MRTD REPORT

# ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

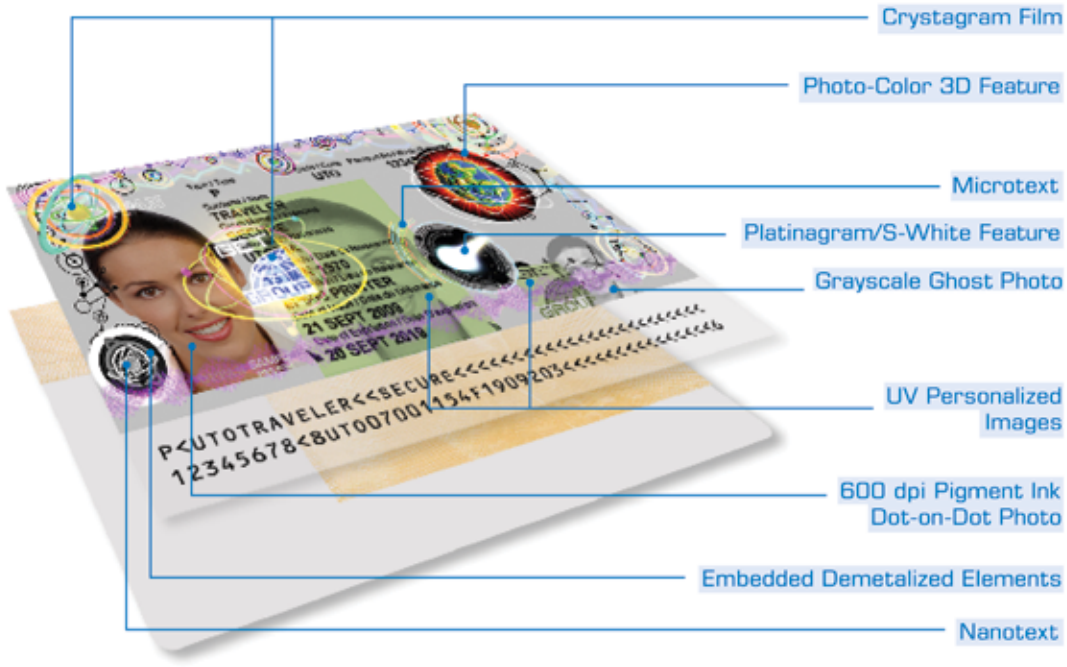
# Security & Identity


**INTERPOL's new Travel Document Initiative for enforcement stakeholders highlights a new convergence in global security and identity frameworks enabled by ICAO MRTD progress.**

**Also in this issue:**
**Breeder Documents and Global Identity Vulnerabilities • Busting the MRTD Myths**
**Interview – ICAO AVSEC Chief James Marriott • OSCE PKD Outreach**
**HJP MRTD Project Management Series**

Vol. 5, No. 3

**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. Secure

The new eP600 ePassport printer from GET Group produces our most secure passports ever, employing unique EDE Crystagram security film which incorporates extraordinary features to protect the integrity of the data page.

With fully automatic book processing, high speed, 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 3, 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 site: 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 around the world each year. Our solutions and services include:

- **Enrollment Services** including ICAO-Compliant Biometric Images
- **Enrollment and Renewal Self-Service Kiosks**
- **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

# Capitalizing on Convergence

This special Symposium issue of the MRTD Report provides me with an excellent opportunity to summarize some important developments and upcoming events, and also the pleasure of making a special introduction to the global MRTD community.

Earlier this year, ICAO was very fortunate to attract Jim Marriott, formerly of Transport Canada, to serve as the new Chief of the Organization's Aviation Security (AVSEC) Branch. Jim's background is a virtual wish-list of talents and achievements that will prove highly useful to ICAO as it begins lead the uniquely cooperative and more integrated AVSEC, facilitation and law enforcement framework that is emerging as a result of recent technological and MRTD compliance achievements.

During his 25 years with the Canadian government, Jim occupied a variety of positions with increasing responsibility and complexity in the transportation security field. At the senior executive level he has extensive experience in international relations, policy and regulatory development, oversight, critical incident management and organization development. It is also noteworthy that he has been Canada's member on the ICAO Aviation Security Panel since 1989 and has a clear understanding of how and why ICAO remains the most important forum for leading international air transport policy development. You can get a more first-hand impression of Jim's thoughts and intentions concerning ICAO's AVSEC and Facilitation areas in the special interview we've featured on page 16 of this issue.

The theme of a more integrated and cooperative AVSEC/enforcement framework also figures prominently in the Ralph Markert article in this issue on the new INTERPOL Travel Document Initiative (TDI). This is a very exciting development that promises to significantly enhance global law enforcement capabilities and which has been uniquely enabled by the ongoing convergences that global MRTD interoperability is helping to realize.

The themes of evolving security- and MRTD-related cooperation will doubtless figure prominently in many discussions and presentations at this year's Symposium as well. Of significant importance in this regard are the persisting vulnerabilities relating to identity issuance. The remaining weaknesses in identity management and travel documents tend to be exploited by terrorists and criminals worldwide and represent a weak link in our global efforts to ensure security, stability, good governance and the rule of law.

Breeder documents and other issuance concerns will also be high on the agenda at the MRTD Regional Seminar in Maputo later this month. ICAO is very grateful for the support and assistance it has received from the government of Mozambique in hosting this important event, which will be extremely useful for all African officials and companies involved in any aspect of identity issuance, border control, customs, law enforcement and immigration. ICAO-compliant secure tra vel documents and a robust identity management regime are powerful tools in preventing and combating terrorism and serious transnational crime. All of these issues will be front-and-center when we visit Maputo in the coming weeks.

In closing, I would like to remind all *MRTD Report* readers about the MRTD Community Web site we've developed for you at **www.icao.int/mrtdc**. This site is a very useful repository for MRTD information and States are strongly encouraged to reference it to obtain assistance on the implementation of technologies and services to comply with current MRTD requirements. For your convenience a directory listing of industry suppliers is also featured on the site which can be of great assistance to your State should it require specialized assistance.

I wish you all an informative and thought-provoking Sixth MRTD Symposium.

**Mauricio Siciliano**
Editor ■

### Easy Access to ICAO's MRTD-related Guidance

For free copies of ICAO Doc 9303 and other very useful reference and guidance tools relating to MRTD compliance and e-Passport development, please visit:

**http://www2.icao.int/en/MRTD/Pages/Downloads.aspx**

### African Regional Seminar on Machine Readable Travel Documents (MRTDs)

24 to 26 November 2010, Maputo, Mozambique

For more information or to register please visit:

**http://www.icao.int/mrtdseminar/2010africa/**

www.icao.int

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

| Member | Nominated by | Member | Nominated by |
|---|---|---|---|
| Mr. R. M. Greenwood | Australia | Mr. J. Verschuren | Netherlands |
| Mr. G. K. McDonald | Canada | Ms. A. Offenberger | New Zealand |
| Ms. M. Cabello | Chile | Ms. I.O. Sosina | Nigeria |
| Mr. M. Vacek | Czech Republic | Mr. C. Ferreira Gonçalves | Portugal |
| Ms. M. Pujau-Bosq | France | Mr. O. Demidov | Russian Federation |
| Dr. E. Brauer | Germany | Mr. S. Tilling | Sweden |
| Mr. A. Manickam | India | Mr. R. Vanek | Switzerland |
| Mr. J. Nugent | Ireland | Mrs. K. Mitchinson | United Kingdom |
| Mr. N. Kawamura | Japan | Mr. M. Holly | United States |

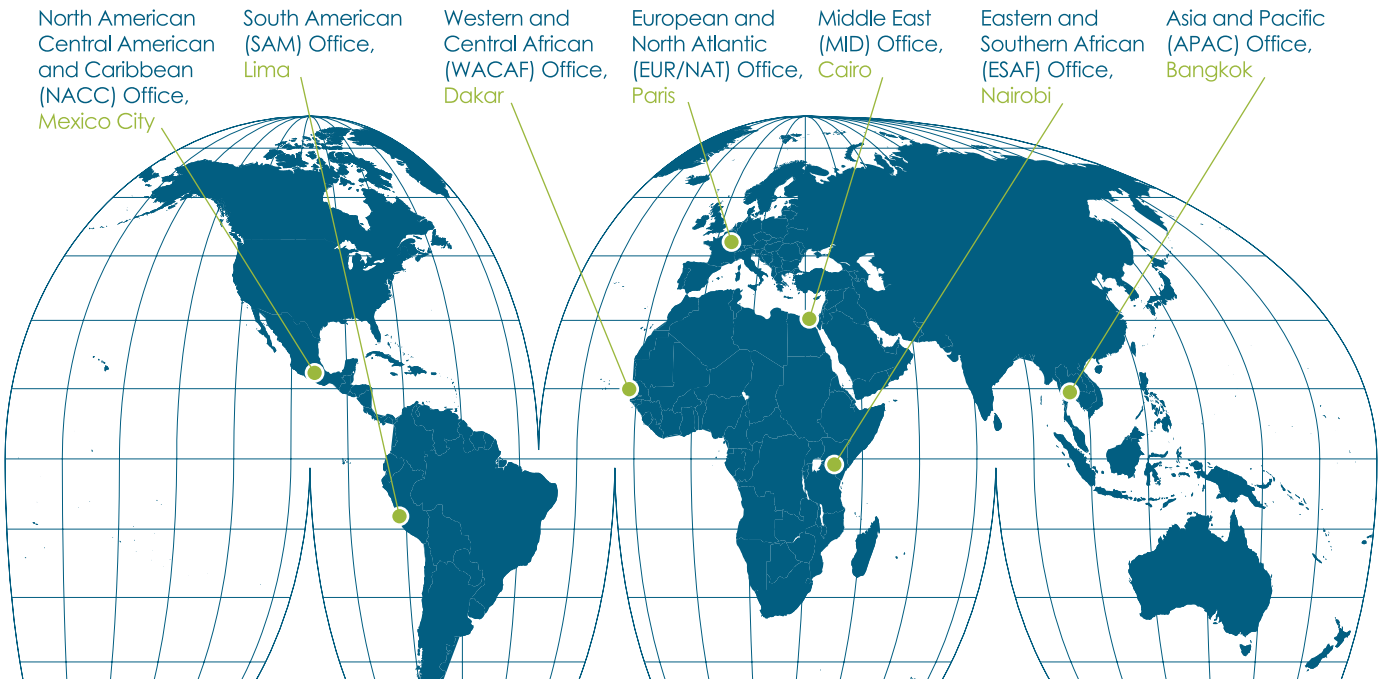
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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)
Organization of American States (OAS) - Inter-American Committee on Terrorism (CICTE)

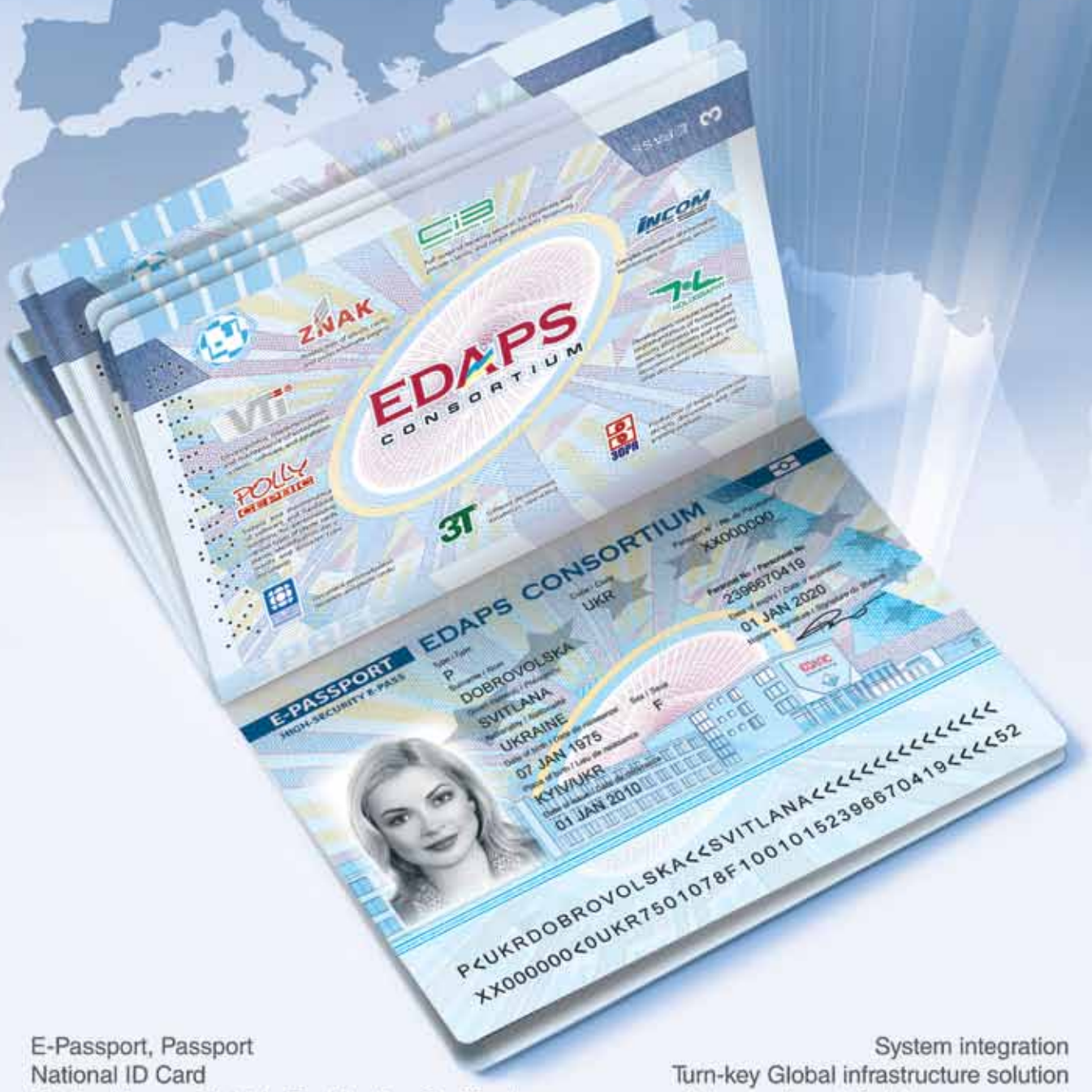
# ICAO's Global Presence



www.edaps.ua

EDAPS
CONSORTIUM

EDAPS CONSORTIUM IS SUCCESSFULLY INTRODUCING
ITS ADVANCED TECHNOLOGIES FOR SECURITY PRINTING INDUSTRY




E-Passport, Passport
National ID Card
Driving Licence, Vehicle Registration Certificate
E-Vehicle Inspection Certificate

System integration
Turn-key Global infrastructure solution
Data enrollment & data management
Document production and personalization


# INTERPOL Travel Documents

## A Revolutionary Step in International Police Co-operation

**In March 2009, The International Criminal Police Organization's (INTERPOL's) Executive Committee approved the launch of a new Travel Document Initiative. The renowned international enforcement body is now seeking recognition of its two new Travel Document formats—the INTERPOL e-Passport Booklet & e-ID Card—as well as the granting of special visa status to holders of these identification tools by INTERPOL's 188 member countries.**

**Ralph Markert, General Project Manager of the INTERPOL Travel Document Initiative and Assistant Director of the organization's Strategic Planning Directorate, explains how these new identification tools are seen as crucial to ensuring more effective and collaborative international law enforcement responses to challenges such as trans-national crime or devastating natural disasters.**

The International Criminal Police Organization, more commonly know as INTERPOL, is an organization that many people have heard of but few can actually claim to understand. Its representation in Hollywood films has often led to notions of secret agents chasing criminals across borders, or of an organization able to track every individual around the world. People can rarely tell you why or when the organization was founded, or what its official mandate is.

International police cooperation is not actually a new idea. First attempts at formalizing such cooperation date back to 1914, when Prince Albert I of Monaco invited lawyers and police officials from 23 nations and territories to meet in Monaco for the first International Criminal Police Congress. In 1923, following the success of the first Congress in Monaco and several attempts to renew international police cooperation efforts, Johan Schober, President of the Vienna

# ▶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*


Police, finally convened the Second International Police Congress in Vienna. The establishment of the International Criminal Police Commission, to be based in Vienna, was the principal outcome of this congress. Article 2 of its Constitution detailed its principal goals:

> "…to ensure and promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws existing in the different countries' and 'to establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes."

INTERPOL today is based in Lyon, France, and counts 188 member countries. The core tenet of the organization has not wavered since its inception—INTERPOL is still in the business of fighting transnational crime.

As an organization, INTERPOL has had to continually evolve to remain effective against crime; a constantly changing phenomenon now increasingly operating across national borders. INTERPOL's priority crime areas now include Fugitive Investigation Support, Drugs and Criminal Organizations, Financial and High-Tech Crime, Public Safety and Terrorism, Trafficking in Human Beings, and Anti-Corruption. Each of these areas necessitates cross-border operation by international law enforcement officials to effectively counteract the perpetrators' activities.

In June 2002, with the support of the United Nations Security Council, INTERPOL created the Stolen or Lost Travel Document database (SLTD) to register all reported stolen and lost documents in order to prevent their misuse. Lost and stolen documents are often vital to the illegal activities that make up INTERPOL's priority crime areas and the creation of the SLTD database, containing more than 22 million documents as of August 2010, represents a major step in countering them.

The SLTD has since been endorsed by ICAO, as well as other international organizations, and has resulted in some 32,000 hits between January and September 2010.

While additional developments, such as the creation of INTERPOL's 24-hour Command and Co-ordination Centre, the implementation of its global DNA Profile and Child Abuse Image databases, and the expedited processing of INTERPOL Red Notices for internationally-wanted individuals, have all allowed INTERPOL to better tackle criminal activity, border-crossing procedures for INTERPOL officials still considerably impede the organization's ability to provide rapid support to its member countries.

When their support is requested by member countries, INTERPOL Major Event Support Teams (IMESTs) must often cross borders as part of their deployment to major public events. This was the case recently with the Winter Olympics in Canada in February 2010. Related administrative procedures, however, can often complicate a team's deployment and its ability to fulfill its duties.

Similarly, it is essential that INTERPOL Response Teams (IRTs, first established in 2002) are able to respond as

Delegates to INTERPOL's 1924 Second General Assembly in Berlin. This meeting formalized the Organization's mandate following its inception the previous year.

**"ICAO will be essential during the outreach phase of the initiative by providing a platform from which to engage with international stakeholders and market the project's many benefits. The Organization's endorsement of the project can only encourage further international recognition of the initiative by INTERPOL member countries."**

quickly as possible to disasters and incidents, such as the earthquake in Haiti in January 2010 or the Kampala suicide bombings of July 2010, and arrive on the ground with minimal impediments to their mission. In the aftermath of major crises such as these, delays caused by legitimate yet time-consuming visa requirements could indirectly result in key leads to international investigations being lost or compromised, and potentially to lives being endangered.

### INTERPOL Travel Document Solutions

In today's world, criminals are often able to swiftly cross borders while international law enforcement officials cannot.

The quicker that law enforcement can mobilize its responses to answer a country's call for assistance, however, whether to combat serious crime or in response to cases of disaster or major events, the safer that country, its region, or indeed the entire world will be.

It is in response to this need that the INTERPOL Executive Committee—one of the Organization's major governance bodies—approved the proposal to create a special INTERPOL Travel Document in March 2009. This decision will ensure that member countries can benefit from support and assistance without delay, whenever and wherever needed.



The new INTERPOL Travel Documents will take two forms: the e-Passport Booklet (bottom) and the e-ID Card (top and middle), which are being developed in partnership with the EDAPS Consortium and Entrust. Each will provide the most advanced and secure identification possible for future visa-facilitated travel by law enforcement officials.

The INTERPOL Travel Document will take two forms: the e-Passport and the e-Identification (e-ID) Card, which are being developed in partnership with the EDAPS Consortium, a Ukrainian-based secure ID specialist, and Entrust, a U.S. specialist in identity-based security solutions. Providing the most advanced and secure identification for future visa-facilitated travel by law enforcement officials, the INTERPOL Travel Document will set the international standard for many years due to sophisticated visible security features combined with high-end software enhancements.

The INTERPOL e-Passport booklet is a 34-page, fully machine-readable booklet containing a polycarbonate biographical data page. A high-capacity, contactless integrated circuit contained in the back page allows the document to meet ICAO requirements and ISO standards. It includes an embedded crypto processor with memory for storing the personal and biometric data of the authorized holder.

The state-of-the-art INTERPOL e-ID Card has an embedded high-capacity contactless integrated circuit, in compliance with ICAO requirements and ISO standards and containing the holder's biometric data and a duplicate of the MRZ data. The biometric data stored includes a high-resolution image of the holder's fingerprints and a photograph identical to the one printed on the front of the card.

INTERPOL is currently seeking official recognition of its Travel Documents from its 188 member countries and the granting of special visa status to authorized international law enforcement officials presenting them at border-controls. Countries recognizing these documents can decide what form the special visa status may take: a visa exemption, an expedited visa-issuance, or a similar special visa treatment to be determined by each country.

For INTERPOL, the world's largest international police organization, the successful completion of this project will enable international law enforcement officials to work more efficiently with each other and allow INTERPOL to fully carry out its original mandate of ensuring and promoting international police cooperation.

National borders, while legitimate and essential to territorial sovereignty, should no longer act as a barrier that criminals can manipulate to evade the police. With special visa status, law enforcement officials will be able to travel with minimal delay in order to follow-up on potential leads, respond to calls for aid, and effectively fulfill their primary duties.

To date, four countries have officially recognized the INTERPOL Travel Document, with a further 21 countries showing significant interest. INTERPOL continues to promote the Travel Document amongst its member countries to obtain further recognition and will officially present the project this November

to the organization's 2010 General Assembly in Doha, Qatar.

Since the beginning of this project, ICAO has been a key partner in supporting INTERPOL's efforts to launch its Travel Document. The three-letter 'XPO' code that ICAO has graciously allocated to the INTERPOL Travel Documents legitimizes them internationally and allows both formats to be accepted at borders around the world. The Travel Documents have additionally been allocated the two letter code 'XP' by the International Organization for Standardization.

ICAO will be essential during the outreach phase of the initiative by providing a platform from which to engage with international stakeholders and market the project's many benefits. The Organization's endorsement of the project can only encourage further international recognition of the initiative by INTERPOL member countries.

ICAO will also be pivotal in the processing of the INTERPOL Travel Document at border points. Its role in facilitating frontline border security through customs officials training programmes will help familiarize customs and immigration officials with INTERPOL's two formats of the Travel Document.

**"This partnership enhances the significant operational links which already exist between ICAO and INTERPOL, such as those established through the development of the Stolen or Lost Travel Documents (SLTD) database."**

This partnership enhances the significant operational links which already exist between ICAO and INTERPOL, such as those established through the development of the Stolen or Lost Travel Documents (SLTD) database. Border security activities, including the fight against international terrorism, have also benefitted from significant cooperation between the two organizations.

## Conclusion

By granting the INTERPOL Travel Document a special visa status, member countries will ensure that law enforcement officials will be able to react as quickly as possible to calls for assistance in combating international crime or in response to natural disasters and major events. Law enforcement officials traveling on INTERPOL-related matters will no longer have to delay their response to fulfill visa requirements and administrative procedures. Countries seeking assistance will receive it without delay, whenever and wherever it is needed. The INTERPOL Travel Document Initiative therefore represents a revolutionary step in international law enforcement cooperation and in ensuring greater security assistance to citizens worldwide. ■

# Best Practices in National Identity Management

**Last December, during the 19th meeting of the ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD), its New Technologies Working Group (NTWG) presented a working paper calling for a global focus on weaknesses in breeder documents and civil registries.**

**This vulnerability in the world's increasingly harmonized global border security and travel document regime represents a significant and persistent security failing—one which can compromise recent progress made through the implementation of Machine-readable Travel Documents (MRTDs) and electronic MRTDs (eMRTDs).**

**As Mauricio Siciliano of the ICAO MRTD Programme reports, while MRTD specifications are well-established in ICAO Doc 9303, little international regulation, if any, applies to breeder documents. During the TAG-MRTD 19th meeting, participants reached consensus that breeder documents and civil registry gaps require additional attention and global effort in order to codify best practices. These actions will help to ensure that this knowledge can be effectively shared by international stakeholders and leveraged for new programmes and capacity-building worldwide.**

While ICAO has no direct mandate to regulate breeder document norms, the TAG-MRTD agreed that addressing them is a legitimate and important area for ICAO involvement due to the vulnerabilities they can create for MRTDs and eMRTDs. The Group stressed that the upcoming 37th Assembly in 2010 presented a good opportunity to address this issue and for States to encourage ICAO to work in this direction.

It was also noted that the cost implications and diversity of existing practices worldwide should be considered when developing breeder document norms, as high costs or unreasonably high standards might hinder efforts toward universal implementation.

The TAG-MRTD acknowledged the importance of the breeder document issue and the necessity to undertake a review in order to identify suitable enhancements and improvements. It authorized the NTWG to engage in work directed to those ends and to develop approaches as outlined in this working paper, noting it remained at the NTWG's disposal for further clarifications and sanctions as needed.

### TAG-MRTD 19 Working Paper

Over the past several years, many nations have invested time, money and great expectation in enhanced travel document programmes. Machine-readable ePassports employing biometric identification capabilities have proven to be the new tool of choice in this regard for State travel document specialists.

By all accounts, the current generation of ICAO-compliant travel documents is the best and most secure the world has ever known. The travel document community can take great pride in this accomplishment, but a vulnerability remains that affects virtually all issuing authorities and which threatens to undermine or indeed subvert this important work: National Identity Management (NIM).

NIM refers to the various documents, civil registry systems and related media and methods that are used today to verify and/or validate a citizen or citizenship applicant's identity. Currently, many of the judgments that States arrive at regarding the issuance of a travel document are based in large part on the multitudinous and often unverifiable identity documents that the applicant can submit to validate their bona fides.

At last year's Fifth ICAO MRTD Symposium, speaker after speaker called for improvements and concerted effort on addressing and improving this situation.

In managing identity requirements for the benefit of their communities and citizens, National Civil Registration and passport issuing authorities must:

- Establish identity.
- Confirm citizenship.
- Assess entitlement.

While the latter two areas are primarily sovereign matters determined by national laws and policies, virtually all of the issues which these States must address and investigate in establishing identity are universal, common and shared.

Every applicant seeking a State identity card or travel document makes a claim to a particular identity. The first step of the respective issuing authority is to test that claim in order to establish identity. This is accomplished primarily through the following types of inquiry:

1. What does the applicant 'know' about the identity that is being claimed.
2. Who 'is' the applicant.
3. What does the applicant 'have' to support the claimed identity.

It is only through effective investigation into in all three of these areas that a high level of assurance of identity can be achieved.

Testing what the applicant 'knows' about the identity they are claiming usually involves completion of an application form in order to provide the State with information that can be further verified through an interview. Corroborating checks may extend to confirmations that the claimed identity is actually being used in the community—a process sometimes referred to as assessing the applicant's social 'footprint'. Identifying and articulating best practices in this area is one of the tasks identified in ICAO's Vision 2020.

Checking who the client 'is'usually involves the collection of and comparison with prior records of unique biometric information. For passports, photographs and signatures have been the traditional biometrics for this purpose; however with ICAO's development of the e-Passport, facial recognition and fingerprint and/or iris images now facilitate more automated biometric comparisons and verifications at issuance and at border clearance.

### Identity 'Haves' and 'Have-nots': Breeder Document Assessment Concerns

The primary subject of this paper is the final category, the testing of what applicants 'have' to support their claim to a particular identity.

The civil registration and identity documents which accompany an application for a travel document or identity card and which ultimately entitle passport issuance will be referred to henceforth in this paper as 'breeder' documents. They constitute the fundamental physical evidence accepted by national authorities to establish a *prime facie* claim to an identity.

This paper calls for a global focus on breeder document concerns, outlines several possible paths forward to improve the foundations on which the world's travel documents rely, and seeks TAG endorsement to carry out this work.

*Background and Present Status*

The threat of an individual presenting a genuine passport that was issued on the basis of false breeder documentation is very real. In today's identity issuance environment, presentation of these false bona fides and claims of entitlement can be rewarded with a new State travel, residence or identity document that has far more credibility than ever before.

Today's identity and travel documents contain advanced security features of great capability, such as chips containing the biometric information of the bearer. When present, these advanced capabilities and the information they carry can serve to enhance the legitimacy of the bearer who carries them and the documents that substantiated their creation. There is a much quicker and widespread presumption on the part of inspection authorities to 'accept' the legitimacy of these types of technologically-advanced documents.

In addition to introducing improved security features and biometrics through the latest chip-based technologies, many countries have also moved from a decentralized to a centralized system of personalization. This evolution allows issuing authorities to apply higher-quality personalization techniques and respond more quickly to the latest developments in the area of document fraud.

The introduction of new security features, production methods and personalization techniques has made the most recent generation of identification documents more difficult to forge than ever before. Moreover, improved staff training has also increased the likelihood of a counterfeit ID document or passport being detected by State officials.

These types of improvements have resulted today in an increasingly prevalent global shift from document fraud to identity fraud. Although look-alike fraud is still quite common, it is expected that the use of biometrics will shortly begin to impede this type of crime with much greater effectiveness. Over the next few years, a large number of identity, travel, residence and other identity documents will contain a biometric identifier that will enable verification within an automated environment—and even remotely if desired.

We live in an increasingly global context that more and more relies on high-quality identity documentation. In addition to the breeder documents themselves that are the 'usual suspects' used by individuals applying for travel documents (birth certificates, cards of national identity, drivers licenses, etc.), often, though not universally, the information that is captured in these and other breeder documents also resides in a national database.

While the existence, quality and ease of accessing these databases can vary dramatically from country to country, increasingly, governments have been focusing on them as sources of identity verification information either in lieu of or in addition to the breeder documents themselves. Some countries are beginning to link these data sources, for example birth and death records, to serve as automatic checks and verifications. This initiative seeks to acknowledge the importance of these secure sources of information and to offer suggestions on their use in addition to the documents themselves.

While databases can serve a very useful purpose in the verification of entitlement claims, limitations of a legal or privacy nature can also arise that impede the use and utility of database techniques.

*Avenues Forward*

To limit the impact and effect of this endemic and pervasive security vulnerability as much as possible, it is essential that the document community develop and articulate best practices, successful approaches and, where feasible, minimal security norms for civil status documents and the databases on which they depend.

This should be viewed and approached on the same basis as the process by which ICAO Member States have recently and very successfully defined minimum yet globally-interoperable security specifications for MRTDs, establishing a new coordinated level of global security while maintaining ultimate respect for State sovereignty concerns. One of the most important lessons to be taken away from the success which ICAO has achieved in the area of global MRTD advances is that globally coordinated and collaborative security advances and State sovereignty concerns are not mutually-exclusive.

There are two fundamental tools that the ICAO TAG has employed to this point to develop, assess, articulate and convey guidance and technical specifications: ICAO Doc 9303 and the Technical Report. While ICAO has the authority and capability to develop and publish travel document standards as outlined in Annex 9, the nature of breeder documentation does not neatly fall within that mandate.

Since the veracity and validity of the documents issued within the context of 9303 depend directly on the reliability of breeder documentation, however, ICAO could be seen to have a role and a responsibility to employ any and all measures available to improve this foundational component of the global MRTD system.

The first approach to the establishment of best practices in the area of breeder documentation could be considered within the same context and mechanisms by which 9303 has been able to codify non-mandatory minimum security expectations for travel documents. Admittedly, a very careful approach to this type of standards approach would be in order.

Secondly, in a historical sense the NTWG has focused on a number of specific issues and matters and addressed them through the drafting of Technical Reports. These work items have frequently, though not always, been codified eventually into document 9303.

The content of a Technical Report can be either normative or informative with respect to its relationship to 9303. With respect to the subject of breeder documentation, an area whose breadth and scope and sovereignty implications clearly suggest that standards might not be appropriate, the use of a Technical Report could be the vehicle to capture and codify best practices and other forms of helpful guidance in this area for States.

Technical Reports can also serve to underscore the specific nature of the breeder document problem and provide tailored solutions by which issuing authorities can enhance their assessment and judgement abilities in this area.

No matter what the final objective or destination, it remains clear that the path forward must fully respect the larger spectrum of State government direction, purpose, policy and need, in addition to being consistent with the ICAO Business Plan and the recently-introduced Vision 2020 Forum. In summary, this path should seek:

- To address the global threat to travel document integrity caused by entitlement judgments that are detrimentally affected by the weaknesses evident in current breeder document systems and processes.
- To focus broad international attention on the importance and magnitude of these threats with a view toward their mitigation and ultimate elimination.
- To create a forum and foundation for the development of worldwide security enhancements to breeder document verification systems, in the spirit that Annex 9 focuses on travel documents.

In addition, it should be noted that work will eventually be required as well over time in the other two areas that were noted previously as being important to the process and results associated with identity establishment. Specifically, this will involve the testing of what the applicant 'knows' and methods employed to verify who the client 'is'. ■

# Integrated AVSEC

**The 21st Century is witnessing law enforcement and security coordination on a level never before seen or possible. New database and chip-based technologies, combined with advanced communications networks, are now helping to coordinate law enforcement, intelligence gathering and border/identity security into a seamless and effective web to ensnare criminals.**

**In this special interview with the ICAO *MRTD Report*, new ICAO Aviation Security (AVSEC) Branch Chief, Jim Marriott, discusses his objectives for leveraging technological advances and integrating Security/MRTD strengths as the Organization drives forward new programmes that will lead to a stronger and more integrated global AVSEC/facilitation system.**

Jim Marriot is the current Chief of the ICAO Aviation Security (AVSEC) Branch. Prior to this posting, Marriott served for 25 years in a variety of senior level positions related to air transport and general transportation security with the Government of Canada. He was also a long-serving member on ICAO's AVSEC Panel during this period.

***ICAO Journal:*** **You spent a lot of time on the 'outside looking in' as far as ICAO is concerned… What was your view of the Organization over the years and what made it an appealing move to come to ICAO as head of the AVSEC Branch at this juncture in your career?**

**Jim Marriott:** As a speaker at the Machine-Readable Travel Document (MRTD) Symposium a few years ago, and especially during my time on the ICAO AVSEC Panel over the past years, it became clear to me that the Organization represented the ideal forum to be associated with in order to lead effective policy development and international efforts around all air transport security and facilitation concerns.

**In your view, how has ICAO's work in the area of MRTDs specifically contributed to today's more comprehensive and harmonized border security environment?**


Let me begin by noting that the reach and leadership of ICAO on MRTD development has been exceptional. The entire travel document environment, from passports and visas to national identity cards has benefitted tremendously from the continuous and comprehensive approach that ICAO took in this area. The Organization effectively coordinated the contributions and feedback of its 190 Member States and has helped the global air transport and border security communities to realize a truly amazing level of success over a relatively short period.

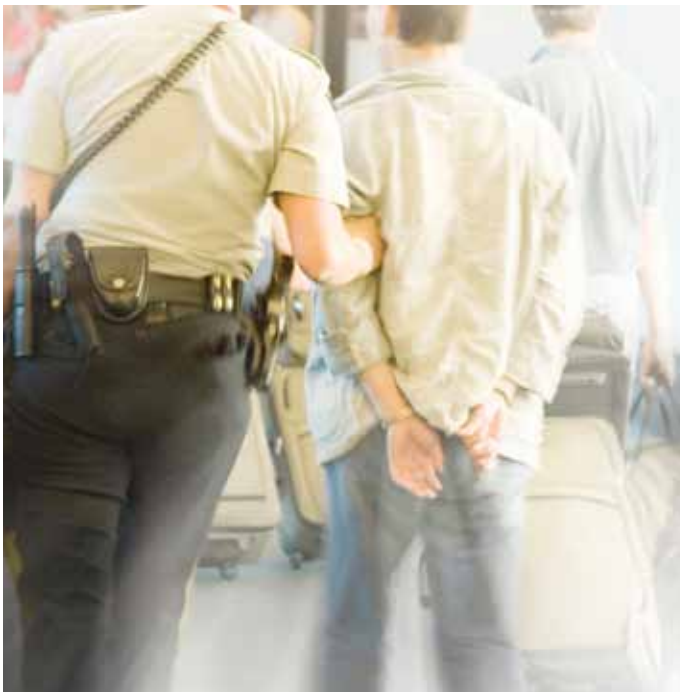
ICAO's ability to unite the international community around a common objective in this manner cannot be underestimated. I believe that untapped potential

**"The MRTD programme has been a very good example of something concrete that has been able to integrate different security disciplines around the idea that effective air transport security is not simply about stopping dangerous or contraband items going on board aircraft or being brought into countries. It is also about focusing security resources and stopping persons with unlawful intentions."**

for even further improvements in this domain still remains and that ICAO's continued leadership will be essential in reaching out to Member States so that further progress can be achieved.

**Do you envisage a more comprehensive security regime being established internationally, one that in part leverages the global interoperability and harmonization that the MRTD programme has achieved thus far?**

One of the things that we've all come to recognize in all security disciplines, whether it is front-line security in the policing sense, conventional aviation security, border security, intelligence, etc., is that security and law enforcement stakeholders experience their highest levels of effectiveness and success when the various security disciplines are working well together. The MRTD programme has been a very good example of something concrete that has been able to integrate different security disciplines around the idea that effective air transport security is not simply about stopping dangerous or contraband items going on board aircraft or being brought into countries. It is also about focusing security resources and stopping persons with unlawful intentions.



**That concept feeds into how INTERPOL and ICAO now are starting to work together more comprehensively in this area.**

Exactly. The point here is that terrorists and criminals want or need to travel at one point or another—for reasons related to the execution of an attack or crime, but also simply to advance their planning phases. Due to the advances in MRTDs and related data-sharing among border security and law enforcement stakeholders, that travel now provides an opportunity for the intervention of international and State-level authorities who can identify passengers of special interest and target their security resources accordingly.

**The MRTD programme began more as a facilitation priority. Do you agree that it's now also evolved into an important component in security-related measures?**

There's always been a dynamic tension by which industry and regulators have characterized the relationship between passenger facilitation and aviation security. Frankly I don't adhere to that view. My interpretation is that aviation security is necessary, border security is necessary, and the regular and efficient travel of people and goods is necessary. The question for all concerned is: how do we balance all those priorities?

MRTD advances have absolutely served to illustrate that there are win-win solutions available to air transport with respect to security and facilitation challenges. The integration of these priorities has led us to the point today where all passengers are now more secure, and yet their experience going through immigration and security checkpoints can be much faster than it was previously.

**How do you see ICAO's near-term security and facilitation objectives leveraging these win-win aspects going forward?**

Earlier this year, aviation security was reorganized in ICAO under the auspices of the Organization's new and more all-encompassing Aviation Security (AVSEC) Branch. This approach enables ICAO to more effectively coordinate its security policy and international regulatory frameworks, international oversight of air transport security and capacity-building efforts.

Aviation security, MRTDs and related facilitation concerns are part of this reorganization. It's absolutely my view that, by bringing together these formerly separate activities under one organizational structure, ICAO will be able to provide much more opportunity for balanced, integrated and win-win solutions to be achieved on all levels. I'm very excited about how some of the lessons we've learned in both the AVSEC and MRTD areas can be applied to the benefit of the other.

**Integration really is the key to success in this area then isn't it?**

This need for more effective integration, in addition to the very concrete benefits that have been demonstrated to accrue


from it, represent the most important lessons that security and enforcement stakeholders at all levels have learned post-9/11.

I remember attending an IATA AVSEC World Conference in 1994 where IATA's Director of Security noted that effective security needed to be founded on what he termed the "3-C's": Communication; Coordination; and Cooperation. Those words were prophetic in many ways and they're as relevant today as they were then. The key today is that we're seeing more and more tools and opportunities becoming available to really drive these types of '3-C' advances.

**How do you see ICAO's role evolving moving forward with respect to both AVSEC and MRTD capacity-building efforts for States?**

I think that it's very important for ICAO to establish particularly strategic and clear priorities with respect to its capacity-


building efforts in the AVSEC and MRTD areas. The Organization cannot be all things to all stakeholders.

That being said, I would also stress that capacity-building efforts are of very high value in security-related areas especially, if only because the old axiom still applies that any security system or framework is only as strong as its weakest links. ICAO is aware that there are States that need assistance and many others who are interested is providing this assistance, but the important role that the Organization has to play is in coordinating these efforts and needs in a way that provides meaningful support and improvement that can be sustained where needed.

I've noted over the years that ICAO is very good at capacity-building and I believe there's still room for us to get better at it.

**There's quite a bit of thinking these days surrounding the area of identity issuance and breeder document systems within States—notably the vulnerabilities that these can pose to the international MRTD regime that has now been established by ICAO. Is this an area where the Organization should begin to play a larger capacity-building and best practices role?**

Capacity-building and sharing of best practices are very much part of the role ICAO's MRTD programme is fulfilling today. I think it's especially important that ICAO work with States, other international organizations and industry to provide this kind of support. We can each leverage off the strengths and capabilities of the other. By working together in this way, we can make the best use of the resources available.

**What are your general MRTD and AVSEC priorities as you look out over the next months in your new role in the Organization?**

One main priority is to keep up the momentum that we've established so that the sustainability and future of the AVSEC and MRTD programmes is best assured.

Because of my AVSEC background I'm also well aware that in different States there are different organizational arrangements for the delivery of security—different ministries, different institutions, all with different responsibilities. Another important priority of mine for ICAO will be to have it promote dialogue between those institutions for the betterment of security. This is true for law enforcement and AVSEC stakeholders within States and between States as well.

Another area of priority would focus around general concerns regarding how ICAO helps States to determine and implement more efficient ways of delivering security. I believe that MRTDs especially can be more integrated into the broader transportation security world but the challenge is: how do we get there?

My belief is that through its leadership role ICAO can promote and enhance the collaboration and coordination of the many and highly motivated professionals and States involved. This is a big challenge but also an exciting one.

**Any additional thoughts in closing?**

My view at present about ICAO and its role in the security domain is that the Organization must continue to reaffirm its position as the 'air traffic controller' of security-related efforts and programmes.

For a variety reasons, security often gets broken down into different streams of delivery; it's my belief though that the MRTD world has clearly demonstrated that security is most effectively enhanced when we truly integrate the different streams of border, document and transportation security activity. There are still many opportunities remaining for global and State-level improvements in this regard and I feel very strongly that ICAO is in an excellent position from which to pursue them. ■

# Advancing PKD Awareness and Participation

## OSCE Event Draws Extensive High-level Input and Participation

**In May 2010, the OSCE Action against Terrorism Unit (ATU), in partnership with the ICAO Secretariat and PKD Board, organized a special OSCE Workshop on Promoting the ICAO Public Key Directory (PKD).**

**The workshop addressed the implementation of technical, operational and administrative elements related to the ICAO PKD—a single, multilateral technical platform designed to validate the authenticity of biographic and biometric data stored on the chips of e-Passports.**

**Some 200 travel document security experts from 53 OSCE and partnering States participated in the event, including 13 from other international organizations and 10 private sector specialists.**

The OSCE's May 2010 Workshop on Promoting the ICAO PKD built on the comprehensive OSCE mandate in the area of Travel Document Security (TDS).

The OSCE Action against Terrorism Unit (ATU), in cooperation with ICAO and INTERPOL, currently assists OSCE participating States with the upgrading of the electronic security features of their travel documents in order to enhance handling and issuance procedures, facilitate coordination with relevant INTERPOL databases and improve the detection of forged documents.

### Main Findings of the Workshop

A wide range of high-level presenters to the Workshop stressed a number of matters relating to the importance of increasing support for, and broader implementation of, the PKD system amongst OSCE States.

It was generally stressed by all that the broad participation seen at the event confirmed both a significantly increasing level of interest in the PKD and participating States' belief in its role as a fundamental component

in a robust international travel document and border security framework.

The following is an abridged summary of the findings and opinions that helped to shape the proceedings:

*The ICAO-compliant e-Passport is considered to be the most advanced travel document to date.*

Currently, 54 OSCE Participating and Partnering States are issuing the technologically-advanced and biometrically-enabled e-Passport. In many of these cases, a good portion of the investment involved has been aimed at developing State Public Key Infrastructures (PKIs) to help bolster overall national identity management systems. It was stressed that that ICAO-compliant e-Passports, together with supporting PKI efforts, have contributed to a more harmonized and citizen-friendly travel environment by providing border control authorities with the right tools to make more informed, safe and rapid assessments.

*The ICAO PKD completes the authentication process of e-Passports at border control.*

It was reaffirmed at the OSCE event that e-Passports are only as good as the authenticity of the electronic information contained in them. Failing to give border control agencies the tools to validate the authenticity of this information negates many advantages of the e-Passport. The PKD not only offers the information needed to validate the authenticity of e-Passports, it also ensures the accuracy of their data and simplifies methods of exchange. The PKD enhances the security of e-Passports by offering a global multilateral framework to verify the entire chain of certificates which together ensure that the biographic and biometric data stored on e-Passports chips has not been tampered with.

*The ICAO PKD facilitates fast and secure cross border movement.*

The PKD simplifies and enhances the security of the e-Passport validation process at border control. This provides citizens with the tangible benefit of being able to cross borders ever more quickly and easily as associated facilitation technologies which take advantage of this functionality continue to be implemented. In turn, the validation of e-Passports through the ICAO PKD offers border control authorities the highest possible chance of preventing terrorists and other criminals from crossing borders undetected using false identities.

*The ICAO PKD is a resource for increasing trust in e-Passports.*

Through their sharing of certificates and revocation lists via the PKD with foreign border control agencies, States promote increased trust in their travel documents. Specifically, the timely distribution of information about compromised or otherwise invalidated certificates—the certificate revocation lists—via the PKD enables border control officials to more effectively detect potential fraud. The PKD is also an important measure to address the citizen privacy and data protection concerns which are often associated with e-Passports, mainly due to media misrepresentations of the associated technologies and capabilities.

*The ICAO PKD is cost-effective and efficient.*

The bilateral exchange of certificates and certificate revocation lists is complex, cumbersome, error prone and time consuming. Sharing such data via the PKD streamlines this process and consequently reduces administration costs. Costs are further reduced by more States joining the PKD which lowers the Annual Fee for each PKD Participant. Considering the expenses of introducing e-Passports and creating the related PKI necessary to process such data, the expenditure of participating in the PKD is very low.

*The participation in the PKD requires due diligence.*

The event helped to establish that careful planning and preparation before PKD participation ensures quality and standard compliance from the onset and reduces related implementation costs. This preparation includes defining roles and responsibilities for the PKD within the national context and reviewing national legislative frameworks as part of initiating the participation process. Once participation becomes effective, countries have a window of 15 months before becoming an active PKD participant; i.e. before they begin to upload and download their data. During this period technical support is readily available from the PKD entities, including compliance testing support and an interface test benchmark. In addition, experience from other PKD participants enables new adopter States to fine-tune process designs related to PKD implementation and border control operational issues.

*e-Passport adoption and PKD participation should be part of a comprehensive national identity management system.*

Rather than solely investing in the physical security and trustworthiness of travel documents, investments should also focus on strengthening national identity management systems, in particular as they relate to the assessment of travel documents. Securing the identity chain through the development of robust issuance systems, interlinked with civil registry information, is an important prerequisite to prevent criminals or terrorists from obtaining a genuine e-Passport under a false identity.

In addition, any State investing in a national PKI should also consider its versatile applicability beyond travel document

security. It could form part of an even more advanced and harmonized border, travel, and identity management environment that makes use of the latest technologies in line with broader State security and mobility objectives affecting areas such as aviation and trade.

### Future OSCE/ICAO Cooperation Relating to the PKD

Participants agreed on a range of suggestions relating to possible OSCE support and participation in future outreach efforts relating to ICAO PKD adoption by States. Some of the ideas discussed included:

- Organizing a follow-up OSCE-wide Workshop examining the ongoing progress of OSCE participating States seeking to join the PKD and addressing potential stumbling blocks.
- Organizing follow-up national and regional awareness raising workshops in close co¬ordination with ICAO and the ICAO PKD Board, in order to increase participation in, and use of, the ICAO PKD. This could include:
  - Facilitating the exchange of experiences and best practises between ICAO PKD participants and potential PKD participants.
  - Demonstrating the technical, operational and administrative elements related to the PKD.
- Developing a national ICAO PKD training programme, targeted at decision makers and senior officers, as part of the preparation process in States seeking to participate in the ICAO PKD. This could include:
  - Drafting and providing model legislation to overcome initial legislative obstacles in the adoption process.
- Facilitating expert technical assessment visits for OSCE participating States requesting PKD participation and assisting with the review of national identity management systems as part of a broader process to enhance the overall security and trustworthiness of the e-Passport network.
- Promoting e-Passports and the ICAO PKD in the public/media sphere, including popular and specialized publications, in order to placate misunderstandings and concerns pertaining to privacy and data protection issues surrounding advanced chip-based, biometric identity tools. ■

# Implementing e-MRTD
## Part 3: Approval and Operation

**In this third and final instalment in his series describing the structures and processes required for ensuring the successful management of an e-MRTD implementation project, Markus Hartmann of HJP Consulting discusses the final Approval and Operating measures.**

**He and special guest co-author, Diana Ombelli, stress the importance of a professional testing approach, both for individual components and the entire system prior to completed delivery. They also cover the required quality assurance measures that are needed in the early operational phases. To conclude, the final section of this joint submission deals with the importance and benefits of a properly structured Service Level Agreement.**

Markus Hartmann is the founder and CEO of HJP Consulting GmbH, a consulting firm specializing in the planning, procurement and approval of e-Passport and e-ID card projects. Hartmann is an expert in e-MRTD solutions and project management and has advised governments implementing national e-Passport projects in Germany, the UK, U.A.E. and Oman. He also serves as ISO delegate in the ICAO Implementation and Capacity Building Working Group and, prior to forming HJP Consulting, was a member of the executive management board of a leading smart card manufacturer.

Diana Ombelli MSc. is a Senior Consultant and Project Manager. She is well-known in the travel document community through her recent work with many companies and government departments across Europe. Ombelli previously worked with Morpho (formerly known as SDU Identification) on projects involving the development of travel and identity documents and the implementation of related IT systems. In 2008, she co-edited the book about the development of secure documents entitled: Documents: the Developer's Toolkit.

Take a close look at your passport for a moment. Feel its outside cover; admire the elegant presentation of its coat of arms. Now open and count how many designs and colours you can see on the different pages.

If you rotate the booklet and view it from above, you'll partially discover the dozens of different materials furnished by an even higher number of suppliers that are responsible for helping to produce the document: from security paper to plastic and transparent foils; multilayered cover material; gold/silver block foil; durable glue; several offset, intaglio and serigraphy inks; binding thread; electronic components; etc.

Your passport is not simply 'a booklet', after all, but rather an intricately designed and ultra-secure identity tool. e-Passport manufacture in particular requires up to 25 different production steps. Supporting the manufacturing process is the e-Passport issuance system, containing countless components often widely distributed at multiple sites (e.g. 5,700 municipalities in Germany). The related systems are generally integrated into a larger National Registration IT infrastructure.

### e-MRTD Implementation Final Stages: Approvals

Assuming that all the tasks in the previous e-MRTD implementation phases we have discussed in past issues of ICAO's *MRTD Report* (i.e. Initiating; Planning; Procuring; Implementing) have been performed in accordance with established benchmarks, stakeholders at this stage in their e-MRTD transition project will now be faced with the specific process aspects needing to be approved. The two most important components requiring approval testing are the e-Passport booklet itself and the issuance system supporting it.

If one considers the e-Passport booklet as the key security anchor in the overall system, it becomes apparent that in-depth testing will be required at this stage, both internally between the

producer and the issuing authority and externally between the issuing authority and other national or international authorities.

The focus of the booklet's testing will be durability, security and its conformity with international standards (particularly ICAO Doc 9303, incl. supplements, and related ISO materials). The following sections in this article, entitled *Interoperability Testing and Product Testing* will extensively discuss all relevant booklet testing considerations.

Regarding the e-Passport issuing system, the testing in this instance will include component tests and system integration testing. The focus of these measures is functionality and usability, security, and lastly performance. These are discussed in more detail the section entitled *FAT/SAT*.

**Figure 1: The e-MRTD-related planning and approval process based on the HJP V-Model**

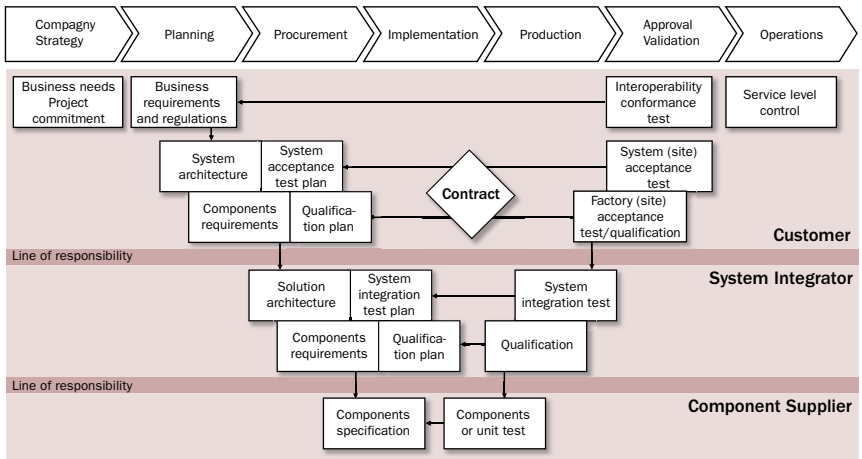
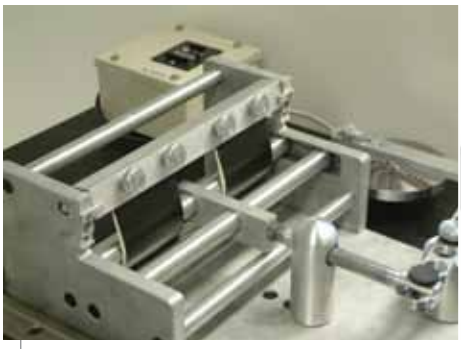



Figure 1, above, illustrates the project steps associated with these requirements and highlights the deliverables in relation to testing for each of the three project parties (customer or issuing authority; system integrator; and component supplier).

The planning and approval model follows three basic principles: analyze; specify; and qualify. Analysis requirements include the observation of the 'as-is' situation. Specifying defines the 'to-be' situation. Qualifying refers to the



A typical e-Passport bending test.
(Courtesy Pira International)

An e-Passport impact test.
(Courtesy Pira International)

verification of the new system's practical compliance to the determined specifications.

The following discusses how one can make sure that an electronic passport is manufactured according to the supplier's specifications and that it will provide identity information worldwide with guaranteed interoperability.

*Interoperability Testing*

Extensive interoperability e-MRTD testing took place in Berlin (2006) and Prague (2008). Later, the Brussels Interoperability Group (BIG) organized various test events. These latter events brought industry and government officials together with the objective of verifying whether electronic hardware and software components could communicate with each other. The results achieved, however, were often simply a snapshot of the specific hardware components working over a finite time period with arbitrary software versions still under development.

As International Standards have reached a more mature and robust approval level in recent years, we tend to be concerned today more about conformity testing. Laboratories in these instances perform experiments in order to verify that a given e-Passport complies with the appropriate standards —the interoperability aspect of the booklet implicitly being verified as well.

ICAO provides the relevant test standards, but for the time being, refrains from facilitating any testing and certification schemes which authorities could use when seeking final approval upon their e-Passport achieving conformity with the standards. In order to more comprehensive levels of global interoperability, the conformity test schemes (test contents and accreditation of the laboratories) may eventually be standardized and endorsed by ICAO as well.

Additional information on conformity testing and related requirements follows in the next section.

*Product Testing*

The highly complex nature of an e-MRTD implementation process calls for rigorous testing activities. Some passports may be valid for periods of up to 10 years; however authorities are often granted far fewer years of warranty from their suppliers. If passports should fail, the reputation of the issuing State and of the holders themselves is at risk. Intensive testing and a focussed quality assurance regime aim to minimize this risk.

There are basically two main streams of testing objectives. The first is in line with each project's methodology: compare the product to the initial requirements' respective specifications. The qualification plan includes the testing aspects and pass/fail criteria for this comparison. The second testing stream is related to the function of the product: the e-Passport as an effective and secure carrier of identity information which needs to be read worldwide during the entire period of its validity.

We can also distinguish additional areas that benefit from adequate testing:

- Compliance to International Standards.
- Functionality.
- Durability.
- Effectiveness of security features.
- Interaction with personalization technologies.

We assume in every case that an e-Passport's requirements conform to recommendations from ICAO Doc 9303, Part 1, Machine Readable Passports, Volume 1: Passports with Machine Readable Data Stored in Optical Character Recognition Format (physical and OCR requirements); as well as Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability (electronic requirements).

It is then crucial that both aspects, the physical and the electronic, be addressed during the conformity testing.

Table 1 on page 28, provides some insight into the current reference literature associated with the testing of e-Passports.

ICAO has not yet issued a comprehensive test specification covering the optical and physical security features as specified in Doc 9303, Volume 1, but this gap should hopefully be closed soon. There have been a few proposals regarding how to quantitatively evaluate the value of the optical security features but as yet no methodological approach to assess the

effectiveness of the chosen security features. The current practice is to ask an expert panel to give its opinion based on a formal checklist.

ICAO's Technical Report, *Durability of Machine Readable Passports*, is conceived as a set of instructions for the prototype evaluation of e-Passports where the physical characteristics are considered. The introduction of this report states:

> *"Prototype evaluation is an instrument to establish the ability in principle of a specified type of document to fulfil the requirements of use".*

It suggests this type of testing be conducted at an intermediate stage prior to mass production. The proposed method tests the functionality and durability of the e-Passport, as well as its compliance to International Standards.

Finally, the interaction of the booklet with the personalization technology is considered. Take care about this aspect, particularly when it is performed by the issuing authority. A good practice is to include pre-production batches of the appropriate e-Passport booklets in the FAT and SAT. As a matter of fact, during those test activities mechanical, electronic or chemical issues may arise, requiring adjustments to both the booklets and the machinery.

*FAT /SAT*

Testing of the e-Passport issuance system became an even more important consideration upon the introduction chips into e-Passports. This now means that the issuing authority actually becomes part of the production process of the e-Passport. Personalization of the chip requires multiple interfaces, to the manufacturer's IT system as well as to existing legacy systems at an authority's site.

The test and approval of the e-Passport issuance system is therefore one of the issuing authority's key responsibilities. This is the point where final checks are made to ensure that the supplier has performed as initially proposed. In return, the supplier is seeking approval for the final milestone before starting operations. Be cautious however: after all the boxes are ticked the supplier will effectively be intending to transfer the full risk of failure to the customer at a point when said customer also has to release the balance of payment to the supplier.

In light of the above it is imperative that all issuing authorities carry out due diligence before providing their final acceptance of the certificate. The process involved in doing so is often divided into the Factory Acceptance Test (FAT) and the Site Acceptance Test (SAT).

**TABLE 1: REFERENCE LITERATURE ASSOCIATED WITH THE TESTING OF e-PASSPORTS.**

1. ICAO Technical Report, Durability of Machine Readable Passports
2. ICAO Technical Report, RF Protocol and Application Test Standard for e-Passport – Part 2: Tests for Air interface, Initialisation, Anti-collision and Transport Protocol
3. ICAO Technical Report, RF Protocol and Application Test Standard for e-Passport – Part 3: Tests for Application Protocol and Logical Data Structure
4. ISO/IEC 10373-1:2006: Identification cards – Test methods – Part 1: General Characteristics
5. ISO/IEC 10373-6:2001: Identification Cards – Test Methods – Part 6: Proximity Cards

During the FAT the overall issuance system or parts therein are tested at the supplier's site. The issuance system will be tested separately from the customer's existing legacy systems. From the authority's viewpoint this is not a particularly useful exercise. In the next phase, the supplier is required to deploy a fully functional smaller test system at the customer's site – generally referred to as a Site Acceptance Test 1 (SAT1). After all tests in the real environment have been passed, the supplier then deploys the complete scope of the project. A SAT2 process ensures that the overall system is working fine.

The acceptance testing itself should follow a predefined procedure. All testing steps should be well documented, forming a sequential chain of tests comparing actual performance metrics all the way back to the initial requirements. The detailed scope of work of this project shall be fixed within the requirements specification. In the related qualification plan, the customer defines how each deliverable shall be tested. The supplier then derives a comprehensive set of test cases conforming to the respective test specification.

The execution of the tests is again the supplier's responsibility, while the customer shall audit and review the test process. This sharing of responsibilities between customer and supplier should become an integral part of the procurement contract.

Whether the test and approval process was successful or not has a direct impact on the operating phase. When it comes to a warranty claim, the supplier might only provide a 'free of charge' replacement if the defective feature had been tested properly during the SAT phase. Another impact can be seen in this respect on the Service Level Agreement (SLA): the performances measured during SAT need to define the expected performance of the system fixed in the SLA.

## Operating

### *Quality control*

HJP considers quality to be reflected most clearly by the final product's ultimate compliance to the customer's original expectations. Quality is essential not only with respect to complete project documentation but also to all components and systems.

The common business requirement for e-Passport suppliers is to have a valid ISO 9001 certification. That is, however, only a starting point. The ISO certification guarantees that the organization's main processes are described and that it acts according to them. This certification doesn't include the quality assurance of its products, which needs to be documented as a part of the project's earlier-stated deliverables (in the HJP V-Model this would be realized during the Service Level Control step).

Quality Assurance (QA) can be defined as all those activities necessary to ensure that a component or a system conforms to the established technical specifications. We can state in this sense that "what you can measure, you can control".

Quality control (QC) involves checking objectively those characteristics which are measurable. As a part of the QC process, all deviations observed during the inspections have to be reported within the supplier's organization and appropriate corrective measures need to be agreed and documented.

Referring specifically to e-Passports, QC therefore primarily applies to:

- **Incoming goods inspection:** The examination of purchased raw materials and semi-manufactured products: e.g. paper; inks; or chips inlays.
- **Process control:** Performed during or at the end of the manufacturing process. Features are checked by the operator in order to monitor the production process: e.g. the de-lamination risk of a polymeric data page.
- **Outgoing inspection:** Final check of the end product before shipping.

Products manufactured within the same production batch can differ from each other, mainly because the production processes are subject to climatic, technological and staffing related influences resulting in variations of the associated outputs. This is the reason why suppliers try to minimize waste and start discussions with their customer on Acceptable Quality Levels (AQL's). This determines the range of tolerance for acceptance of the product.

It is also a good practice to establish a formal procedure for the outgoing inspection between supplier and customer. In this case a number (to be agreed upon) of documents are randomly extracted from the boxes and inspected

by the customer according to an agreed checklist, including norms and AQL's. If the documents comply with the agreed norms, the complete batch is approved and can be shipped. Do not be shy to ask questions during this check and to look for all possible deviations.

*Service Level Agreement*

It is equally important that the issuing authority ensures the continuity of supply of its e-Passports at any time. Often this is done by keeping extensive stocks of booklets and consumables and by over-sizing the IT infrastructure: however the agreement of specified service levels with the supplier is a much more cost effective approach.

Service levels agreements are common practice when it comes to the delivery of goods and reaction times within the service and maintenance agreements. Lately, authorities have also begun requesting that their suppliers grant transaction times; i.e. for the enrolment process or passport personalization regardless of any maintenance breaks, etc.

The more stringently all processes and deliverables have been documented throughout all the project phases, the easier it is to develop, execute and control this type of detailed SLA.

## Conclusion

Operating an e-Passport issuance system remains an everyday challenge for the issuing authority. During the operating phase in particular, however, all the efforts and attention spent during previous project phases will begin to pay off. SLAs and AQLs will keep the performance levels high. The intensive testing of the e-Passport booklet and the IT infrastructure will have reduced the probability of failures down to a very low percentage.

This was the last out of four articles on the project management considerations involved with 'Implementing e-MRTDs'. Best practices in all six phases, from initiating to operating, have now been covered. Beyond the many benefits already illustrated, the most important is that the issuing authority applies their own intelligence and resources to their e-Passport issuance system. This know-how ensures that the authority's project teams always remain in the driver's seat. This is the best means of empowering the team operating the system and of initiating effective improvement projects in the years that follow. ■


# 39 Myths about e-Passports: Part III

**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 27 thru 39 are reflected in this final instalment.**

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 has been grateful to Keesing for providing it with the permission to reproduce this very useful review 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 final instalment in the *MRTD Report*'s review of related facts to help readers debunk common fallacies and myths currently being reported about e-Passports.

MYTH #27

**The EU has stated that e-Passport security is 'poorly conceived'.**

In September 2006, the 'Future of Identity in the Information Society' (FIDIS) published their 'Budapest Declaration', which attacked the concept of the e-Passport. Unfortunately, they used for their information some of the previously published reports from hackers and 'security researchers' (most of which are included here as 'myths'). Their report included the statement that 'the current implementation of the European passport utilises technologies and standards that are poorly conceived for its purpose'.

FIDIS was in fact funded by the EU, but their declaration does not represent the views of the EU. If it did, then it would be inconceivable that all the countries of the EU would have introduced e-Passports.

Among the 'weaknesses' described by the FIDIS was the reading of the chip once the BAC key had been determined (Myth #8); tracking of citizens (Myth #11); setting off explosives (Myth #31); and that sensitive biometrics such as fingerprints would not be protected by Extended Access Control (EAC) (Myth #23).

MYTH #28

**Outsourcing the manufacturing of e-Passports to overseas companies is a national security threat**

This myth started when the United States granted a contract to a company that was manufacturing the e-Passport booklets in Thailand. This was done apparently for cost saving – but it was claimed that this threatened national security.


While the theft or diversion of traditional passports is a security issue – as the blank passports, containing security safeguards, can be filled in and effectively used – the same does not apply to e-Passports. The e-Passports are only personalised and digital signatures are added after they are delivered to the passport issuance agency. Anyone programming a stolen blank e-Passport with their own information and digital signature (see Myth #20) will be detected by the PKI authentication.

MYTH #29

**The e-Passport should be protected by a PIN**

This myth is usually mentioned as an alternative to the BAC key derived from the MRZ data. There are a number of problems with this idea. Firstly, passports are generally used infrequently, so a large percentage of travellers would probably forget their PINs. Would this then lead to them being refused entry? Secondly, people can only usually reliably remember PINs with 4 or 5 digits, a few might remember 8 digits. Unless the number of tries was restricted (the passport being 'locked' if the PIN was entered incorrectly say three times), hackers would be able to guess the PIN by brute force attack much more easily than the 24 digits of the BAC.

Another consideration is efficiency—it is very efficient to machine read the optical MRZ and use the key derived from the data to unlock the chip—manually entering a PIN on a keypad takes much longer.

MYTH #30

**Metal shields or jackets do not protect against unauthorized access**

The chip of the e-Passport cannot be read if the booklet is placed in a metal jacket. The jacket forms a 'Faraday cage' which prevents radio waves from reaching the chip's antenna. A metal shield, such as a metal insert in a page, is just as effective as it 'decouples' the antenna and prevents it from resonating at the frequency of the radio waves.

If the radio waves cannot reach the chip's antenna and resonate it, then the chip cannot be powered and it cannot communicate.

The myth arises when alternatives to metal are used as shields or jackets. Aluminized plastic is a common alternative, and its thin coating of aluminium does not effectively block strong radio waves.

MYTH #31

**The e-Passport can be used to set off explosives**

This myth started with a demonstration that the company Flexilis made in 2006 showing a partially open e-Passport setting off a small explosive charge as it was moved by on a cable. The e-Passport was open ½' (12.5mm) and the claimed reading distance was 4' (10cm). The e-Passport contained a single metal inlay shield page. The company was attempting to show that two shield pages were more effective in protecting the e-Passport data. The e-Passport was not protected by BAC.

There are a number of difficulties with this demonstration. The chances of a person walking past with their e-Passport less than 4' from a reader attached to an explosive charge and triggering it because their e-Passport is open by ½' is minute. It is fairly obvious too that the demonstration relied on the presence of e-Passport being detected, rather than any comprehensive read to find the nationality. The e-Passport would have to be within the 4' range for at least a couple of seconds for the reading process to get useful data. As well, the orientation of the e-Passport antenna with the reader antenna would have to be favourable, any mismatch causing the radio waves to be attenuated would break the communication.

Most e-Passports are now protected by BAC, so accessing the chip in this way is impossible. Even if the BAC key was known, and the target was one person, the BAC process and reading the data would take 3 to 4 seconds at least, that is, the target's e-Passport would have to be within perfect range of the reader for this time. In any case, if the target was known, there would be simpler ways of achieving the explosion—detecting their cell phone or recognizing their face using facial recognition techniques comes to mind. A system targeting one nationality or specific people is just a myth.

MYTH #32

**Sending illegal commands and observing the e-Passport response can be used to determine the nationality of the owner**

A group of security researchers experimented with sending illegal commands and observing the responses from different e-Passports. As illegal commands are not specified in the ICAO standard, different manufacturers have implemented their handling systems differently. The researchers claimed to be able to identify the nationalities of the e-Passports and hence speculated that terrorists could use this technique to target specific nationalities.

The researchers were not identifying nationalities but the manufacturers of the chips. It just so happened that their small collection of e-Passports were all made by different manufacturers. There are only a few manufacturers, and so as many countries buy from the same manufacturer, or as countries change their supplier from one manufacturer to another, the connection between manufacturer and nationality is broken. Thus the nationality of the owner cannot be reliably determined.

MYTH #33

**The BAC is easy to overcome**

This myth takes the form of: 'a Dutch passport was hacked live on television' or 'highly structured sequences that are easy to overcome'. Hackers attack the e-Passport by brute force, trying to guess the BAC key by trying different combinations. However these publicized attacks always reduce the document number, the date of birth and the date of expiry to a manageable small set, say one or two hundred combinations, to be able to succeed.

If we take a more reasonable scenario: we guess the person's age to plus or minus 5 years; we estimate the e-Passport number to within a typical 1 year production of 3,000,000 booklets (and this fails as countries randomise their passport numbers); we estimate the issue date to within 1 year; and each attempt to guess the BAC key takes 30ms as the e-Passport takes this long to respond.

So then we have 10 years (3650 days) multiplied by 3,000,000 multiplied by 1 year (365 days), which equals 3,996,750,000,000. At 30ms per try, this number of combinations would take 119,902,500,000 seconds, or 3,802 years. Even if we assume that it is reasonable that there is a 50/50 chance of the right key being guessed by half-way though the guesses, this would still take 1901 years.

Even if the person's date of birth is known from other sources, the above favourable scenario would still take 380 years in total, or 190 years on average.

So to say the BAC is easy to overcome is a myth.

MYTH #34

**The BAC is based on place of birth; name; etc**

The BAC is based on the passport number, the date of birth and the date of expiry. As only the date of birth is potentially available from other sources, this gives considerable protection. Issuing authorities now randomise the passport number, so there is no connection between this number and the expiry date (as there might be if passports were issued in chronological and numerical order).

Hackers speculate that the BAC is based on other data such as the place of birth or the name as these are also potentially available from other sources. But this is a myth.

MYTH #35

**The e-Passport data can be eavesdropped by listening to the radio wave transmissions**

The BAC also encrypts the radio wave transmissions between the e-Passport and the reader. These can be intercepted at a distance. The furthest distance we have seen is about 10m, although some hackers claim 50m or more. However, even if the hacker intercepts ('eavesdrops') the transmission, the data is encrypted and they have to undertake a brute force attack as described above in myth #33. Thus the e-Passport data cannot simply be eavesdropped by listening to the radio wave transmissions.

As well, readers are now designed with anti-eavesdropping properties, either by reduce stray transmissions or by masking the transmissions with 'noise'. In any case, places where readers are most often used, such as airports, contain multiple readers whose radio transmissions are most likely to interfere with each other at a distance, making eavesdropping impractical.

It is worth noting that unwanted stray transmissions are not just the property of contactless chips. All electronic devices radiate to some extent, one of the most common sources being the computers where the e-Passport data is processed. Power and communication lines (eg USB) also radiate. Therefore authorities usually take a system-wide approach to this problem and eliminate unwanted transmissions from all sources, not just the reader-to-e-Passport link.

MYTH #36

**The e-Passport can be easily cloned and this is a vulnerability**

This is a common myth and usually takes the form of hackers and journalists claiming that they have 'cracked it!'. All they have done is to read the data from the e-Passport chip (after satisfying the BAC protection as per the standard) and to programme another chip with the same data. Reading the data from the chip is exactly how the system is meant to work. Programming another chip with the same data is about as useful as photocopying a traditional passport—it is not going to get a different person through border control. In any case, the cloned chip has to be incorporated into the traditional paper passport booklet, with all its security features, which is not a trivial exercise.

The myth often implies that the cloned chip can then be altered with a different photo or personal data (eg the 'Elvis' e-Passport story). While once the data is altered this is no longer a cloned chip (ie an exact copy), any tampering will be detected by the digital signatures and the PKI authentication process.

An optional specification in the ICAO Doc 9303 standard is 'Active Authentication' (AA). AA works by having a private/public key pair, where the private key is imbedded in the chip and cannot be read out. If the public key is then copied (cloned) to another chip along with the rest of the data, the keys will no longer match and an AA authentication check will reveal this. Many countries have adopted AA and this will effectively eliminate cloning, although we believe that cloning was never a serious vulnerability.

MYTH #37

**Active Authentication can be defeated by turning off the indicator in the Data Group Presence map**

We have to delve into the technicalities here as the hackers sometimes get into this level of detail. In brief, the Data Group Presence Map (the EF.COM file) indicates which data groups are present in the e-Passport's chip. This is for the convenience of reading systems which would otherwise waste time trying to read non-existent data. The EF.COM file is not protected by a digital signature, so hackers can remove the AA indication here and claim that their cloned chips will not be inspected for AA as the inspection system will not be aware that it is present. In fact, hackers could remove the indication for any other data group, eg fingerprints, and try to circumvent border controls.

ICAO has recommended that, as a matter of good design, the EF.COM should not be relied upon, but in fact the Document Security Object (the EF.SOD) should be used to find which data groups are present. The EF.SOD is protected by a digital signature so any tampering will be detected.

MYTH #38

**Extended Access Control can be circumvented as the chip has no clock and cannot tell if a stolen reader certificate has expired**

Another technical detail myth. Extended Access Control (EAC) works by both the e-Passport chip and the inspection system proving to each other, by means of certificates, that they are authorised to access each other. If an inspection system is stolen then its certificate will expire and it will be unable to access the sensitive EAC-protected data (fingerprints and iris scans).

The hackers claim that because the chip has no clock then it cannot know what the current date is and that a stolen inspection system's certificate has expired. However, the e-Passport chip has its date updated every time it encounters an inspection system. It is most unlikely that when travelling the first inspection system that is encountered would be stolen. Therefore the first inspection system encountered will update the chip's date, and any subsequent attempts by a stolen inspection system to acces js the chip's data will be denied. The inspection system certificates are typically issued on a daily basis, and so expire quickly.

It should also be noted that typically the certificate does not reside in the reader part of the inspection system. If a machine reader is stolen it is unlikely to contain the necessary certificate. It would be entirely another matter, and very difficult, to steal a complete inspection system.

MYTH #39

**Because only a small percentage of countries have joined ICAO's Public Key Directory, country signing certificates are not being checked and forged e-Passports are getting through border control**

The ICAO Public Key Directory (PKD) offers the best way for countries to obtain current Document Signer (DS) certificates and Country Signing Certification Authority (CSCA) certificates. The PKD is also planning to hold Revocation Lists (RL) of compromised e-Passports.

However, this is not the only way that border control authorities can obtain these certificates. Commonly they can also be obtained by bi-lateral means (eg diplomatic channels) or from Master Lists held in a region. Therefore hackers should not assume that because a country does not belong to the PKD that it is not using DS and CSCA certificates to validate e-Passports at its borders.

As more countries start to issue e-Passports, the complexity of obtaining the certificates by bi-lateral means increases, so we can expect to see more countries joining the PKD in time. ■

## 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.

# Does Your Data Quality Jeopardize Your Investments?

Which photo will pass the biometric control? Correct matching relies on biometric data quality.

Who's who?
With the right data quality the fraudster is detected instantly.

Which is real, which is fake?
Your biometric data quality will determine the verdict.

What do the eyes say?
High-quality biometric data tells more than a thousand words.

No matter how much you invest in Automatic Border Control and E-Passport Solutions, low-quality biometric data will render the system useless. The cost of additional quality reviews after installation will be high and unpredictable and both the financial pay-back and the rule of law will be severely compromised.

Speed Identity is the world leader in biometric data capture. We help authorities and organizations worldwide in securing the quality of passport controls, ports, power plants or wherever the demand for quality and precision in identification is high.

At the ICAO and Biometrics exhibitions we give you the opportunity to try the biometrical product of tomorrow; Speed Capture G3, called "Sherlook" thanks to its ability to identify differences and find out "who's who".

Welcome to Speed Identity!

Welcome to our stand at ICAO and Biometrics 2010.

**SPEED IDENTITY™**

High quality for passport and border controls.

Mediavägen 11, 135 26 Tyresö, Sweden, www.speed-identity.com, +46 (0) 8-448 70 00

**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.

## MRTD Partnership Community — Industry Partners

Visit them at www.icao.int/mrtdc

**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.

## MRTD Partnership Community — Industry Partners

Visit them at www.icao.int/mrtdc

**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.

## MRTD Partnership Community — Industry Partners

Visit them at www.icao.int/mrtdc

# Enhance your visibility


## The world's most trusted MRTD Web site

The **MRTD Partnership Community** is the only globally recognized Web site that can help you reach all of ICAO's Contracting States. Major industry experts in the MRTD, Border Control, Security and Facilitation field use our Web site to deliver their corporate message to key players in the MRTD community worldwide.

For more information on our comprehensive media package and marketing tools, visit us at:

**www.icao.int/mrtdc**


## 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.