight frequencies)
- Performance Benchmarking
- Financial and Operating Cost Analyses
- Investment Project Evaluation (e.g. privatization, IPO, due diligence)
- Air Transport Economic Studies
- Aviation Consulting Assignments

Global Aviation Data at your Fingertips

INFORMATION?
Contact:
eap@icao.int

DAILY
UPDATES

SHOP ONLINE
icao.int/store

The source you can trust

39 Myths about e-Passports: Part II

In response to the often inaccurate critiques of e-Passport technology and functionality that occasionally find their way into popular media, the following is the second in a three-part instalment for *MRTD Report* readers highlighting 39 of the most prominent e-Passport myths and debunking the faulty data or premises underlying each.

These myths have been compiled and addressed by the ISO's Mike Ellis, one of the world's foremost experts on passport and e-Passport security. Myths 11 thru 26 are reflected here and the remainder will be published in the last *MRTD Report* issue of 2010.

KEESING Reference Systems FIGHT FRAUD

The full text of the following article originally appeared in issue No. 30 of the Keesing Journal of Documents & Identity, published by Keesing Reference Systems. The MRTD Report is grateful to Keesing for providing it with the permission to reproduce this very useful list to its readership.

In 1998 ICAO, through the New Technologies Working Group (NTWG) of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), began work on the next generation of passport, now known as the "e-Passport" or "biometric passport". The main driver for this work was the need to improve the security of the passport by linking it more positively to its owner.

For some time there had been a rising incidence of forged passports which were used by criminals, such as drug couriers, and illegal immigrants. There was also the increasing threat of terrorism. Typically, a lost or stolen passport would have its owner's photograph replaced by

the criminal's, a process known as "photo substitution". Often the printed data would be altered too, for example, the date of birth would be made to match the age of the new owner.

The NTWG started with a plan to place a biometric of the owner in the passport, so that the owner could be reliably linked to their passport, but there were a number of issues that had to be resolved. Which biometric? How would the biometric be stored? How would it be read? How would it be authenticated? After all, there would be no advantage if the criminal could forge the biometric too.

There are now over 100 million e-Passports in circulation, issued by over 50 countries, and the number grows every day. Almost all of them comply with the ICAO standard, which means that they are truly "globally interoperable" and can be read by any country. A Public Key Infrastructure (PKI) system provides certificates that can be used to check their authenticity.

While the original driver for these developments was security, interesting facilitation schemes are also now emerging which employ the face, fingerprint or iris biometric to get travellers through borders more quickly and efficiently.

Without a doubt, a true success story.

However, there are always detractors, and newspaper and web articles critical of the e-Passport have persisted. Most often these are based on fiction, a misinterpretation of the facts, or on a mixing-up of MRTD technologies with other chip-based applications. Sometimes the articles are written by "hackers" seeking fame, or "security researchers" working in pristine laboratories, a little divorced from reality. Journalists then seize upon these purported "facts" and write stories that generally imply that "the sky is falling".

Lastly there are the articles written for political gain by activists concerned with a specific government policy. While we have no quarrel with other points of view, we do object when the technical data is twisted and selectively quoted to suit a particular agenda.

The following is the second part of the MRTD Report's ongoing review of related facts to help readers debunk common fallacies and myths currently being reported about e-Passports.

MYTH #11

The RF chip was chosen so that people could be tracked

The most radical version of this myth is that the RF chip can be interrogated from a great distance, even from satellites. Tracking from satellites is definitely not possible. This is basically confusion over

technologies. The RF tags used in warehouses can be tracked at a distance, perhaps tens of metres, but these comply with other ISO standards and generally are small chips which require miniscule power to operate.

Even assuming that your e-Passport is within the range of the machine reader, say within 75cm, it must be there for approximately three or four seconds for the read to complete. Any interruption of transmissions, say by the e-Passport antenna being at an inefficient angle to the reader antenna, will cause the reading to abort.

But this whole scenario is academic as all e-passports now have Basic Access Control which prevents unauthorized access, and some have in-built shields which prevent any reading unless the e-Passport is open. So tracking, by reading the e-Passport at any distance, is impossible.

Some commentators have pointed to the Unique Identifier (UID) as a potential tracking mode. When the e-Passport is first contacted by the reader, it identifies itself by sending a UID. The theory is that once an e-Passport is associated with a UID it can be tracked, and its owner tracked too, even though nothing further can be read from the e-Passport because the Basic Access Control blocks access to the personal data. The problem with this theory is that most, if not all, countries have implemented random UID. Each time the e-Passport is contacted it generates a different UID for that session. This prevents tracking.

It is curious to note that we already live with more efficient and widespread tracking systems that do not seem to raise the same concern. The venerable one is car registration numbers. Almost everyone now carries a cell phone. And our faces can now be tracked through city centres by using facial recognition with CCTV. This is not to excuse any potential tracking using the e-passport, but really, the chances of tracking anyone by their e-Passport are so slight that it is decidedly impractical.

MYTH #12

The contactless chip in the e-Passport is prone to failure

Failure of the chip was certainly a concern of the NTWG. Most countries advise their citizens to care for their e-passports, not to unduly bend, twist, or puncture them. There was a question of the warranty that chip companies would give on their chips, given that there had been no experience of chips in passports before. The preliminary evidence is that the chips are reliable. Some countries have reported that after three or four years they have had no failures of chips, or else only minimal failures, in hundreds of thousands of issued e-passports. There is good reason therefore to believe that the chips will last for the five or 10 year life of the e-passport.

MYTH #13

The Machine Readable Zone (MRZ) is a "bar code"

While this is more correctly a fallacy about machine readable passports, it nonetheless also finds its way into discussions about e-passports. The MRZ is represented by the two lines of printing (88 characters) at the base of the data page that holds the photo or printed facial image. The font used for the characters is Optical Character Recognition, Type B (OCR-B). ICAO has specified OCR-B since the very first edition of Doc 9303 in 1980, as OCR-B reading was by then a mature technology.

MYTH #14

e-Passports vary from country to country

This comment is usually made with respect to the comparing of passports from different countries in order to grade them or to try to remotely identify them. Practically all e-passports conform to the ICAO standard Doc 9303. They also implement a set of the minimum security standards. While there are small differences between the e-Passports of different countries, they have overwhelmingly more in common than not. e-Passports are issued by one country to its citizens, and have to be read by all the other countries to which they travel. To achieve this level of global interoperability, all e-Passports must conform to ICAO Doc 9303 in all essential respects, so the amount of variation is minor.

MYTH #15

The e-Passport is read in two stages, which slows border processing

Writers who want to emphasize the slowness of border processing describe e-Passport reading as a two-step process, using two distinct pieces of equipment. Firstly the MRZ is read using an optical reader, and then the chip is read using an RF reader. While this scenario is possible, there are a number of combined readers (optical and RF) on the market which would carry out the two reads in a seamless manner. Use of the single combined reader is the preferred way for implementing e-Passport reading.

MYTH #16

The e-Passport is authentic if the printed and chip data agree

While it is true that the printed and chip data must agree, and this would be one of the border control checks, this agreement is not a guarantee that the e-Passport is authentic. The authenticity is ascertained based on the paper security features, plus the Public Key Infrastructure (PKI) verification of the digital signatures in the chip. Often, attacks—such as the "Elvis" passport forgery variation

using forged digital signatures—will not validate against the PKI.

MYTH #17

All the chip data does is to confirm the printed data

While the chip data, in the mandatory data groups 1 and 2 (MRZ and facial image), does confirm the printed data, the chip can contain additional, optional data, including fingerprint and iris biometrics. As well, the chip data is secured by the PKI, which is a further strong security feature.

The chip data can also assist border officials in other ways. For example, the facial image stored in the chip is a higher resolution version of the printed photo, so when it is displayed on the border official's screen this can mean a more confident match with the traveller in question.

MYTH #18

If the chip is cloned and the passport faked, it will easily pass muster

There are number of difficulties with this myth. If the chip is cloned (i.e. copied exactly), then it will only really match the original owner. Therefore it will not "pass muster" for an impersonator. If the chip is cloned and then altered—for example, if the photo is replaced—then PKI verification will detect this. Forging the traditional paper part of the passport is also fraught with danger for the forger, as there are always several advanced security features which must be forged and for which border officials are trained to look.

Many e-Passports are now equipped with "Active Authentication", which detects cloning. This is a public/private key protocol where the private key is embedded in the original chip and cannot be copied. The cloned chip does not have this private key, so the cloning can be detected.

This myth seems to revolve around the supposition that because the e-Passport is highly secure and therefore trusted, it will be given only cursory inspection and forgeries will not be detected. As has been stated above, the e-Passport does not supersede the judgement of the border official—it is an extra tool that makes the detection of forgery more likely. Even for "look-alikes", impersonators who attempt to pass themselves off as the owner of the passport (a problem which pre-dates the introduction of the e-Passport), detection is more likely. Border officials now have access to the higher resolution photo in the chip to make the comparison, and the introduction of sophisticated facial recognition systems (made possible by the same higher resolution photo) will also flag differences.

MYTH #19

The US "PASS" border card is an e-Passport

The US "PASS" card is not an e-Passport. It is a vicinity card that contains a number and can be read at a distance, typically 50 metres. It has no protection against unauthorized reading, other than that the owner can place it in a protective, metal-lined pouch to prevent access. The idea is that the card can be interrogated by US border control as the owner approaches the border control point. The number can then be used to access the owner's file in a database. The card then fulfils the traditional role of a visa.

However, many journalists and bloggers confuse the PASS card with an e-Passport, and claim that because the PASS card can be read at 50 metres, then the e-Passport can be read also at 50 metres. This is a fallacy.

MYTH #20

Golden Reader software is the ICAO-Standard border control software

The "Golden Reader" tool was used by ICAO for interoperability tests to check the operation of e-Passport chips and RF readers. It was never intended, nor was it ever advertised, nor is it used, as "standard border control software".

This myth persists as "security researchers" who have altered the digital signature hashes have found that the Golden Reader will read their altered e-passports. However, and most importantly, the Golden Reader does not check the PKI certificates. Real border control software will check the certificates and detect their forgeries.

MYTH #21

A "wanted" person can swap their e-Passport chip for another person's and get through border control

This myth is really stretching credibility. The idea is that a terrorist, whose name is on a watch list, could carry an e-Passport with his real name and photo printed on the data page, but with a chip that contains different information cloned from someone else's e-Passport. The border official checks the printed data against the terrorist and finds it to be correct. The automated border screening checks the chip, finds a legitimate and safe person, and passes the terrorist through the border.

As we said above, the e-Passport does not supersede the control of the border official. No border control system is going to allow a person to pass based solely on the unseen evidence of the chip. If the border is manually operated, the border official is going to check the chip data against the printed data, as a first and simple step, and find the forgery. If the border control is automated, not only will the chip data be checked against the printed data, but also the biometric in the chip data is going to be checked against the owner.

MYTH #22

The e-Passport can be programmed to "crash" a border control system or introduce viruses

This myth originated from the exploit of a "security researcher" who altered the

JPEG image in an e-Passport chip. At a trade fair he found two machine readers that "crashed" when they attempted to display the JPEG image. From this he speculated that he could introduce viruses and gain control of the border inspection system, and in so doing permit terrorists to pass.

The operation of machine readers at a trade fair is a far cry from the operation of a border control system. At a trade fair, readers are set up to read sample and real documents and display their contents without any real checking of their validity. After all, the vendors are trying to show the operation of their readers and will not be unduly bothered about checking the PKI, which is not an intrinsic reader function. A corrupted JPEG file could cause a reader to crash if the reader's software had not been properly written. But in this case, the operator would simply reset the reader and clear the fault.

A border inspection system will first read the chip data and check its authenticity by passive authentication (checking the digital signature hashes and authenticating these through the PKI). Only when the chip data has passed this test will any execution of the code proceed, for example, the display of the JPEG image. Reading the chip data is safe, as it is not executed and so exploits and viruses cannot be activated. It is doubtful in any case that a virus could gain a foothold. The "security researcher" did not actually demonstrate this.

MYTH #23

The biometric data can be used for other purposes, thus violating privacy

The mandatory biometric is the facial image. As this is freely available from other sources (for example, cameras, CCTV), obtaining the facial image from the chip, assuming that the BAC protection is overcome, is hardly a matter for concern. The other biometrics, fingerprints and iris, are considered more sensitive and are protected by Extended Access Control (EAC). EAC operates by having the inspection system prove that it is legitimate to the e-Passport before the reader can access the data.

MYTH #24

Criminals can steal your identity by remotely reading your e-Passport

The e-Passport is protected against unauthorized reading and eavesdropping by Basic Access Control, and in some cases, by metallic shields (see Myth #8 in MRTD 01/2010 for a description of this). To overcome the BAC and gain access, the criminals either have to have the e-Passport in their possession (in which case they can simply read the printed data); or they have to have the e-Passport in the field of their reader for years while they attempt a brute force attack. The effort required to remotely read an e-Passport and get any sort of information makes this very unattractive.

MYTH #25

A non-working chip will invalidate the e-Passport and you will be denied entry

ICAO has definitively stated that an e-Passport with a non-working chip must be regarded as a legitimate travel document, and the owner should not be denied entry based on this alone. It was recognized that a small percentage of chips will fail due to natural causes. Most border officials will simply advise that an e-Passport with a failed chip should be replaced as soon as practicable.

However, it also recognized that criminals, finding that they cannot subvert the chip, will destroy it rather than risk being detected. Border officials will therefore check an e-Passport with a non-functioning chip very carefully, looking for signs of tampering.

Therefore, bloggers who advocate disabling the chip (for example, by hitting it with a hammer) because of some misguided fear of being tracked or such, should take note that this action may lead to some difficulties at borders if the tampering is detected.

MYTH #26

"Look-alikes" can use e-Passports too

Impersonators, or "look-alikes", have always been a problem. In the "Day of the Jackal" movie, the assassin steals a passport and then alters his appearance using hair dye and so on to make himself look like the original owner. The drawback with traditional passports is that the photo on the data page is small, and it is difficult to detect look-alikes.

However, the e-Passport contains a high resolution facial image, as mentioned before, which can be displayed on the border official's screen in a much larger size. This definitely aids in the detection of look-alikes. If a facial recognition system is used, there is probably even more chance of the criminal being detected. And if the e-Passport contains a fingerprint or iris pattern the look-alike will definitely be detected.

The automated immigration line at Sydney airport, "SmartGate", has facial recognition software which matches the facial image in the e-Passport with the owner's face. If a perfect match is not obtained then he or she is referred to a Customs officer for manual processing. SmartGate also authenticates the data in the e-Passport by checking the digital signature to make sure there has been no tampering of the facial image or personal details. ■

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

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

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

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

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

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

Biometric system An automated system capable of:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Holder A person possessing an ePassport, submitting a biometric sample for verification or identification while claiming

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Metallic ink Ink exhibiting a metallic-like appearance.

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

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

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

Multiple biometric The use of more than one biometric.

One-to-a-few A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against

a small number of biometric reference templates on file. It is commonly referred to when matching against a "watch list" of persons who warrant detailed identity investigation or are known criminals, terrorists, etc.

One-to-many Synonym for "Identification."

One-to-one Synonym for "Verification."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UV Ultraviolet light.

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

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

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

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

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

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

2010 ICAO CALENDAR OF EVENTS

Meetings	Site	Duration
International Conference on Air Law Diplomatic Conference on Aviation Security (DCAS 2010)	Beijing, China	30 August–10 September 2010
Global Aviation Strategy Summit	Vancouver, Canada	20–21 September 2010
ICAO/McGill University Assembly Pre-Conference	Montreal, Canada	26–27 September 2010
ICAO Assembly – 37th Session	ICAO Headquarters, Montreal	28 September—8 October 2010
Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards	ICAO Headquarters, Montreal	1–4 November 2010
ICAO Regional Seminar on MRTDs, Biometrics and Security Standards	Maputo, Mozambique	24–26 November 2010

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 20 national ePassport programs worldwide including Côte d'Ivoire, Estonia, Denmark, France, India (diplomatic), Norway, Malta, Portugal, Qatar, Singapore, 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

Secure identification systems from Giesecke & Devrient

Creating Confidence. G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport and border control systems, ID card solutions and have become a trusted adviser and supplier to governments. We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. G&D will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards. ID system implementation by G&D – individual, international and secure. **www.gi-de.com**

Giesecke & Devrient

Creating Confidence.