MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Unified vision

Attendees to the Fifth Symposium and Exhibition of ICAO MRTDs, Biometrics and Security Standards support ICAO's Vision 2020 objective for more cooperative, effective and State-centric progress.

Vol. 5, No. 1

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

GET. THE PERFECT FIT

For over twenty years, GET Group has been trusted by governments around the world to deliver state-of-the-art high security Passport and ID solutions. Contact us to find out how our technologies can help manage your Passport and ID security risks. Our solutions include:

TOPPAN ePASSPORT P600
The New Passport Printer

TOPPAN CP400
Card Printer

ePIS
Electronic Passport Issuing Solution

eBCS
Electronic Border Control Solution

eNID
Electronic National Identification Solution

GET. Into the future

ICAO MRTD REPORT
VOLUME 5, NUMBER 1, 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: +01 (514) 886-7746
E-mail: info@philbin.ca
Web Site: www.philbin.ca

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

Advertising
Keith Miller, Advertising Representative
Tel: +01 (514) 954 8219, ext. 6293
Fax: +01 (514) 954 6769
E-mail: kmiller@icao.int

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

www.icao.int

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

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

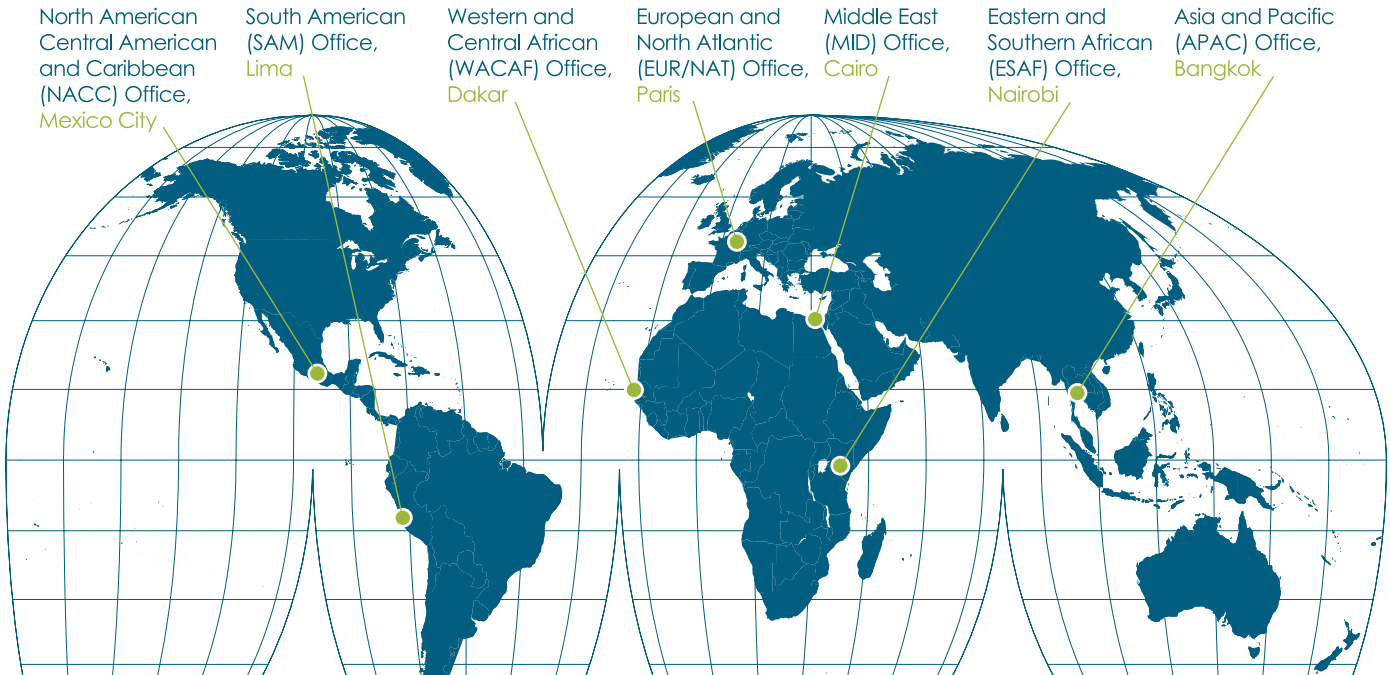
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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

Observer organizations

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

ICAO's Global Presence



Toward 2020: A more integrated approach to security and facilitation

The failed terror plot of December 25, 2009, highlighted two key realities: the trans-border nature of the threat and the urgent need for a comprehensive, intelligence-led security approach that would integrate current AVSEC screening policies and practices with border security—based on real-time information sharing and inter-agency cooperation.

Effective national and international security requires a comprehensive system built on global harmonization, efficient technology, effective information exchange, industry-government cooperation, competent risk assessment, and taking effective action. This plot, while regrettable in a number of ways, has placed renewed focus on the need for the political will necessary to redefine aviation security and to effectively integrate it with border control, intelligence, law enforcement and other related areas.

ICAO and its AVSEC, Facilitation and MRTD Programmes are well placed to integrate and lead this opportunity and the evolving security agenda. This issue includes an article by Dominique Antonini (Director of the Geneva-based AVS&C security consultancy and former Chief of the ICAO Aviation Security and Facilitation Policy Section) in which he addresses this matter and the fundamental role played by the MRTD Programme and the use of biometrics in developing a comprehensive and integrated security vision.

2010 will be a year of reforms and of intensifying global cooperation on data sharing in order to meet current and future security needs. The focus has increasingly been shifting to combining latest technologies, intelligence and human skills for proactively identifying and detecting dangerous individuals—instead of simply deploying more technology to detect prohibited items at airports, where it probably will be too late….

Addressing many of these concerns and their possible solutions, the goal of last September's Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards was to anticipate the next decade of challenges and identify State needs and expectations concerning the future of travel documents and border control security. We've labeled this initiative "Vision 2020", and I must express my sincere thanks to the many speakers who contributed with their excellent presentations.

There were many significant issues raised at this landmark event. As Barry Kefauver elaborated in his closing remarks, we are without doubt going to encounter more areas of risk in the coming years. First and foremost we need to prepare ourselves to be able to confront these risks and maximize our abilities to deal with them. Barry emphasized that: *"The stakes have never been higher"* in this regard and I, among many who were present, whole-heartedly agreed.

I'm also very grateful to ICAO's Air Transport Bureau Director, Folasade Odutola, who underscored the pivotal role that ICAO must play in all of the areas of focus that surfaced throughout the Symposium. From capacity-building to technology definition, ICAO is the only global Organization which can serve as the meeting ground and standard-setter for harmonized, effective State MRTD and e-MRTD developments and programmes.

Without a doubt, the 2009 event was one of the most successful ICAO has thus far had the privilege to host. All in attendance underscored the urgency of the challenges that were presented to us and each emphasized that ICAO has a unique and pivotal role to play in continuing to provide the global leadership that will manage future progress and facilitate more effective partnerships between all stakeholders.

After the events of last December it is clear once again that aviation remains a target for terrorists and that the stakes, indeed, have never been higher for those of us seeking passenger- and industry-friendly solutions to present and future security and facilitation related challenges. Many of the articles in this issue point to the directions where we need to focus our attention and efforts in the important months and years ahead.

Happy reading.

Mauricio Siciliano
Editor ■

ICAO Council President Roberto Kobeh González (right) addresses the Fifth ICAO Symposium on MRTDs, Biometrics and Security Standards. ICAO Air Transport Bureau Director, Folasade Odutola (left) Chairs the proceedings.

Creating a more collaborative future

Over the past two decades, ICAO has benefitted from the intelligence and commitment of hundreds of contributing bodies and individuals in coordinating the complex mix of research, debate and ultimately solutions that have shaped the evolution of MRTDs.

In his opening address to the 2009 Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards, repeated here for the benefit of ICAO's *MRTD Report* readership, ICAO Council President Roberto Kobeh González notes how this collaborative approach has made it possible for ICAO to establish and adopt standards and technical specifications that have helped form a seamless network of procedures on all continents.

Good morning ladies and gentlemen.

It is a pleasure for me to welcome so many senior government officials and industry representatives to our Fifth MRTD Symposium. Mr. Raymond Benjamin, our new Secretary General and I are highly appreciative of the support and contribution of the stakeholders you represent in the global effort to promote the development and harmonized implementation of MRTDs around the world.

Mr. Benjamin is a recognized expert in matters of aviation security and would have very much enjoyed sharing with you our most recent initiative aimed at ensuring that ICAO truly meets the needs of its Member States in the area of MRTDs —an essential component of aviation security. Unfortunately he had to fly to New York at the last minute for a high-level meeting with the Secretary General of the UN, Mr. Ban Ki-moon, on another global challenge par excellence— climate change.

The world of aviation is certainly not short of challenges!

As I mentioned a moment ago, ICAO is launching something new this year—an undertaking we call ICAO's MRTD Vision 2020. Vision 2020 is above all a consultative process designed to gather and analyze the needs and wishes of Member States in relation to travel document and border control in the future. We want to be able to adequately

THE SITUATION MAY CHANGE. SECURITY DOESN'T.

WITH ADAPTABLE VISOCORE® BORDER SOFTWARE.

BUNDESDRUCKEREI
We are family

Whatever the point of entry: airport, seaport or on land – the security situation may change. You are always braced to meet this challenge with Bundesdruckerei's VISOCORE® Border solution. VISOCORE® Border is extremely flexible thanks to its modular structure. Its cutting-edge technology supports and enables effective border control management. With VISOCORE® Border's innovative technology, you are equipped to curb and control any potential threat.

VISOCORE® BORDER – SAFE AND EFFICIENT BORDER CONTROL MANAGEMENT

Advantages

- Faster throughput times thanks to intelligent passenger flow control
- Greater control density by complete screening of all travellers
- Database-supported information to assist border control officials
- Better focus on high-risk groups
- Highly reliable and scalable back-end system

Applications

- Border controls at airports, seaports and on land

Contact:

Bundesdruckerei GmbH
Oranienstrasse 91 • D-10969 Berlin
Tel +49 (0) 30 - 25 98 0
Fax +49 (0) 30 - 25 98 22 05
www.bundesdruckerei.de

respond to them by putting into place, by the year 2020, the necessary policies, standards and related instruments. With your help, we want to begin the process at this year's Symposium. As Peter Drucker, the pre-eminent management expert once said:

> *"The best way to predict the future is to create it".*

This is what this symposium is all about—a dynamic forum for presenting and generating ideas and concepts that will shape the future of document control as it applies to aviation security and the efficient movement of passengers through airports. It was conceived in response to questions and concerns of States in meeting the 2010 deadline for the issuance of Machine Readable Passports. It quickly extended to the application of the impact of new technologies and high-profile issues such as the protection and prevention of identity fraud.

Seeing more clearly what the economic, social and political world of tomorrow will be helps us to better focus our resources and energies in anticipating the systems and procedures that will be needed to keep the global air transport system operating in a secure and efficient manner. This is the essence of the Vision 2020 MRTD mission.

I am particularly pleased that the Secretary General of INTERPOL, Mr. Ronald Noble, was able to take time out of his extremely busy schedule to speak to us today. Earlier this morning, I had the pleasure of reviewing with him some of the major issues confronting both our organizations and I want to personally thank him for the role played by INTERPOL over the years in supporting international cooperation in the field of identity management and travel document security.

This collaborative effort reflects the fact that the ICAO MRTD Programme, although developed in the frame of civil aviation matters, has an impact that goes far beyond aviation security. It also substantially contributes to establishing and implementing national and international security policies and is instrumental in combating terrorism and trans-border crimes.

In fact, the UN Security Council Resolution 1373, among other issues, mandates States to implement ICAO MRTD Standards and specifications to achieve secure and integral issuance of travel documents, and to avoid document and identity fraud at borders.

Also on the agenda are highly respected influencers in their particular fields of expertise that will help shape the future. This includes the technological, political and economic dimensions of MRTD programmes. All of these points of views will serve as the building blocks of a security and facilitation environment that will provide ease of travel for passengers and more cost-effective operations for industry.

It will also make ICAO's job much easier and more productive. Over the past two decades especially, the Organization has benefitted from the intelligence and commitment of hundreds of contributing bodies and individuals in coordinating the complex mix of research, debate and ultimately solutions that have shaped the evolution of MRTDs. This in turn has made it possible for us to establish and adopt Standards and technical specifications that have been incorporated by States into their national legislations in a seamless network of procedures across all continents.

Such is the power of global cooperation. From INTERPOL to the International Standards Organization (ISO), the International Organization for Migration (IOM), the UN Counter-Terrorism Executive Directorate, the Inter-American Committee Against Terrorism of the Organization of American States, the Organization of Security and Co-operation in Europe and ICAO Member States. And, of course, all of you in this room as we embark on another phase of our journey with Vision 2020.

In closing, I also wish to thank the record number of exhibitors who will showcase the products and services that can expedite the handling of international passengers by all modes of transportation—whether road, rail sea and air—through security, customs, immigration and other control points. We encourage you to take advantage of this one-stop consultation environment to familiarize yourselves with the tools you and your organizations may need to ensure the successful implementation of MRTD systems and procedures in your respective States. They too can feed the Vision 2020 process.

I wish you all a very stimulating and engaging Symposium. ■

"Seeing more clearly what the economic, social and political world of tomorrow will be helps us to better focus our resources and energies in anticipating the systems and procedures that will be needed to keep the global air transport system operating in a secure and efficient manner. This is the essence of the Vision 2020 MRTD mission."

secunet GRT platinum edition

GOLD GOES PLATINUM

New edition of Golden Reader Tool now available

Better than gold – secunet presents the new platinum version of the well-proven Golden Reader Tool. This new extended version is totally flexible, modular and innovative. The new approach allows the usage of biometrics as well as further electronic documents beside epassports. This makes it the best guarantee for protecting identities in times of globalisation where eID-documents are becoming increasingly important and widespread.

For more details see:

www.secunet.com/GRTplatinum

Key benefits of the new platinum edition:

- Commercially available
- Supports biometrics via BioAPI/biomiddle
- Supports all EAC versions
- Flexible in terms of features, design and use cases
- Internationally recognised as the reference implementation

The Golden Reader Tool is a joint project of the Federal Office for Information Security and secunet

The future: A vision

The following is a segment of the concluding remarks as delivered by Barry Kefauver to the attendees and participants to the 2009 Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards.

This coming year will see the work begin on the issuance of the next ICAO Request for Information (RFI), the medium through which the travel document community as a whole can communicate with industry, spell out what needs to be done and seek the technologies to carry out its objectives. Kefauver notes here how an ICAO 2020 Steering Body must be formed and activated in the near-term in order to conceptualize and document those directions for the coming decade.

In my view, we are now poised on a very delicate and important point in the history of travel document standards, issuance and inspection. Recall that Jim Wayman observed that ICAO took a risk, but it paid off. I think we are going to encounter yet more areas of risk in the coming years. We need to prepare ourselves to be able to confront these risks and maximize our abilities to deal with them. The stakes have never been higher.

Throughout the Symposium I have tried to be attentive to threads and themes of continuity that might help shape a portion of what the future holds and give us something of an edge in dealing with the unknowns. The first two of these are directly and inherently related:

1. ICAO is the fulcrum around which the implementation of travel document and border security programmes revolves.
2. We must enhance and consolidate the foundations of the partnerships that are needed now, more than ever, to be able to meet the global challenges.

"The time is now to develop that vision of the future and to be able to clearly articulate those long-term needs and the kinds of government policy objectives that need to be served by industry."

The demands on resources, both financial as well as human, have increased dramatically over the past few years. Much of the role of the ICAO Implementation and Capacity Building Working Group (ICBWG) is intertwined with the ability to deliver assistance to those countries that need it most, which are frequently those same countries that we are most concerned about in terms of enhancing their travel document programmes from multifaceted foreign policy perspectives. The *Annex 9* and other related provisions acceded to by all 192 ICAO Member States clearly point to ICAO as the center of the travel document universe.

You have heard from several of the critical, multilateral organizations who share in this worldwide partnership and responsibility—the Organization for Security and Co-operation in Europe (OSCE); the International Organization for Migration (IOM); Interpol; the Organization of American States (OAS); the United Nations Counter-Terrorism Committee Executive Directorate (UN CTED); the International Centre for Migration Policy Development (ICMPD); and the International Standards Organization (ISO)—and there are a number of others who have not made presentations at this Symposium but who share intimately with ICAO the goals and objectives of the coming decade.

As always, these activities will focus broadly on technologies. However, more than ever before, these partnerships will revolve around policy directions, the determinations of what the world's governments need from travel document functionality and from that the kinds of technologies that will best turn those goals into realities. The magnitude of the challenges and the breadth of expertise required make these partnerships perhaps the single most important foundation of the coming decade.

Also, as I noted earlier, there is work being focused on the systems aspects of the issuance and inspection processes. With the leaps forward in document enhancement, the paths of least resistance now for bad people to travel with false identities for insalubrious purposes is through the porosities found in ANY issuance programme. ICAO and its partnership community is now seized with seeking ways to shore up these threats and vulnerabilities in a concerted worldwide manner. These initiatives will go far beyond the documents themselves and into the heart of the ways in which applicants and travelers must demonstrate their bona fides. Once again, you have heard several of our speakers call for this; we have heard their call and the work is now underway.

This coming year will see the work begin for the issuance of the next ICAO Request for Information (RFI). The first RFI in 1995 specifically sought biometrics and data carrying media and resulted directly in facial recognition and contactless chips. This was a result of governments collaborating and deciding that the global priorities were to be focused on biometrics and the kinds of ways in which that data could be carried in travel documents.

It is now time to develop that vision of the future and to be able to clearly articulate those long-term needs and government policy objectives that need to be served by industry. That must be the first step to a meaningful RFI: to lay out clearly to industry what governments need and THEN for the private sector to respond with pre-existing technologies or, perhaps, to launch R&D processes to develop technologies that do not currently exist.

It is here that an ICAO 2020 Steering Body must be formed and activated in order to broadly and deeply conceptualize and document those directions for the coming decade. I submit that the time for that is now.

We have great travel document challenges ahead. As well, we have a greater and more cohesive critical mass than we have ever had before to meet those challenges. I thank all of you for your time and attention throughout the Symposium and I look forward to the next steps of our future travel document generation. So as far as sound bites are concerned I will leave you with only one:

Onward. ■

The role of INTERPOL in travel document security

The following is an abridged review of the September 2009 presentation by INTERPOL Secretary General Ronald K. Noble, as delivered to the Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards.

Through several interesting case studies, Noble highlights here the critical importance of Machine-Readable Travel Documents (MRTDs) to global and national border enforcement strategies, the cost-effectiveness of implementing MRTD and e-MRTD solutions, and the vital roles played by his organization and ICAO in this area over the last decade.

Ronald K. Noble was elected Secretary General by the 69th INTERPOL General Assembly in 2000 and unanimously re-elected to a second five-year term in 2005. He is also a tenured Professor of Law at the New York University School of Law, on leave while serving as INTERPOL's Secretary General. He previously served as the Undersecretary for Enforcement in the United States Department of the Treasury, overseeing the U.S. Secret Service, Bureau of Alcohol, Tobacco and Firearms, Federal Law Enforcement Training Centre, Office of Foreign Assets Control and the Financial Crimes Enforcement Network. He is a former Assistant U.S. Attorney and Deputy Assistant Attorney General in the U.S. Department of Justice.

It's a great pleasure for me to be back in Montreal today. This city has lured people from all over the world throughout its rich history and is still defined today by global mobility. Montreal's airport welcomes a higher percentage of international arrivals than any other airport in Canada. Not too far into the future, one out of every four of this city's residents will have been born in another country. It's fitting, therefore, that we have come to Montreal to discuss the best ways to facilitate the movement of people and goods that drives today's global economy, while effectively restricting the mobility of those few who may wish us harm.

The year 2009 marked the 10th anniversary of the signing of the Memorandum of Understanding between INTERPOL and ICAO, yet this partnership is more vital today than ever before. The 9/11 attacks that followed shortly after this MOU was signed opened the world's eyes even further to the critical security importance of travel documents.

To those seeking to commit horrific acts of violence and terrorism and to those of us working to stop them, there has certainly been a tremendous amount of progress since the 9/11 attacks in making our documents more secure and our systems more foolproof. But we are still nowhere near where we should be.

Confirming the security role of travel documents

In many countries today, a passenger's water bottle usually undergoes more thorough and rigorous screening at an airport than a passenger's passport does. In my capacity as Secretary General of INTERPOL, I invariably seize every opportunity to engage leaders and decision-makers about this specific issue—highlighting the facts that ensuring travel document security will have the greatest positive consequences for the overall security of our borders and our communities and that the upgrades required to improve document security are generally quite simple and inexpensive to implement.

"Ensuring travel document security will have the greatest positive consequences for the overall security of our borders and our communities, and the upgrades required to improve document security are generally quite simple and inexpensive to implement."

To illustrate this point, let me begin by discussing a specific crime trend INTERPOL has been monitoring.

While the evidence suggests that individuals who are caught in smuggling networks are generally traveling to seek asylum or a better way of life, the networks themselves and the loopholes they employ are often used by other criminal elements or terrorist organizations for a variety of illicit purposes.

In January 2007, 11 individuals were stopped at the airport in Monterrey, Mexico, after a vigilant border officer became suspicious of their reasons for visiting the country. Eight of the individuals were traveling on Cypriot passports and two on Polish passports, while one infant was traveling on her mother's passport. Checks against INTERPOL's database of stolen and lost travel documents revealed that the eight Cypriot passports were part of a lot of 850 passports that had been stolen as blanks in April 2003 from a government office in Nicosia, Cyprus. They were recorded by law enforcement into INTERPOL's database that same day.

Can you believe that criminals would be so brazen as to use passports stolen four years earlier to cross borders internationally? Compare this to the value-window for stolen credit cards, which usually need to be used within hours or minutes of their theft in order for them to have any value. We must learn from these examples before, not after, terrorists and other transnational criminals exploit these global security

Ronald Noble discusses new developments with an exhibit representative from Sagem Identification during ICAO's Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards.

gaps, and ICAO, in conjunction with the States and private-sector entities with us at this Symposium, can help us to do so.

To return to this specific case for a moment, the two Polish passports under scrutiny were not registered in the INTERPOL database, but the photos shown on them had clearly been substituted. It was later determined that these two passports had probably been sold by the legitimate bearers. Had ICAO's Standards been followed when the documents were produced, that photo substitution should never have been able to occur.

Our investigation of this case eventually revealed that the 11 individuals were in fact Iraqis who were attempting to travel to Tijuana, Mexico, and then cross into the United States illegally—most likely to claim asylum. Follow-up investigations of this network continue and, in addition to several arrests made around the world, we discovered that a number of individuals involved had sold their own passports for profit, making our work that much more difficult.

I'd like to discuss another case to highlight a weakness—let me stress that: a weakness—in the way that governments handle criminals who try to cross borders using fraudulent travel documents. In this case, INTERPOL found that, in a two-month period, an Iraqi national had been stopped on three separate occasions carrying three forged passports from three different European countries. On the third occasion, he, along with two other men, had made it successfully to Costa Rica and even passed through Costa Rican border control and caught another flight to Guatemala.

Guatemalan border officials, working closely with INTERPOL National Central Bureaus and our 24/7 Command and Coordination Centre at INTERPOL General Secretariat Headquarters in Lyon, France, determined that the three individuals were carrying fraudulent passports *(see Figure 1, page 14)*. They were sent back to Costa Rica, where they were arrested. Analysis of their passports showed that one of the two other men had also been stopped in Madrid in May 2008. The three individuals were interrogated by Costa Rican authorities and it was concluded that they, too, were Iraqis intending to travel to the United States.

In the end, this case would be traced back to the same smuggling network that facilitated the illegal travel of the 11 Iraqis described in the first example —a network which appears to be led by two men who are of Middle Eastern origin but who hold European Union passports. This helped them cross borders more easily to facilitate the smuggling.

The risk we expose ourselves to by not taking this crime seriously and by not consulting INTERPOL's database systematically worldwide—like we check the carry-on luggage of travelers—is that determined terrorists and other transnational criminals will reach their target countries and strike us. One focus of this ICAO Symposium is specifically how the implementation of machine-readable travel documents can much more effectively stem this flow of illegal international migration.

As we can see from the examples I've just illustrated, machine-readable passports provide an extremely effective means of protecting our borders and thus our citizens from terrorists and other transnational criminal groups. As you heard, these sample cases involved numerous fraudulent passports and journeys of thousands of miles through several countries on three different continents—and this is where INTERPOL is vital. By connecting police, border control and law enforcement specialists around the globe, INTERPOL helps to secure the world and individual countries. It can provide the support and connect the dots that help to ignite a global investigation, all based on the identification of one fraudulent travel document and the important investigative follow-up by police forces in our member countries.

Four pillars of INTERPOL border control assistance

Pillar 1—Technical support and 'MIND/FIND'

I'd now like to outline four key areas where INTERPOL specifically complements and reinforces these efforts. The first pillar of INTERPOL's activity is technical support.

By 'technical support' I'm referring to the tools and services we've created with the express purpose of providing the data that best assists law enforcement in our member countries. It also refers to the mechanisms that allow us to get this data to the greatest number of officers in the greatest number of locations.

By now I'm sure you're familiar with INTERPOL's database of stolen and lost travel documents, which has been endorsed by the ICAO Technical Advisory Group (TAG/MRTD) and a host of other international bodies. Created following the 9/11 attacks, the database contains almost 20 million records—including more than 11 million passports—contributed by 147 countries. Please think for a moment about these statistics, as they represent no small degree of tribute to the work of ICAO, our law enforcement colleagues and the private sector, all of whose creativity and ingenuity make our efforts so much more effective.

Annual checks of passports by law enforcement worldwide against what is currently the only database of stolen and lost passports have grown from a mere 145 in 2002 to more than 300 million this year. Let me stress that again: from fewer than 200 to more than 300 million in less than a decade. This is nothing short of phenomenal.

Using the INTERPOL database, passport officers have identified more than 28,000 documents to date as having been reported as lost or stolen. Also noteworthy is that, while these 28,000 passengers were being more closely scrutinized, the remaining 200 million or so international travelers who crossed borders during this period were allowed to do so without incident or delay.

INTERPOL has also set up a network of contact points in our member countries that are available around the clock to verify 'hit alarms'. Obtaining a document holder's identification details as quickly as possible is essential when control officers at border entry points have minutes or even seconds to determine their next course of action after receiving a hit. As we saw in the Iraqi examples, it was human intervention, not technology alone, which ultimately exposed the full extent of the crimes taking place.

"Machine-readable passports provide an extremely effective means of protecting our borders and thus our citizens from terrorists and other transnational criminal groups."

Besides initial access to this and our other global police databases in our National Central Bureaus located in every member country, 56 of our member countries have expanded access to INTERPOL data using our innovative MIND/FIND technology—with many more countries in various stages of implementation. In participating MIND/FIND countries, the information in the databases does not simply reside in an office; it is out there in the hands of officers at airports, seaports, border control units and other critical locations, providing one more key operational and investigative resource.

Here in Canada that means more than 66,000 officers from over 380 law enforcement agencies across the country have daily access to INTERPOL's databases. In its first two months of operating MIND/FIND, Canada recorded 200 hits—including a Nigerian national with a prior criminal record who was arrested trying to cross the border from the U.S. on a Spanish passport that had been reported stolen by INTERPOL's National Central Bureau in Madrid.

We've seen tremendous uptake in our member countries in implementing MIND/FIND, but there are still far too few countries that conduct systematic checks of travel documents of all incoming passengers. This relates back to what I was saying earlier about the need for simple, cost-effective solutions with the greatest potential benefit to our security.

Pillar 2—Operational support

The provision of operational support for police forces in countries that lack specific resources and/or expertise is increasingly taking up a greater proportion of INTERPOL's core activities. One noteworthy recent example was Operation Anaconda, which involved the installation of INTERPOL's MIND/FIND system at the international airport in Lima, Peru.

Conducted in October 2008, Operation Anaconda led to the training of hundreds of police and immigration officers in fraud detection and other investigative techniques used to capture smugglers. The INTERPOL stolen and lost travel documents database was integrated into Peru's national system to enable simultaneous checks and instant responses. Standard operating procedures were also established for handling hit alarms quickly and effectively.

Based on the success of Operation Anaconda, INTERPOL now has a similar operation taking place in El Salvador and others are currently planned for the Philippines and Germany.

In a more recent example, last autumn a team of INTERPOL experts was sent to Liberia to assist authorities with a smuggling investigation. The investigation related to a trend detected by airline staff which involved Pakistanis flying from Liberia to Brussels without passports, intending to claim asylum upon arrival.

Two Pakistani men had been stopped just as they were about to get on an airplane. They did not have their passports in their possession at the time. Checks by INTERPOL's National Central Bureau in Monrovia, Liberia, of the stolen and lost travel documents database revealed that the names and passport numbers that appeared on the

FIGURE 1: INTERPOL'S GLOBAL REACH

During a two-month period a single Iraqi national was stopped on three separate occasions carrying three forged passports from three different European countries. On the third occasion, he and two other men made it successfully to Costa Rica and even passed through Costa Rican border control and caught another flight to Guatemala where local officials, in collaboration with INTERPOL, detected them and sent them back to Costa Rica where they were arrested. The case was eventually traced back to a smuggling network.

Stolen Greek passport registered in SLTD DB

Stolen UK passport registered in SLTD DB

Former Yugoslav passport not registered in SLTD DB

mens' boarding passes matched those of two passports reported as stolen by the US. The two men led authorities to a house with other Pakistanis, including three who also hoped to travel to Europe and a known smuggler.

I am sure many of you are wondering how two men were able to board an airplane and almost leave a country without proper travel documents. Investigators suspect that possible corruption involving officials and airport employees may have enabled the men to get that far without detection.

Pillar 3—Capacity-building and training

Beyond the practical tools which INTERPOL offers its member countries, it also understands its critical role in enhancing the capabilities of law enforcement in all countries to respond to border and other security challenges.

A clear problem area identified by INTERPOL and ICAO in this regard is that certain countries still do not use or issue machine-readable passports in compliance with ICAO Standards. Unfortunately, these States also don't seem likely to have this capability in place in time for ICAO's April 1 2010 deadline.

Through INTERPOL's OASIS program, which provides operational training, services and infrastructure support to police officers in Africa, three sets of equipment, including MRTD readers, have now been deployed to several countries in Africa, with many more countries in the pipeline.

Pillar 4—Improved cooperation with international bodies and the private sector

Just as no single country can accomplish effective border security on its own, I believe that no one organization can either.

I've already mentioned the common vision and the long-standing cooperation between INTERPOL and ICAO, for which we thank ICAO very much. INTERPOL is an active partner in all of ICAO's expert working groups and capacity-building activities related to travel documents and border security. In particular, INTERPOL participates in the ICAO New Technologies Working Group (NTWG), which brings together experts from government, law enforcement and the private sector and which is responsible for setting standards for MRTDs, biometrics and e-Passports.

INTERPOL is also a member of the recently created ICAO Implementation and Capacity-Building Working Group (ICBWG), whose aim is to provide real-time support in the field. Currently, the ICBWG is focusing on the development of specially-designed workshops to share knowledge and exchange good practices.

Conclusion: The new 'INTERPOL e-Passport'

As the nature of crime and security threats evolves, so, too, do our needs in terms of travel documents, biometrics and other areas. At INTERPOL, this means we will continue to further enhance the initiatives already described here and that we will always be on the lookout for new opportunities for development.

In 2010, INTERPOL will be launching in earnest a unique 'INTERPOL e-Passport' to make it easier for the heads of our National Central Bureaus in our member countries to travel freely and better assist in the apprehension and transport of fugitives. The INTERPOL e-Passport will also facilitate the movement of INTERPOL staff and members of our Executive Committee in the function of their official duties internationally.

For far too long it has been a great source of frustration that some of our officials have more difficulty crossing borders than the criminals we are pursuing. This is particularly true for our member countries in Central and South America as well as Africa and Asia—which is to say the vast majority of our member countries. Therefore, following an industry-wide call for interest, INTERPOL selected a consortium led by EDAPS to design and develop the first-ever INTERPOL e-Passport.

At this stage we are developing the INTERPOL e-Passport as an identity document that will serve to highlight state-of-the-art security features for travel documents and encourage INTERPOL's member countries to adopt similar levels of security. This is especially important since the use of fraudulent passports by terrorists poses the number one threat to the safety of citizens everywhere. Let me also highlight that, befitting that an organization with 188 countries, this undertaking is a truly international effort—bringing together 20 leading suppliers from 12 countries. It will, of course, duly comply with all relevant ICAO Standards.

I have spent some time today discussing in detail how far INTERPOL has come during the 10 years that we have more closely aligned ourselves with ICAO, but this is really still just the beginning. Let me close now by saying that this ICAO Symposium is a great sign of the progress we have made in our ongoing collective efforts to enhance the security of our travel documents and strengthen the security of our borders. It represents a unique international mechanism which gives us the chance to significantly benefit from the critical mass of expertise gathered in this room and engage one-on-one with our colleagues in this field.

I encourage all of you to take advantage of the tremendous opportunity represented by this ICAO MRTD Symposium and thank you for your kind attention. ■

About INTERPOL

Headquartered in Lyon, France, INTERPOL is the world's largest international police organization with 188 member countries.

Created in 1923, INTERPOL facilitates cross-border police co-operation and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. INTERPOL aims to facilitate international police cooperation even where diplomatic relations do not exist between particular countries.

Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights.

INTERPOL's constitution prohibits any intervention or activities of a political, military, religious or racial character.

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

In this first part of the second of his three articles on implementing e-MRTDs, Markus Hartmann of HJP Consulting GmbH focuses on the execution of a professional procurement process—one that allows for the transfer of technical and commercial requirements into a professional legal agreement that will keep respective State authorities in full control, during the implementation of their e-MRTD project and beyond. The legal aspects involved have been detailed here with the assistance of article co-author Chris Coulter, of the law firm Morrision & Foerster.

Procurement and Implementation Part II-B will be included in the second *MRTD Report* issue of 2010, with the last instalment in this very useful and practical series appearing in our third and final 2010 edition, later this fall.

Procurement processes related to e-MRTD issuing systems can be a source of significant frustration for both buyers and sellers. Bid managers in the e-MRTD industry have to work through invitations to tender which can often read like *The Thousand and One Nights* fairy tales and have little reference to the buyer's actual requirements. Technical experts in the bid team practically end up needing to act as qualified clairvoyants, designing solutions suitable for unspecified requirements and scalable to uncertain quantities. The bid team's lawyer meanwhile may find him or herself challenged by hundreds of pages of General Terms and Conditions attached to the invitation to tender which are rarely tailored to the specific character of a complex IT infrastructure for issuing e-MRTDs.

And the industry knows how to fight back under these circumstances. They generally produce colossal tender documents containing thousands of pages nicely wrapped in silver binders and placed into sealed aluminium boxes.

On average about 15 such proposals from international and national security printers or IT system integrators can be expected during the bid process for an e-MRTD project.

The receiving issuing authority's technical committee therefore finds itself faced with 20,000 or more pages to be worked through, however the real challenge still lies in comparing the different bids—often an exercise of comparing apples and oranges. In addition, the decision makers are pestered by the different lobbying troops trying to influence the process in their favour.

In the end, the respective authority's decision makers often see only one way out of the labyrinth—namely cancelling and re-issuing the invitation to tender. HJP has been witness to several States' e-MRTD projects being afflicted by these same mistakes as they're repeated again and again in what eventually becomes a vicious circle that stagnates any attempt at moving forward.

The authors of this article have advised both issuing authorities and industry in order to help them design and benefit from a more professional procurement process. For us it is of key importance that buyers incorporate their multiple technical and commercial requirements into a proper legal framework.

Because they often have very little expertise in this area, only a professional procurement contract will give issuing authorities the control they need over complex IT projects of this nature. The following article highlights the different steps that need to be taken procuring and implementing an e-MRTD issuing system—however the steps we'll demonstrate are also applicable to any other complex, security-sensitive IT project.

Procurement

In the first article in this series (*MRTD Report* Vol.4 No.3, autumn 2009) we covered the basic and preliminary steps in getting an effective e-MRTD issuing system implementation project off the ground. In a nutshell, we described how to produce a comprehensive scope statement for a project covering all the requirements with respect to the technical system architecture, protection needs and project management components. This scope statement describes in great detail what the issuing authority expects from the future e-MRTD issuing system.

Finally we described how to break down a complete solution into manageable work packages and deliverables—a process leading to the creation of what we termed the "Work-Breakdown-Structure (WBS)".

The scope statement mentioned above establishes the necessary foundation for the procurement process, although it is only one side of the coin. Issuing authorities also need to develop an adequate budget, a realistic schedule, and a plan for coping with potential risks during the implementation and operational phases of the project.

Strategic procurement and planning

Having a technical solution in mind, issuing authorities should develop their budget and a rough timeline. The Work-Breakdown-Structure only references what has to be done in order to implement and operate an e-MRTD system. The first question that arises is: who should perform the various tasks? It is essential that the issuing authority has a clear idea regarding how extensively it wants to get involved in the project in order to stay in full control of the e-MRTD issuance system.

Once this question has been answered, the issuing authority can decide if they want to look for a prime contractor and tender for a turn-key solution, or to source suppliers for different parts of the solution and assume the project management tasks themselves. In the later case, the issuing authority may become a system integrator or implement parts of the solution with internal staff. In order to achieve this strategic direction, the issuing authority may have to consider the following:

- Are there any strategic government policies that it has to follow (e.g. national security, e-government strategies)?
- Are there any security sensitive areas which need to stay with the authority, such as the Country Signing Certificate Authority (CSCA)?
- How is the project financed? Is the budget for initial investments and operations covered or should other financing models such as Buy-Operate-Transfer (BOT) approaches be considered?
- How will the risk of failure be accounted for? How can an authority ensure continuity of supply even if the supplier fails deploying the project successfully or possibly discontinues the business due to reasons such as embargos, changes of strategy, security concerns, etc.
- Which components of the e-MRTD system does the authority want to develop and/or operate on its own?
- Which components of the e-MRTD system can the authority purchase and/or operate?
- What know-how and what resources does the authority need internally?

Based on the answers to these queries, the issuing authority can derive an operator model that is most appropriate to its situation and resources. If this strategic direction is clear, the operational procurement processes can be planned and the authority can decide on making vs. buying. The make-or-buy decision is essential for the design of the relevant procurement contract.

Procurement guidelines

The procurement of e-MRTD issuing systems falls under both national and supra-national procurement law regulations. Each state has its own rules and regulations to follow in this respect. As e-MRTD projects will attract many international bidders, it is recommended to follow internationally acknowledged procurement guidelines. The most common are issued by the World Bank and the European Union:

- World Bank: *Procurement Guidelines Under IBRD Loans and IDA Credits*
- European Commission: *Guide to the Community Rules on Public Supply Contracts*

In the event that the e-MRTD project is financed by third party donor states or organized by international organizations, such as the OSCE or IOM, etc., specific procurement guidelines are mandatory. Local national procurement regulations will also invariably apply.

Notwithstanding the existence of these guidelines, the key to a successful procurement process is finding the right balance between transparency-enabling competition and the feasibility of managing the process. The issuing authority should select with care the method of procurement which fits the specific needs of its particular e-MRTD project. The Limited International Bidding methodology, structured into a pre-qualifying RFI and a detailed RFP process, has proven to be the most suitable process under many circumstances.

Notwithstanding all rules and procedures, the biggest challenge for all stakeholders is following the rules in order to benefit from the competitive bidding and not to fall into any unfair practises.

Developing market expertise

Prior to issuing an RFP, it is essential for the issuing authorities to gain a rough understanding of the availability, over all pricing and delivery schedules of the required solution.

An initial understanding of what the market is offering can be obtained from relevant publications, exhibitions and conferences, such as the yearly ICAO MRTD Symposium in Montreal.

Comprehensive information about the e-MRTD market space and respective suppliers is also provided on the ICAO MRTD Community Web site at: *www2.icao.int/en/MRTD2*.

Other publications and events are listed in Figure 1, *(right)*.

States will often look for an independent and unbiased consultant who can accompany them throughout their e-MRTD project. The ICAO Implementation and Capacity Building Working Group (ICBWG) has been established by the ICAO TAG/MRTD to support States in these instances. The group operates a database of recommended consultants from government and the private sector and its chair can be contacted by e-mail via: *icbwg@icao.int*

An alternative procurement and project management service is offered by the ICAO Technical Co-operation Bureau (TCB). They have a dedicated staff that monitors project implementations on behalf of Contracting States from start to finish and from both the technical and financial perspectives. ICAO TCB has been doing this very successfully for aviation related projects for many decades now and they are currently extending their services into the e-MRTD sector.

Regardless of how the issuing authority wants to proceed, they should always deal either via an unbiased consultant or at the least engage with multiple vendors. Never deal with one vendor only, regardless of how generous and free of charge their services may appear. The big bill always comes at the end.

Face it: It is all about money

Budgeting of e-MRTD projects appears to be a real challenge. Prices of new booklets with contactless chips are multiple times more expensive than

Figure 1: e-MRTD Market Research Sources

ICAO MRTD Symposium, Montreal, Canada *www.icao.int/MRTDsymposium*
CARTES exhibition, Paris, France *www.cartes.com*
ID World International Congress, Milan, Italy *www.idworldonline.com*
Asia Pasific Smart Card Association *www.apsca.org*
INTERGRAF *www.intergraf.eu*
Security Document World, Website and Congress *www.securitydocumentworld.com*
ICAO e-MRTD Community Website *www2.icao.int/en/MRTD2*

Figure 2: List of RFI/RFP documents

Request for Information (RFI)	Request for Proposal (RFP)
Section A	**Section A**
Transmittal letter	Transmittal letter
Consortium's Letter of Intent (LOI)	Consortium's contract, signed by all parties
Company details	Draft contract
Certificate of Incorporation (COI)	Bank guarantee
Audited profit and loss statement from the last three years	Checklist of submitted documents
Letter concerning corrupt or fraudulent practices	
Letter concerning insolvency	
Letter concerning taxes and insurance policy	
Letter concerning bank guarantee	
Section B	**Section B**
Scope of expertise	Model of solution architecture
Curricula vitae of key project personnel	Project Charter
Business references	Set of requirements specifications, covering all aspects of e-MRTD issue systems:
Research and development / patents	1. Systems architecture
Checklist for submitting documents	2. Enrolment and delivery
Terms and conditions of the RFP	3. Key management
	4. Passport management
	5. Interfaces
	6. Electronic passport
	7. Personalization system
	8. IT security
	9. PKD requirements
	Project management requirements including Project Schedule objectives
	Curricula vitae of key project personnel
	Sample passports
	Product brochures
Section C	**Section C**
Other informative materials provided by the bidder	Financial proposal
	1. Total amounts
	2. Detailed price statements

traditional booklets. Often a new IT infrastructure has to be procured and processes have to be changed. There are multiple methods established for estimating these costs and efforts, however it is essential to contact experts with experience, either by bi-lateral contact with other States or by asking the ICAO ICBWG for its opinion.

It remains, however, that the internal costs are often forgotten, such as those related to the design and execution of:

1. Rules, regulations, national laws.
2. Project management.
3. Contract Management.
4. Business process reengineering.
5. Construction of new buildings.
6. Security Management Systems.
7. HR for hiring of new personnel.
8. Training of staff.
9. International testing and certification services.
10. Public relations.

Budgets should also consider contingency funds for any and all risks which will definitely arise during the project implementation phase.

Scheduling must be realistic

Let's begin with a simple truth: the implementation of a new e-MRTD issuing system, from the point when a contractor has been awarded the contract up to the start of operations, takes about of one full year.

Success stories where States claim to complete the project in less than six months are either an exaggeration or the supplier has started its work before the official project start. A realistic time schedule is essential for both parties and these plans should already be part of the project management requirements of the invitation to tender. If the issuing authority does not feel comfortable in planning these schedules, then it should ensure it helps to establish the decision making criteria so that the bidder will provide a realistic schedule with its bid.

RFI/RFP: Filtering from worst to the best

The design of a professional invitation to tender document is one of the most crucial parts within the e-MRTD planning process. It should invite all capable suppliers proposing the best e-MRTD issuance systems available for the given set of requirements.

While buyers appreciate getting a greater variety of state-of-the-art solutions, at the same time the invitation to tender should limit the creativity of the bidders to help maintain the 'comparability' of the proposals that will be provided. Finding the best supplier is therefore not only a question of technology and price. Moreover the suppliers' project management capabilities are paramount for a successful deployment of the project.

Finally, a supplier's references relating to successful projects in the field of e-MRTD issuance systems need to be analysed with great care, as often they can claim responsibility for an entire project when they may have only had a tiny share in the overall effort. The invitation to tender should therefore mandate the provision of contact persons of the referenced client, who shall be available to be contacted by the buying issuing authority. All these requirements shall be covered in a comprehensive set of invitation to tender documents. In Figure 2 *(see page 20)*, an example of an RFI/RFP document has been provided for reader reference.

Regardless of how accurately the invitation-to-tender documents have been prepared, the final decision making process remains difficult. A detailed decision making matrix combining evaluating factors with weighting elements should serve as a basis for the discussion between the decision making parties. Notwithstanding this, we should realize that human beings tend to make very subjective decisions, beyond all rationality. The decision making process should therefore make allowances for 'gut feeling' contributions.

After all the planning is completed and the invitation to tender is prepared, it is of utmost importance to design a professional procurement contract so that the issuing authority has a tool in place which can protect their rights during the implementation of the project and beyond.

In our next instalment the co-author of this article, Chris Coulter, will cover the key elements of a sound legal agreement between the buying and the selling parties in an e-MRTD procurement and implementation relationship.

Conclusion

Procurement is the most crucial component in implementing an e-MRTD system, as it connects technical requirements with commercial and legal frameworks. An independent advisor will allow states to remain at arm's length with suppliers and avoid unnecessary high costs, and it is essential to conduct a thoroughly planned tender process and not rush into sole-source solutions. In the next article of this series the authors will be pointing out how to develop a professional procurement contract and how to effectively manage the implementation phase of an e-MRTD project. ■

39 Myths about e-Passports: Part I

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 first of 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 debunked by Mike Ellis of the ISO, one of the world's foremost experts on passport and e-Passport security. The first 10 of the 39 e-Passport myths are reflected here and the remainder will be published in subsequent *MRTD Report* issues during 2010.

KEESING Reference Systems FIGHT FRAUD

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

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

For some time there had been a rising incidence of forged passports which were used by criminals, such as drug couriers, and illegal immigrants. There was also the increasing threat of terrorism. Typically, a lost or stolen passport would have its owner's photograph replaced by the criminal's, a process known as "photo substitution". Often the printed data would be altered too, for example, the date of birth would be made to match the age of the new owner.

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

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

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

Without a doubt, a true success story.

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

Lastly there are the articles written for political gain by activists concerned with a specific government policy. While we have no quarrel with other points of view,

we do object when the technical data is twisted and selectively quoted to suit a particular agenda.

The following is a review of some MRTD and e-MRTD facts to help readers debunk common fallacies and myths currently being reported about e-Passports.

MYTH #1

The e-Passport replaces border officials

e-Passports are not designed and are not intended to supersede the judgment of border officials. We have always trusted humans to intervene and determine state admittance and this technology is only here to assist them. The e-Passport is a traditional passport with an electronic chip. It still has the traditional security features—watermarks, special inks, etc., that are checked by the border official. The same official is trained to look for signs of unease in the owner that might indicate a hidden intent. And when an automated border control scheme is operating, you will find a border official overseeing it. Anything other than a perfect match of the biometric, or any question about the security of the document, will result in an instant referral to that border official.

> **"e-Passports do not supersede the judgement of border officials."**

MYTH #2

The e-Passport was introduced for facilitation reasons

The reasoning behind this myth goes something like this: with e-Passports governments can introduce automated border control to facilitate the passage of travellers through their borders. This leads to a saving of money, but also a lowering of standards as somehow criminals fool the biometric systems with plastic surgery, contact lenses or rubber finger tips. The whole system becomes a "glaring security breach".

As noted in the introduction, the e-Passport was primarily introduced to combat forgery. However, a direct consequence of the more secure passport, with its definitive link to its owner, is that automated border control is made possible. Surveying the systems being introduced, the overriding feature is that they are all being established with careful regard to security, which is paramount. For example, tests for 'liveness' are common to counter attempts to fool the system. As stated in Myth #1, e-Passports do not supersede the judgement of border officials.

MYTH #3

The e-Passport was introduced in response to 9/11; or the U.S. Government designed it for their visa waiver program

ICAO commenced work on the e-Passport in 1998, well before the tragic events of 9/11 or the subsequent changes to the U.S. visa waiver program. However, the e-Passport is well suited to the increased demands for security in the current situation.

MYTH #4

The e-Passport was introduced because the smartcard/RFID industry was desperate for sales

The NTWG spent several years analysing the different ways that various biometrics could be incorporated into the e-Passport. The first step was to decide on the biometric. The facial image was the obvious front runner as photos were already present in passports and were acceptable to all countries. It must be remembered that the passport has to acceptable in all countries, across a wide range of cultures. Some countries regard fingerprints with suspicion and would never incorporate them in the passports of their citizens. Mandatory facial biometrics, with optional fingerprint and iris components, were eventually selected after an exhaustive study.

The next step was to consider how to incorporate the biometric in the passport given that the data requirement was large: at least 10K bytes. This immediately disqualified some technologies, such as the magnetic stripe. Other technologies were proprietary, and thus not acceptable. The two-dimensional bar code was an early favourite, but was found not to store enough information. The contact chip, as found in credit and phone cards, was also considered, but the difficulty there was attaching the contacts in the paper passport. The short-range proximity radio-frequency chip was finally selected because it stores enough information (typically 75K) and can easily be integrated into the passport. The NTWG wisely specified the ISO/IEC 14443 standard as the basis for the contactless chip. It was only after that decision that the smartcard industry became involved.

MYTH #5

The e-Passport was introduced as a plot by the UN (or ICAO, or the U.S. Government, etc.) to regiment the world by gathering biometrics

Conspiracy theories are often difficult to debunk, as they usually rely on no evidence. Passports, however, are issued by a country to its citizens to enable their international travel. Most e-Passports contain the facial image as the only biometric—no change from the traditional passport. e-Passports that contain fingerprints or iris patterns have

increased encryption that severely restricts who can read them.

Countries have always collected the primary biometric, the photo of the face and more often than not have a database of these photos to detect people who apply for passports in other names. These days, most countries have privacy laws which restrict the dissemination of biometrics to other organizations; certainly international interchange does not happen. Other countries do collect biometrics, facial images or fingerprints, to satisfy their security requirements when you enter, but these are voluntary—if you don't want to have your biometric collected by another country, simply do not go to that country.

MYTH #6

All countries must be issuing e-Passports by 2014

As a UN Organization, ICAO sets the international standard for passports under the authority vested to it under the Chicago Convention of 1947. Most countries have machine readable passports which contain recommended minimum security standards. ICAO has mandated that all 190 countries that are signatories to the Chicago Convention must be issuing machine readable passports by April 1, 2010. There is no requirement for countries to issue e-Passports. Most countries, however, recognize the benefits of e-Passports and it is expected that by 2010 over 100 countries will in fact be issuing them.

MYTH #7

The e-Passport was introduced by "a bunch of bureaucrats making decisions about technologies they don't understand"

The ICAO NTWG consists of government officials who are almost all either involved in passport production or border control, with many years of practical experience. Some are encryption experts. The NTWG is supported by technical experts from the International Standards Organization (ISO). Under the ISO/IEC rules, members of the ISO technical committees give their professional expertise and do not represent the interests of their companies. The ISO representatives that attend the NTWG meetings are a range of chemists, engineers, physicists, IT experts, and lawyers. They work for a wide range of companies, including security printers, reader manufacturers and software developers. As well, the NTWG has a number of observers, from Interpol, IATA, Airports Council International, etc. It would be true to say that the NTWG is definitely not "a bunch of bureaucrats" and that the e-Passport technologies are very well understood—especially as they apply to travel documents.

MYTH #8

The e-Passport chip data should be secret

Some of the more sensational news-paper stories over the past few years have involved journalists, with the assistance of "security researchers",

"...most countries have privacy laws which restrict the dissemination of biometrics to other organizations; certainly international interchange does not happen."

reading the data from a passport's chip. Typically they get a copy of the ICAO standard, implement the reading process, and then seem surprised when it works. This is exactly how the e-Passports are meant to work. Otherwise border officials in other countries would not be able to read them.

To prevent unauthorized reading, ICAO specified an optional Basic Access Control (BAC), which most countries have implemented. Unauthorized reading involves either using a hidden reader to access the chip data (this typically works at up to 10 cm, with increased power and antenna size the upper limit would appear to be about 75 cm); or intercepting the data being transmitted between the chip and a legitimate reader ("eavesdropping"). BAC works by using a combination of the printed data as a key that allows access to the chip data. The idea is that any person who has access to the printed data, by opening the passport book, should be regarded as having legitimate reason to access the chip data too.

The journalists then also seem surprised that the BAC procedure is public knowledge: but how else could foreign border control officials access the chip data?

Some countries also equip their e-Passports with integral metal foil pages. When the e-Passport is closed, the metal foil decouples the chip's antenna and thus disables it. When the e-Passport is opened, the metal foil page moves away from the chip's antenna and the chip can be powered again.

While the chip data is open for reading to anyone who has legitimate reason, that does not mean the chip data is

insecure. The chip data is secured by Passive Authentication—that is, digital signature hashes which when recalculated will reveal if any of the data has been tampered with (for example, if the photo has been replaced). The issuing authority calculates the digital signatures using their private key and writes them in the chip; the border official authenticates the same digital signatures using the public key. This public key is available in a certificate, often included in the chip data. The certificate can be authenticated in turn by reference to ICAO's Public Key Infrastructure (PKI) directory, or by bilateral exchange.

Some of the biometric data, fingerprints and iris, are recognized as being more sensitive and are secured by another level of access control, called Extended Access Control (EAC). Under EAC, the inspection system must authenticate itself to the chip before the data is released.

MYTH #9

Contact cards are more secure

This comment is usually made by people objecting to the radio frequency technology, in particular, the potential for interception of the radio transmissions ("eavesdropping") or for unauthorized access. However, contact cards have also been intercepted; one only has to look at the inventiveness of criminals who try to capture credit card details at ATMs. As well, the NTWG investigated eavesdropping and found that data could be intercepted elsewhere in the computer system (eg the radio waves from the USB link, modulation of the power supply). The problem of course is a system-wide one and must be treated as such. It is not peculiar to radio frequency technology alone. The incorporation of shields in the e-Passport and the introduction of Basic Access Control and Extended Access Control have made the problem of eavesdropping and unauthorized access practically non-existent.

A variation of this myth is that bar codes are more secure. Again the system security would be no different. But the problem with bar codes is that they cannot hold enough data for the biometric. Even proprietary versions, which ICAO would never specify anyway, cannot hold enough data.

MYTH #10

The e-Passport chip radiates personal information continuously

The e-Passport chip is powered by the electromagnetic field of the reader; it has no battery or other power source of its own. Therefore when an e-Passport is not close to a reader and powered-up it cannot radiate information. Even when the chip is powered it only responds to commands sent from the reader and the data is protected by the Basic Access Control encryption, so it cannot be eavesdropped upon.

The e-Passport chips are large and power hungry, and have to be powered by the electromagnetic field of the reader. Typically an e-Passport will operate at 4 to 10 cm (2" to 4") from a conforming reader. Of course, it is possible to build non-standard readers with increased power and large antennas, but this is a situation of diminishing returns. Our analysis of the reports of distance reading indicates that practical equipment reaches a limit at about 75 cm (30"). Doubling or tripling the power might result in a small percentage of distance gained, but there is a practical limit. ■

New CSCA Certificate uploads

South Korea, Canada and France formalize ICAO PKD participation

Country Signing Certificate Authority (CSCA) Certificate import ceremonies serve to formalize State participation in the ICAO Public Key Directory (PKD). State representatives, together with senior officials of ICAO, witness the upload of States' CSCA Certificates or *public keys* into the secure facilities at the ICAO PKD Operations Center.

The CSCA Certificate permits the validation by border officials of Document Signer Certificates and the Document Signer Public Key included on e-Passport travel documents. Officials can also use the Certificate data to validate whether an electronic travel document was issued by a competent authority, as well as confirming if its data has been altered in any way subsequent to its issuance by that authority. ■

Canadian International Policy Analyst, Bruce Kelly, shakes hands with ICAO's Walter Amaro, Chief of the Organization's Joint Financing Section and Secretary of the PKD Board. They are joined on the occasion of the Canadian CSCA certificate import ceremony, October 15, 2009, by Christiane DerMarkar (far left), JF/PKD Officer in the Joint Financing Section of the Air Transport Bureau, and Marcus Serrao (far right), a consultant at Passport Canada.

Walter Amaro (left), Chief of ICAO's Joint Financing Section and Secretary of the PKD Board, is joined by Won-sam Seo (center), Alternate Representative on the Council of ICAO and Minjeong Park (right) on the occasion of South Korea's CSCA certificate import ceremony, August 26 2009.

France imported its Country Signing Certificate Authority (CSCA) in the PKD on December 7 2009. In attendance are (from left-to-right): Pierre Pape, Alternate Representative on the Council of ICAO in the French Delegation; Christiane DerMarkar, JF/PKD Officer in the Joint Financing Section of the Air Transport Bureau; and Dominique Gatinet, Standardization Manager, French Secure Document Agency.

Ensuring breeder document reliability

Civil status documents are often representations of legal facts contained in civil status registers. A civil status document confirms, as it were, a legal fact recorded in a civil register. If people do not have confidence in such documents, a country the size of the United States can be thrown into complete confusion.

As Fons Knopjes and Diana Ombelli of The Netherlands' ID Management Centre reports in this special feature for the *MRTD Report*, during the past decade, countries and organizations have made efforts to enhance and protect the integrity of the information contained in civil registers in order to prevent abuse.

Fons Knopjes is Managing Director of IDManagement Centre. He is a member of the core group of experts on identity-related crime for the United Nations and for the Implementation and Capacity Building Working Group of ICAO. In 2008 he published "Documents: the Developer's Toolkit", a publication about the development process of secure identity documents.

Diana Ombelli is a freelance ID Management Consultant and Project Manager. She was employed for more than 7 years at Sagem Identification, working on projects involving the development of identity documents and the implementation of related IT systems. She also participated in the design of the biometric acquisition process for the new Dutch e-Passport.

Barack Obama was born in Kenya. His birth certificate from the Coast Province says so and his Kenyan grandmother confirmed the Kenyan roots of the new President of the United States.

However the papers were hardly hot off the press before the first allegations began to emerge. The issue is highly sensitive because only a natural born citizen is eligible to be President of the United States. Even before the presidential election was held, opponents alleged that Barack Hussein Obama had not been born in the State of Hawaii. They rejected the birth certificate that was presented by the Obama campaign, saying it was a forgery.

In a way it was only natural that a misunderstanding had arisen; people thought that the document under scrutiny was the original birth certificate. But in reality the controversial document was only a recent certification of the original birth record (Certification of Live Birth). Obama's opponents asked to see his original birth certificate (the long-form Certificate of Live Birth) drawn up by the Hawaiian hospital so that they could verify it.

Protecting the information in civil status registers

If the reliability of civil status registers is seldom the subject of investigation, questions can nonetheless arise concerning the origin of an excerpt from the original record (which in the case of a birth certificate is a certification of a birth, also referred to as the 'short' birth certificate) or a full and complete copy of the original record (also referred to as a certified copy).

Sometimes citizens and companies require excerpts or certified copies of original entries in civil status registers to prove to other parties that certain information is true. Civil status documents are reliable representations of the

information contained in civil status registers. The information in these documents is therefore extremely valuable to society and its abuse must be prevented at all costs. Although it may seem obvious that we should seek solutions to protect such information in the digital world, we cannot afford to underestimate the continued use of paper documents. Many countries worldwide still issue civil status documents in paper format and it is up to governments to ensure that the recipients of such documents can rely on their authenticity and content.

The choice of information medium (document)—the way in which the information is presented and authenticated—plays an important role. To safeguard the integrity of documents and the information contained in them, it is important that governments take the necessary measures, focusing on registration, the documents themselves and how they are issued.

We cannot risk issuing paper documents that are not protected against forgery or falsification. Governments that issue civil status documents must ensure that the recipients of such documents, as well as the parties requesting them, have confidence in the documents and their issuance.

Municipal measures that build public confidence and prevent abuse

Of course we all know examples of countries where things are either not regulated properly or not regulated at all. This makes it very difficult and time-consuming for governments to verify the legal information contained in civil status documents from such countries.

Although safety paper for making civil status documents has been available in the Netherlands since the mid-1990s, some Dutch municipalities still choose not to use it. 85 percent of Dutch municipalities use safety paper for issuing civil status documents (source: Netherlands Central Purchasing Agency). From a European perspective, 85 percent is not bad (see section on measures of European countries further on in this text). Even so, the choice of some municipalities not to use safety paper creates a weak link that puts the overall system and its dependability at risk.

International guidelines

The United Nations has issued principles and recommendations for establishing civil registers and maintaining and utilising their statistics[1]. Besides describing the principles of compulsory registration and the universality and confidentiality of information, the publication explains which legal and administrative arrangements need to be put in place to safeguard the trustworthiness and dependability of the information. It also recommends that a special type of paper be used for the issuance of civil status documents as a deterrent to fraudulent alteration and abuse.

"We cannot risk issuing paper documents that are not protected against forgery or falsification. Governments that issue civil status documents must ensure that the recipients of such documents, as well as the parties requesting them, have confidence in the documents and their issuance."

Measures of European countries

During the 25th conference of the European Ministers of Justice in 2003, the International Commission on Civil Status (ICCS) presented a memorandum on the growing fraud in civil registration.

Two years later, the ICCS adopted the "Recommendations on combating document fraud with respect to civil status", which maintain that civil status documents should at least bear the date and signature of the issuing authority, and possibly an official seal. The name of the register of origin should also be mentioned. Unfortunately, the recommendations do not set any requirements on the information medium used. This was a missed opportunity to raise the value of the medium (or document) to the level of value of the information, thus minimising the risk of abuse.

Additionally, the recommendations of the ICCS provide methods to spot forged or altered documents.

The ICCS also holds an ongoing survey to obtain information on the legislation and practices of its member states. The survey shows that all member countries apply a signature and stamp or seal to authenticate civil status document. Half of the countries also use safety paper.[2]

Abuse is often related to the recognition of civil status documents from other countries. This is because there are very few international standards for document format and content.

The document that is probably the most widely abused is the birth certificate. Its fraudulent use lies in the fact that in many countries the birth certificate serves as the source document for obtaining other documents, including identity documents. In the United States, people can obtain a social security number on the basis of a birth certificate. They also need a birth certificate to apply for a driver's licence, which in the United States (unofficially) doubles as a national identity document.

The United States does not have a national identity card and not all U.S. nationals own a passport. The country has over 14,000 different versions of birth certificates in circulation[3]. Everyone born in the United States is

[1] Department of Economic and Social Affairs of the United Nations, *Principles and Recommendations for a Vital Statistics System* (Revision 2), New York, Unites States, 2001

[2] International Commission on Civil Status, *Guide Pratique International de l'état civil*, http://www.ciec1.org/GuidePratique/index.htm

[3] Department of Health and Human Services, Office of Inspector General, *Birth Certificate Fraud*, Washington, United States, September 2000

automatically an American citizen. That is why U.S. birth certificates are so sought-after.

To counter fraud in civil status documents, many countries have opted for a judicial approach and threaten sanctions. An example of this is France, which has drawn up anti-fraud guidelines based on three measures: sanctions, caution by the government and the legalisation of foreign civil status documents[4].

In some cases, the legalisation of foreign public documents offers few guarantees that the information in the document is authentic. Ninety-eight countries have become party to the *Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents* and recognize foreign documents without further authentication[5].

As in other fields, measures also need to be developed in the areas of prevention and communication. In June 2009, the European Union published the *Stockholm Programme*[6], a new programme which defines priorities for the areas of freedom, security and justice from 2010 to 2014. It addresses a number of issues, such as the free movement of European citizens, human trafficking and cybercrime. It also pays special attention to civil status and other official documents.

Section 3.4.1 of the *Stockholm Programme* states that:

> *"…certain formalities for the legalisation of documents also represent an obstacle or an excessive burden. Given the possibilities offered by the use of new technologies, including digital signatures, the EU should consider abolishing all formalities for the legalisation of authentic documents between Member States. Where appropriate, thought should be given to the possibility of creating authentic European documents."*

The EU should also consider introducing a system that allows European citizens:

> *"…to obtain the main civil status documents easily and at no extra cost. The system must help overcome any language barriers and guarantee the evidential value of these documents."* (Stockholm Programme, Section 2.1)

Digitization of the process is bound to raise other questions regarding the protection, confidentiality and availability of citizens' data within the EU. The *Stockholm Programme* will also facilitate initiatives to further protect personal data.

The mobility of citizens worldwide and the increased speed with which governments are required to manage their administration demand further improvement of civil status processes in order to safeguard the integrity of personal data and prevent abuse. To achieve this, technological solutions need to be examined and supported by policy measures.

In closing

It is not surprising that new programmes look ahead and explore the possibilities offered by new technologies. Nevertheless, such developments must never draw attention away from existing registers, documents and processes, as this often leads to fraud.

For those of us who did not follow the controversy surrounding Barack Obama's birth certificate, in 2008 experts finally examined the original civil record, establishing its authenticity and verifying that the new president of the United States is in fact a native born American. ■

[4] *Direction des Affaires civiles et du sceau "Circulaire: Fraude en matière d'actes de l'état civil étrangers produits aux autorités françaises"* CIV 2003-03 C/01-04-2003, NOR : JUSC0320085C, Paris, France, 2003

[5] *The Hague Convention Abolishing the Requirement of Legalisation of Foreign Public Documents,* The Hague, The Netherlands, October 1961

[6] European Commission, *Stockholm Programme*, (COM 2009) 262 final, Brussels, Belgium, June 2009

Facilitation:
The ultimate security solution?

Air travel should be about safely getting from Point A to Point B in the quickest possible time. The host of security checks to which passengers are subjected at airports impedes such an objective. Dominique R. Antonini considers what the aviation security world can learn from its counterparts in facilitation and how the two entities can combine forces to provide passengers, staff, airports and airlines with a security solution that embraces speed, quality and effective threat management.

Dominique R. Antonini worked 20 years in the aviation security field, including more than 15 years for ICAO, initially as Technical Officer, then Training Officer, Chief of Aviation Security and lately Chief of the Aviation Security and Facilitation Policy programmes and the MRTD programme. He was Secretary of the UIC, AVSEC Panel, IETC and AH-DE between 1999 and 2006. He is now Consulting Engineer, Director for AVS&C, an aviation security consultancy company based in Geneva, Switzerland (http://avs-c.eu/) also member of the European Biometrics Forum (http://eubiometricsforum.com) and the avsec-center.org consortium (http://avsec-center.org).

This article originally appeared in the June 2009 issue of Aviation Security International and has been reprinted here with the permission of the publisher.

According to the numbering order of the ICAO Annexes to the Chicago Convention, 'facilitation' is obviously a core and essential activity of global civil aviation.

Annex 9—*Facilitation* appears before Aeronautical Telecommunication, Air Traffic Services, Aerodromes and, notably, both Environment and Security—the two "hot topics" for the industry. The first international Facilitation Standards were adopted in March 1949, when ICAO was in its infancy as an Organization. The first Aviation Security (AVSEC) Standards were only adopted 25 years later (in March 1974) by the more mature body which ICAO had by then become.

When in 1996, the ICAO Secretary General[1] decided to merge Facilitation and Aviation Security within the same administrative branch of the Organization, one of the justifications was to *"join the two faces of the same coin"*, reinforcing the widespread assumption that Facilitation and Security were a contradiction in terms and, even worse, had conflicting objectives. Nowadays, in most States, Facilitation and National Security Committees are still separated and, even if they are meeting in the same room, Security's voice is always stronger as it is perceived to be more important.

The ICAO Facilitation programme has always been managed in a long-term, progressive, yet conservative manner, with limited budgetary resources. Meanwhile, the ICAO AVSEC programme exploded onto the scene following the Lockerbie incident, with the inception of the AVSEC Mechanism in 1990[2]. It gradually lost prominence, focus and funding throughout the 90s only to re-emerge post-9/11 with the creation of the universal AVSEC audit programme and, more importantly, the mobilization of huge AVSEC resources within ICAO's regular programme budget (unfortunately for auditing purposes only!).

These two sides of a very strange coin, conjoined by a special 'glue' in the form of biometrics and Machine Readable Travel Documents (MRTDs), were to guarantee the identification and authentication of passengers crossing international borders. The greater the number of passengers providing their personal information utilizing secure tokens (e-Passports), the quicker they can process immigration (automated clearance systems) in comfort and, perhaps, even under pleasant conditions. In parallel, as more States sought to gather information on inbound (and, for some States, outbound) passengers for background check purposes (e.g. national security objectives), the more they force industry stakeholders to extract relevant information from passengers at the earliest stages of their journey (Advanced Passenger Information programmes).

Unfortunately, the ICAO Aviation Security and Facilitation Branch was dismantled in 2007 due to limited resources, which forced internal restructuring to beef up the growing Aviation Security and Safety Audit Programme[3]. This first-ever Universal Security and Safety Audit Programme represented a fair international benchmark for security/safety national quality control measures and implementation. It was an important step forward towards a systemic approach and the provision of proper risk management and we should anticipate that newer information technologies used for Facilitation, such as biometrics, will demonstrate even greater potential for effective security risk management provision.

Even if some objectives or constraints of advanced passenger data programmes can legitimately be discussed or disputed, nobody can deny that the combination of adequate technology and proactive political willingness has dramatically improved facilitation and the comfort of the travelling public. The success of some registered passenger programmes provides a crystal clear message: user-friendly and customer-oriented solutions can be deployed at airports without compromising (indeed augmenting) performance criteria and legal objectives.

Autopsy of the success: a three-dimensional approach

Honestly speaking, twenty years ago, who could have imagined that passengers would have been permitted by immigration authorities to cross international borders automatically? Who could have anticipated airlines' capabilities to provide detailed information about their customers enough time before departure for official assessment and approval by foreign authorities?

The facilitation success of border crossing controls could have been compromised by what I term "the first dimension"; that being the level of legal requirements imposed by some States on the travelling public. The data required about passengers willing to travel to some destinations, while impressive in terms of quantity, is also questionable when considering privacy issues. Travelling is not a right anymore—rather a privilege! Having said that, the legitimate need for some information is not under dispute and, as such, despite the ever-increasing number of States requesting data, there has been little damage to traffic volume on the routes under such scrutiny.

The "second dimension" of recent facilitation success is the deployment of a large variety of different technologies for identification and authentication. Even if face recognition is a 'must' according to ICAO specifications for MRTDs (ICAO Doc 9303), fingerprints, iris, hand recognition and other biometrics are also broadly deployed at airports for border control.

Face recognition is, for example, used in Portugal where the RAPID solution provides a free-of-charge entry/exit/transfer border checking solution for electronic passports (e-MRTDs). These RAPID e-gates work with an average 15-20 second processing time (which is the same average processing time recommended by IATA in its Airport Design Reference Manual) and a maximum daily capacity of 4800 passengers for a working period of 20 continuous hours per day (without breaks or strikes!).

Fingerprints are also used, for instance by SAS and Norwegian Airlines, for Automated Baggage Clearing. Here the objective is simply to ensure that persons who checked-in hold baggage are boarding the correct flights. Security is maintained with better facilitation as passengers do not have to show their identification documents, or even their boarding passes, as their fingerprints *are* their identity! This procedure has

[1] Dr. Philippe Rochat.

[2] Managed by Raymond Benjamin, the current ICAO Secretary General.

[3] The ICAO Aviation Security and Facilitation Branch was once again re-instated as a joint operation shortly therafter.

now been deployed at more than 30 airports and is used by a vast number of customers with high levels of satisfaction (98 percent). Fingerprint-based solutions are also deployed in many airports/installations for staff access control purposes, also with much success.

Iris facilitation solutions are additionally deployed at many airports, including those in the United Kingdom. The PRIVIUM programme in Holland is one of the largest registered traveller programmes in Europe with more than 48,000 members. More than one million automatic border crossings are registered on a yearly basis, with an average processing time of 12 seconds and a rejection rate of less than 1.5 percent. An interesting element of the PRIVIUM programme is its potential for expansion to other airports at very limited additional expense.

The third, and probably the most innovative dimension for this success story is the consideration that customer satisfaction is essential—customers being both those passengers who are registered in programmes on either a fee or free basis and the airports and airlines which have an essential role to play in the process. It should not be forgotten that industry stakeholders are not only those entities that have to respond to the flack from disgruntled passengers, but they are also the messenger of somebody else's bad news as they have also been forced to comply with or enforce new legal requirements imposed whether or not they agree with them. The aim for all is a smooth, user-friendly process that starts even before the arrival at the airport with web-based questionnaires. This is followed by confirmation of the information provided during check-in and then the use of advanced and secure information exchange processes with appropriate overseas authorities for the approval to travel.

The customer satisfaction element has driven the selection of technologies as passengers and industry stakeholders have a common interest; i.e. reducing processing time to the minimum possible. For passengers, this reduces their levels of stress and thus increases both their pleasure of travelling and the impression that they're considered valuable clients. Airports benefit since the shorter the time passengers waste in queues at checkpoints, the more dwell-time they have before flight departure to spend discretionary dollars in airport shops and eateries. Finally, airlines see positive results as registered programmes are a key element helping them to differentiate between frequent and occasional travellers—thus offering greater opportunities to reward loyal clients with differentiated marketing campaigns (reductions for duty free shops, fast tracks for specific routes, etc.).

The three sides of the same coin!

The three-dimensional approach that has been successfully adopted by authorities, airports and airlines for facilitating border controls may not, however, be applied to security.

Aviation security requirements are much more onerous, with a list of prohibited items that has become somewhat obsolete when considering the additional security measures imposed since 9/11. Examples include the need to remove knives or other sharp objects when aircraft are now equipped with reinforced cockpit doors (supposedly preventing any hijacking of an aircraft using these implements), or when 50 ml of certain dangerous liquids is still permitted, and will continue to be permitted, even with new liquid explosive detection systems.

We also need to mention here the survival of the standard on baggage reconciliation (positive passenger bag match) which was understandable when the assumption was that checked baggage could not be effectively screened and that nobody would knowingly blow themselves up on board a flight. Such obsolete requirements have a cost for airports and airlines and are diverting security resources from essential functions, particularly when new security measures tend to be simply stacked on the top of others without a clear, logical or holistic strategy.

"...civil aviation security systems at airports will never be capable of 'fighting terrorism', but intelligence and cooperation between national security agencies will."

The problem in identifying breakthrough solutions in aviation security is caused when harmonization, or even standardization, is imposed without involving all the major players; i.e. manufacturers and more importantly end-users (airports or service providers in this case). Why do new body scanners have to be acceptable to the general public worldwide? Why are experimentations on new technologies stopped at some airports because of the media reaction in other States or even other Regions? Who is driving innovation? Why are authorities so careful about the public perception when dealing with new technologies, and not when imposing useless and ridiculous measures such as the removal of shoes, or even the 100 ml liquid ban? New body scanners will better detect explosives on people, including within their shoes, and if liquid explosives are considered as a credible threat, a total ban would have been more logical pending deployment of any new liquid detection equipment for departing passengers. The sad fact is that some

promising and cost-effective liquid detection systems are indeed currently available, but not yet deployed, because of lack of certification by the very few 'controlling' States.

The new aviation security motto of 'unpredictability' or 'randomness' to counter terrorist attacks seems only applicable for the implementation of procedures and measures at airports, not for the design of security systems and the deployment of new security equipment.

On the third dimension, customer satisfaction, aviation security is just ignoring it when it comes to passenger screening! For Hold Baggage Screening (HBS), the very same authorities have accepted some flexibility in terms of technologies, measures and use of mixed automatic/human detection systems, but this is probably because the introduction of systematic HBS was not directly linked to a security risk or a perceived threat. The ICAO *Annex 17*, 100 percent HBS standard was imposed in the aftermath of 9/11; i.e. 13 years after Lockerbie. Moreover, 100 percent HBS is totally transparent for passengers, which means that passenger facilitation is solely linked to the quality security controls at passenger screening checkpoints.

If the current two-dimensional approach for passenger screening is to become a three-dimensional one, we need to learn the positive lessons from the use of automated border clearance systems and apply them to the security screening checkpoint. This will be achieved through broad industry consultation, rather than just blindly imposing a new rule or technique upon the industry and then by utilizing technology to drive facilitation (e.g. trace detection in shoes, automated liquid explosive detection, identity verification, etc.) and improve the overall customer experience.

Facilitation: The ultimate security solution?

Despite the fundamental objectives of aviation security, we should recognize that airport screening points will never detect terrorists while they are in the process of committing an act of unlawful interference, but may identify mentally challenged or unruly passengers. In other words, civil aviation security systems at airports will never be capable of 'fighting terrorism', but intelligence and cooperation between national security agencies will.

The problem is that current security measures are so complicated, and in some cases obsolete, that current screening checkpoints are generating massive queues of unprotected passengers. If facilitation and customer satisfaction could be equally considered in the design of new passenger screening points, the number of unprotected passengers queuing before security checkpoints could be reduced to an acceptable level.

In addition, the information gathered on departing passengers, via an advanced passenger information programme or even through specific 'behaviour assessment' procedures during the check-in processes, could be recycled by airport security staff for performing better risk assessments on passengers passing security checkpoints. The concept of 'centralized screening points' had some validity ten years ago when savings were necessary and staff screening was not a requirement. The very same concept is questionable when it removes the possibility of differentiating passengers travelling to sensitive destinations or with high risk airlines, thus augmenting operational costs for enhanced security measures imposed on all passengers.

Some solutions exist, such as: the use of IATA tags for cabin baggage (as currently used by some low-cost airlines willing to check the weight of cabin baggage); permitting identification of the final destination during security controls; biometrics on passengers (as used for fast tracks or e-borders) to know where that passenger is flying to and what are his/her background information; or even RFID boarding passes.

Finally, the 'special glue' between facilitation and security (i.e. the MRTD programme), is definitely the only ICAO programme which could be considered as helping to combat terrorism. If all passengers use Machine Readable Passports (MRPs), the tracking of potential perpetrators preparing acts of unlawful interference becomes significantly improved.

It is said that the 9/11 acts required two years preparation, with extensive travel to test security measures at airports, and even encompassed registration with frequent traveller programmes. In this context, it could have been possible to identify some of these perpetrators by proper risk assessment of their travelling behaviours with the information retrieved from automated border clearance systems. Easy to say now, of course, as the ICAO MRTD programme and MRPs were not required back in 2001 and, in any case, the terrorists were flying on domestic flights requiring limited checks.

Fortunately, Standard 3.10 of ICAO's *Annex 9* imposes the issuance of MRPs in accordance with the specification of ICAO Doc 9303, Part 1, not later than April 1 2010. e-Passports should be imposed in *Annex 9* as being a bonus for facilitation, border crossing and additionally for security risk assessment/management.

Let's also hope that ICAO will soon re-establish the late Aviation Security and Facilitation Branch to regenerate long term, and innovative, synergies between security, facilitation and MRTD programmes, with the objective of designing breakthrough solutions, following the three-dimensional approach already adopted by facilitation, so that facilitating travel for all legitimate passengers combined with adequate, customised, and cost-effective systems developed by the industry, will be seen as "the" security solution. ■

it's live!

A new global hub for MRTD suppliers and information!

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

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

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

www2.icao.int/en/MRTD2

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

Identity Management for Safer, More Secure Travel

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

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

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

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

Visit us at Security Document World, INTERGRAF, 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