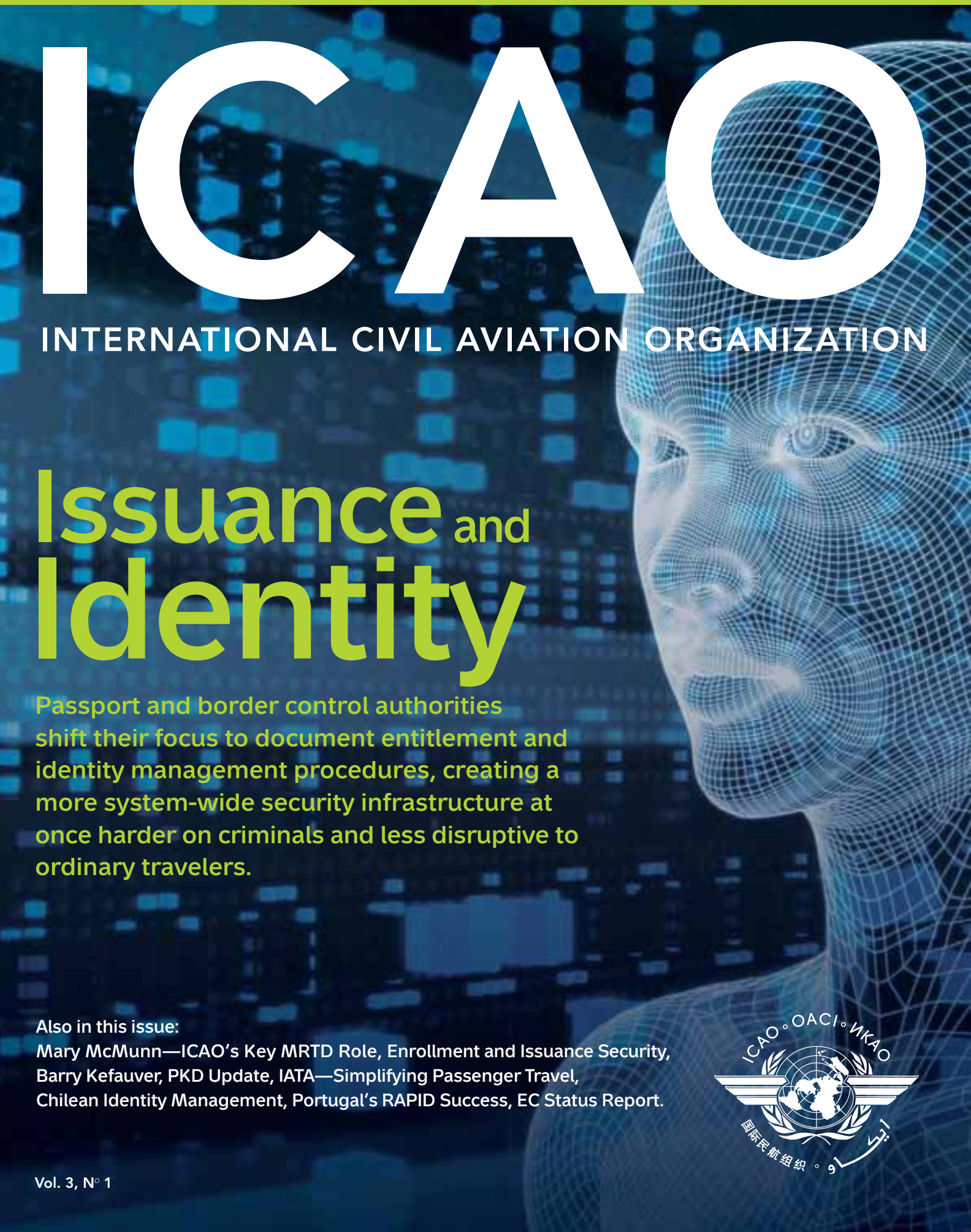
MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION



Issuance and Identity

Passport and border control authorities shift their focus to document entitlement and identity management procedures, creating a more system-wide security infrastructure at once harder on criminals and less disruptive to ordinary travelers.

Also in this issue:
Mary McMunn—ICAO's Key MRTD Role, Enrollment and Issuance Security, Barry Kefauver, PKD Update, IATA—Simplifying Passenger Travel, Chilean Identity Management, Portugal's RAPID Success, EC Status Report.

Vol. 3, N° 1

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

Secure your passport...

GET Group is the world leader in state-of-the-art passport solutions. With references around the world, more than 20 years of experience, and as exclusive distributor of Toppan digital passport printers, GET Group is uniquely positioned to provide passport solutions that meet your highest security needs.

Toppan passport printers employ proprietary digital pigment ink printing and lamination technologies to produce one of the most secure passports in the world. Our latest TOPPAN E2000 passport printer fully meets the requirements for ICAO/ISO ePassports and features on-line chip encoding, automatic book feeding as well as user-friendly operation.

...with our E2000 passport printer.

ICAO MRTD REPORT
VOLUME 3, NUMBER 1, 2008

Editorial
Managing Editor: Mauricio Siciliano
MRTD Program—Specifications and Guidance Material Section
Tel: +1 (514) 954-8219 ext. 7068
E-mail : msiciliano@icao.int

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

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

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

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

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

Leadership and Vision in Global Civil Aviation

www.icao.int

The International Civil Aviation Organization

Extending our Reach

The ICAO MRTD Program elaborates on one of the main ICAO Strategic Objectives: to enhance the security of global civil aviation. In many ways the Program is a perfect example of the effective application of facilitation principles to improve aviation security.

However the MRTD Program also has a broader impact, in the sense that its thorough implementation enhances the aggregate national security of States in their fight against terrorist and criminal mobility. During the Fifth Special Meeting of the United Nations Counter-Terrorism Committee with international, regional and sub-regional organizations in Nairobi last October, the ICAO MRTD Program was duly recognized for this specific benefit.

Additionally, ICAO MRTD standards and specifications benefit average citizens by building confidence in authentic identity documents, primarily by protecting them from identity theft and allowing for the development of machine-assisted border-control systems. These systems greatly reduce the waiting times and associated inconveniences that have been all too frequent occurrences in today's more elevated security environment.

It must be stressed at every opportunity that the key to benefiting from these standards and specifications lies in their *comprehensive* implementation. We have achieved a worldwide consensus in ICAO that by 2010 all member States must begin issuing *only* MRPs, and with the full weight of an ICAO Assembly Resolution now in place we are aggressively pursuing this objective. Some States are considering or have already begun implementation strategies, and many have already achieved their preliminary MRTD goals but are now pursuing security measures to bolster their breeder document, entitlement and MRTD issuance processes.

It is recognized that certain States may need assistance to issue their MRTDs, or perhaps require assistance to establish and provide training in this field. For all these needs we encourage you to consider and take advantage of ongoing ICAO support programs such as the Universal Implementation of Machine Readable Travel Documents (UIMRTD) Project. ICAO, with donor States, international organizations and other United Nations offices, is coordinating efforts and resources to assist States in strengthening their capacities, both in this field and in overall security preparedness. As the UN agency that establishes and updates the standards and specifications on MRTDs, ICAO is best suited to identify the pertinent expertise and technology and has a proven and experienced Technical Cooperation Bureau to assist and support all related development, procurement, training and implementation needs.

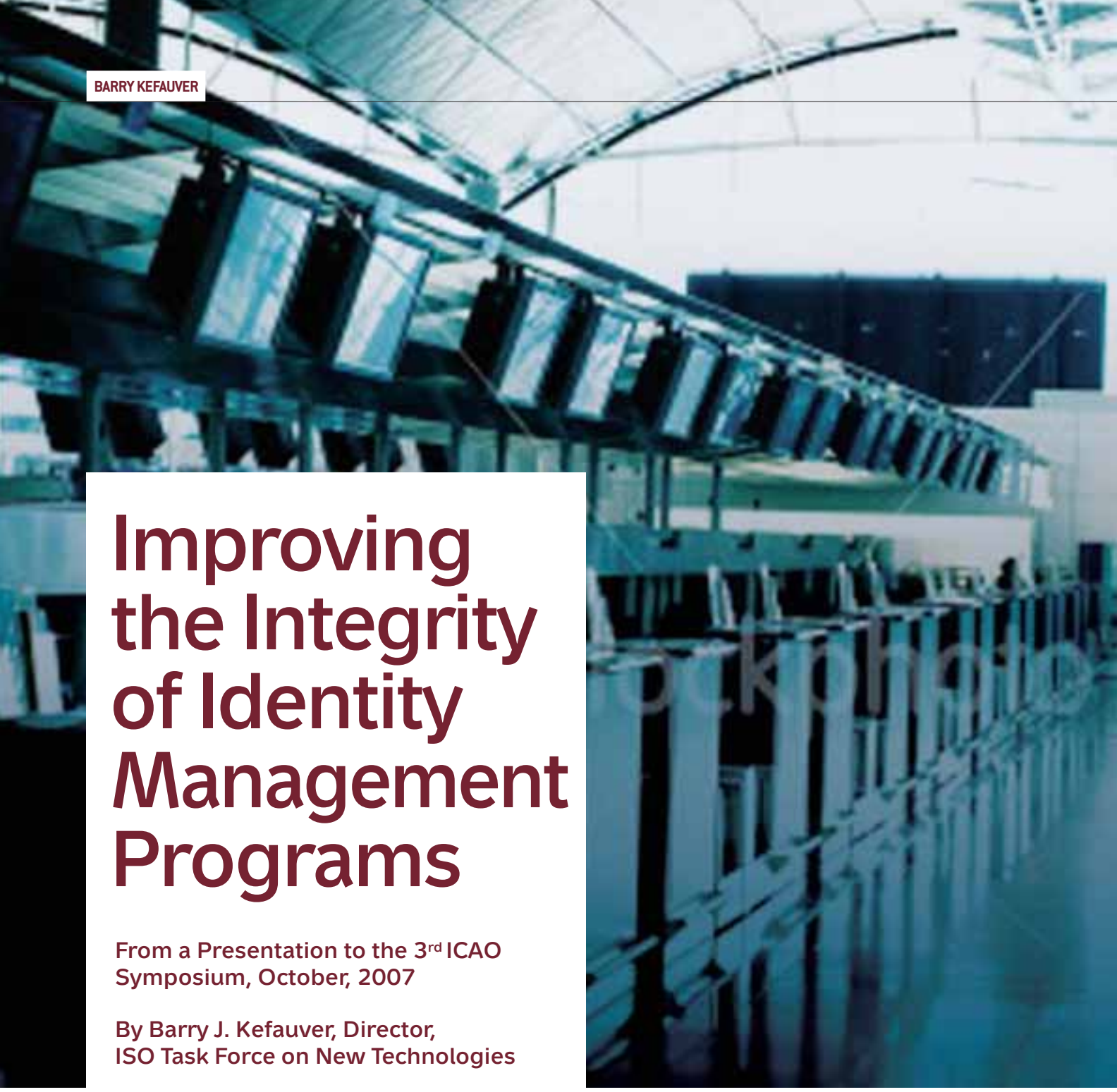
I encourage those Sates requiring assistance with their machine readable travel documents, or needing assistance to improve the secured issuance of their MRTDs, to contact ICAO to find out how to benefit from this program. They may also visit the UIMRTD Section of our web site at: mrtd.icao.int.

As background on the origins of ICAO's important ongoing role with MRTD activities, you will find in this issue an interview with Mary McMunn, former Chief, ICAO Facilitation Section, who shared with the Report the origins, ambitions, and legal and regulatory basis that led ICAO to establish and maintain the MRTD standards and specifications. You will also read an excerpt from a presentation made by Barry Kefauver, during the 2007 Symposium on the integrity and security of breeder documents. ICAO and its partner organizations have established the achievement of this integrity as an important priority, and ICAO now includes it as part of the assistance strategy available through the UIMRTD.

The MRTD program is at the heart of border control and automated initiatives worldwide. In this issue you will also learn about IATA's Simplifying Passenger Travel program, the successful implementation of the Portuguese RAPID system, and an update on the implementation of the ICAO PKD. ■

Enjoy your reading.

Mauricio Siciliano
Editor



Improving the Integrity of Identity Management Programs

From a Presentation to the 3rd ICAO Symposium, October, 2007

By Barry J. Kefauver, Director,
ISO Task Force on New Technologies

I've chosen this topic for this presentation to underscore what I feel is a critical aspect of identity management concern. My focus will be on both the systems through which the entitlement judgments are reached, as well as the systems that issue and personalize identity documents.

I'm quite pleased to have been involved over the past dozen or more years with initiatives to improve the integrity of the documents used for travel, especially the passport. However, the plain truth is that as the documents have been made increasingly secure and tamper-evident, the path of lesser resistance for those of ill intent will be the systems on which these documents rely. Unless urgent and far-reaching measures are taken to shore up these vulnerabilities, the systemic porosities could make, really, a mockery—and I choose that word carefully—a mockery out of the hard work and huge resources that have gone into document improvement.

My presentation will cut across all issuing authorities. These issues and concerns know no national or cultural boundary, and cut across a wide variety of identity management areas of focus: particularly cards of national identity, as well as travel documents.

My focus essentially revolves around the systems on which identity documents rely for meaningful integrity, and associating the document with the rightful bearer and having confidence that that bearer is, indeed, correctly identified. I'll talk about the processes that have gotten us where we are, where I feel that is, and where I think we yet need to go.

Summary of Current Developments

I provide this slide *(see Reference Slide 1, page 6)* to give you a concise history of the development of the standards relating to the MRTD program. There's been quite a bit of turnover among those of us who are getting long in the tooth in the ICAO standards-making arena and I think capturing succinctly what that history has entailed will prove useful.

Many questions have arisen over the past few years regarding the when, what and why relating to these standards and the processes that led to their development. The first bullet, the London meeting, resulted in the first formal endorsement of contactless chips to be placed into a paper substrate. Prior to that, we were looking at cards, plastic cards, and really looking at chips solely for that kind of a medium which I think is relatively recent given where we are now. November 2000 was when we first talked seriously about putting chips into a paper substrate.

The Biometric Selection Technical Report was the first technical report issued. This was the result of nearly five years of work and I consider it to be a major item of focus. The July 2003 meeting resulted in all of us who had been associated with the dialogue and the deliberations that led to the chip initiative patting ourselves on the back thinking how smart we were. We heard during that session that everything was just fine and that we could continue forging on without any undue stress or, specifically, additional standards work. As I'll get to in a short while, that was not quite the case—quite the contrary as a matter of fact.

The three companion technical reports were drafted together and we produced those as closely together as we could. Then came Canberra in February 2004, where some reality began to settle in. What we discovered in Canberra was that these chips and readers that were identifying themselves as '14443-compliant' couldn't actually speak to each other. We had 11 different readers and over a dozen different chips and not one would function with the other. In fact, some of them wouldn't read any of the chips at all. Reviewing this work in Canberra, we realized that we still needed to do a lot of work—in total there remained some 23 specific standards areas relating to 14443 that needed to be developed for effective travel document functionality.

I bring the February 2005 guide to your attention because I think it's still something of value, still something useful for those of you who may yet be looking at implementing chip-based passport programs. Note that this guide is still available on the ICAO website.

REFERENCE SLIDE 1: DEVELOPMENT TIMELINE

1. London November 2000—Contactless chips.
2. Biometrics Selection TR 2001.
3. London July 2003—Joint ICAO/ISO meeting.
4. LDS TR 2003.
5. PKI TR 2003.
6. Biometrics Deployment TR 2003.
7. Canberra, February 2004.
8. *9303 Supplement*—Kyoto, September 2004.
9. NTWG—Auckland, December 2004.
10. Berlin, February 2005—the "Guide".
11. Montreal, September 2005—TAG acceptance of *Edition Six* Draft Part 1.
12. Berlin, May-June 2006—Testing and TF/WG3 meetings.
13. *Supplements, Editions Four* and *Five*, published as posted.
14. *Supplement Edition Six* submitted for posting.
15. *Part 3* drafted, readying for publication before the end of this year.

The most recent reference document noted here—*Supplement Edition Six*—has been drafted and has been posted. This is the maintenance document that we've developed to highlight content sections in document 9303 that either need clarification, amplification, further broadening—whatever the case may be. The supplement is the vehicle for doing that and it is now, as noted, available in its sixth edition. Finally Part Three—*Cards and Other Official Travel Documents*—that has been drafted and is with the Secretariat for publication.

The Wave of the Present

The uses of biometrics and contactless chips are the crucial technological advances in travel documents. I also wanted you to know that there are many other measures that have been taken to enhance document integrity. ICAO began its examination of what we have termed co-existing data storage technologies in 1995.

The watershed point of departure for contactless chips began at that meeting I'd previously mentioned in London, 2003. Since then, there have been tremendous efforts devoted to issues such as data security and interoperability; and the use of biometrics has also been under continuous review since 1995. The process of data sharing is still in what I consider to be its infancy, though the implications for cooperation and intersection in this area are extremely important for the ensuing aspects of this presentation.

With all the focus on the document, we must take cognizance of the systems that issue these documents. As an initial frame of consideration, Reference Slide 2 *(above, right)* calls out some of the measures that need to be employed to effect control over the document processes from within the issuing authority.

The first bullet noted there, the human aspects, are quite crucial in my opinion, and they are the ones that also, in my opinion, are most fraught with porosities of several different forms. I will talk very explicitly later on about the human side of the enterprise. In my opinion, the issuing authorities must take a zero-tolerance stand with respect to the human element. There can be no room for laxity in this area. Finally, the legal infrastructure of penalties must be tight and a distinct disincentive to mischief. Penalties must be commensurate with the breach.

Breeder Documents and Identity Establishment Procedures

If I had to identify one area of insidious impact on document entitlement judgments, procedures and processes, it would be the pivotal role of breeder documents. I have noted here that there are no less than 7,000 different kinds of legitimate US birth documents; I've used this 7,000 figure only because it's the lowest estimate that I've have heard. In general, it's estimated that there may be upwards of 10,000 legitimate forms of birth documents for the US alone.

REFERENCE SLIDE 2: MEASURES FOR INTERNAL CONTROL

- Human systems—zero tolerance.
- Work atmosphere and environment.
- Spoiled documents.
- Blank document controls.
- In-house auditing.
- Penalties-legal judicial system as well as administrative.

The use of training is, of course, endemic in all aspects of the identity document apparatus. Especially critical are the adjudication and entitlement procedures. Distribution and dispersion of adjudication decision-making implies inherent variances. This makes standards and models for such decisions absolutely critical.

The use of IT tools, particularly those that will assist in streamlining the work of the very overworked adjudicators and entitlement decision makers around the world, shows some promise. If I could highlight one useful example I think the security process that's being employed by Continental Airlines at Newark Airport for flights to Tel Aviv can serve as a model for the proper application of IT-related tools in this area.

As well, there is a trend toward trying to eliminate the breeder document, especially the birth document, through the direct linkage of source databases. Here I'd like to cite, in a very positive

" The bottom line is that the new generation of passports is the most secure travel document the world has ever seen. This should prove invaluable in shoring up the integrity of our border control programs—meaning that attention must now be focused on the systems for entitlement judgments and identity management. "

context, New Zealand for its work on linking birth and death and civil registry databases. They have chosen to go this route because it obviates then the need for reliance on the birth document.

As well, I'd like to underscore the work of the Netherlands for its impressive and comprehensive database approach. Their Document Information System for Civil Status, or DISCS, is a database with nearly 1,300 different examples of breeder documents, including birth certificates, death certificates, identity cards and so on. Officials who are working on entitlement judgments, as well as those who are responsible for inspection, have access and can look at what a legitimate identity document is supposed to look like.

The most mundane aspects of the flow and distribution of work functionalities can often be overlooked and therefore become susceptible to security breach. Especially onerous are family and other kinds of emotional connections. Again, this is somethingto which, unfortunately, our human resource is highly subject.

I can't over-emphasize the need for measures to enhance and sharpen the methods by which travel document applicants establish their bona fides. The interrelationship of civil registry records is very important, and once again I mention the New Zealand passport process as an example worthy of many of you to consider with respect to emulation. The 'social footprint' concept, which refers to the aggregate social references that the applicant provides, is also worthy of consideration here. Education, work history, ties to the community, tangible assets and similar kinds of indices can be weighed in this regard and assessed when arriving at a bottom line decision as to an individual's credibility.

To touch upon my own love-hate relationship with current technological availabilities for a moment, the affordability and practicalities of desktop publishing have all but revolutionized the ability and the ease with which personalization can be carried out.

The other side of this coin is that these same technologies are in sufficient availability to those who would abuse their capabilities. It's quite crucial that measures such as the explicit authorization of decision making be an integral component of the deployment of these kinds of technological capabilities.

Finally, though seemingly so obvious and therefore so often given short shrift by issuing authorities, are the security aspects of the document production facilities themselves. Given the increasing levels of reliance that we have on contractors, it is critical that these facilities have stringent and enforced requirements as part of the contracts and agreements that are reached to establish them in the first place. I might mention, as an example of an extremely positive approach, the Belgian passport that's being produced at a facility I visited inLisle, France, where the facilities are extremely secure and the requirements and conditions for those facilities are clearly spelled out in the contracts that have been established to produce those passports. I suggest that everyone here consider similar kinds of measures for their own facilities.

There's no question that the security of an identity document issuing authority, whether it's for a drivers license, something that is associated with access control, or a passport, depends primarily on its staff. Good staffers are essential to the success of any document issuance operation; conversely bad staff can make any system, no matter how modern, efficient, or finely tuned, fail and fail miserably. From selection through appraisal, rewards and penalties, it is important that the human element of the document-issuance operation receive constant and high-level attention, from both a positive as well as negative perspective. I can't over-emphasize enough the importance of that elusive and intangible called 'morale'. Unhappy and/or disgruntled staff can cause immense harm to any operation. If they're of a mind, the kinds of sabotage that can befall a system can be catastrophic. Just as the staff know the system best and can make it work best, so too are they most conversant with the soft spots of its vulnerability and weaknesses and in the best position(s) to take advantage of them.

Another line item that I feel needs to be explored more thoroughly is the legal framework on which document-abuse resides. This is really of pivotal importance. I took great pleasure a while back in the announcement of the UK on increasing penalties for the deliberate and wilful misuse of personal data as an integral component of the trend toward enhanced data sharing. The Data Protection Act has been quite a dull deterrent. This initiative has as its premise that greater data sharing has—and these are quotes from the UK release itself—"... hugely beneficial aspects for the public good and is wholly compatible with respect for individual privacy."

I also need to mention the dampening and deterrent effects of strong measures for breaches and violations. The kinds of 'slap on the wrist' that have been employed over the years and, unfortunately, still continue to be employed, really provide very little deterrent to individuals. To cite one example from my own state, seven of the 19 terrorists who were responsible for the tragic events of 9/11 obtained actual Virginia drivers licenses from one corrupt motor vehicle department staff member for a mere US$100 each. That individual received very, very light penalties and this sort of situation simply cannot go on. I know that a number of countries are now moving in the direction of additional and much tighter penalties. I urge all of you to work within your own respective states and have these measures urgently approved.

Lost and stolen. I single this out here because the US 9/11 Commission identified lost and stolen passports as the single greatest source of illegitimate documents in the hands of terrorists. Remember the quote that they had in that same travel document section of the 9/11 Commission report that, quote: "A false passport in the hands of a terrorist is as dangerous as a bomb."

I'd like to add a quick note on centralized versus decentralized organizational structures, which is an area that needs to

Who's behind?

ePassport, enrolment, issuance, border control and more… from Gemalto

Gemalto is a reliable and trusted partner for all your public sector ID initiatives including ePassports, eVisas and other international and national identification schemes as well as healthcare and social security programs.

We offer a complete range of secure solutions that are tailored to local markets, and we deliver what you want where you want it with the support of a strong network of local partners.

Gemalto relies on 120 years of experience in secure printing, and our unique expertise in digital security means we provide innovative, trusted solutions that you can count on.

Gemalto's ePassport references include the Czech Republic, Estonia, Denmark, France, Latvia, Norway, Poland, Portugal, Italy, Singapore, Slovenia, Sweden and the United States of America.

gemalto
security to be free

be looked at with great scrutiny. The trade-off between customer service and security, for example, must be assessed in concert with the other factors that lead to organizational determinations. And I caution here, especially to those who are looking at issuing passports at embassies, please give ample thought to the idea of handing over complete passport accountability responsibilities to overseas offices and personnel. This type of satellite authority is fraught with vulnerabilities that, although capable of a certain degree of control, in general heighten security risks in geometric proportion to a centralized system

Which brings us to a quick summary of the generic nature of threats. Reference Slide 3 *(below, top)* categorizes the various threats and the kinds of areas that you need to be cognizant of in assessing potential weak points. More specifically, there are a wide variety of threats to which travel documents are vulnerable: this slide lists just a few broad examples and each one of these can take on a number of different forms. The third bullet has received, and will continue to receive, greater attention in my presentation. The final bullet, I think, points out the urgent need to provide training for individuals who will be responsible for receiving the documents. These are individuals not necessarily in the travel document assessment business at all, such as car rental agents, bank clerks, building guards, etc. This increasing use of passports for non-travel identity management is with us now and therefore training these individuals is critical.

REFERENCE SLIDE 3: NATURE OF SPECIFIC THREATS

- Counterfeit documents.
- Theft of blank documents.
- Malfeasance, nonfeasance, corruption.
- False identity—using genuine evidence obtained improperly to obtain a genuine document.
- False identity—using manufactured evidence of support to obtain a genuine document.
- False identity—using lost or stolen already-issued genuine documents.
- Multiple issuance/multiple identities.
- Increasing trend to use of passports for non-travel Identity purposes.

REFERENCE SLIDE 4: SECURITY DETECTION AND UPDATING (NOTED FROM REAL ID)

Detection of security features can be at any or all of the following three levels of inspection:

- Level 1 – Cursory examination for rapid inspection at the point of usage (easily identifiable visual or tactile features)
- Level 2 – Examination by trained inspectors with simple equipment
- Level 3 – Inspection by forensic specialists

To maintain security and integrity of document security, annual reviews of card design should be conducted to certify the document's ability to resist compromise and document fraud activity attempts:

- Photo substitution
- De-lamination or other effects of deconstruction
- Reverse engineering of chip as well as other components
- Modification of any data element
- Erasure or modification of other information
- Duplication, reproduction or facsimile creation
- Effectiveness of security features at all three levels: cursory examination, trained examiners with simple equipment and inspection by forensic specialists
- Confidence and ease of second level authentication purposes.

These points *(see Reference Slide 4, below, left)* came up last week at a conference that I was associated with dealing with the Real ID Act, which is US legislation involving standards for driving licenses. I thought that these points were very succinct, very nicely summarized and I thought I'd put them on this slide for the benefit of this conference's attendees. I was especially taken with the striation of the three levels of inspection and then the kinds of flaws that can occur therein.

Which takes us to what I hope will be, in all of your operations, a conscious model of risk analysis—one that must be designed to meet your own organization's specific requirements *(see Reference Slide 5, page 11)*. In this regard, one size absolutely will not fit all. The bullets call out some of the thinking that I've been associated with in respect to the EU concept of risk analysis. My advice here is to take a look at the concepts behind these factors: I think they're worthy of adoption.

These bullets *(see Reference Slide 6, page 12)* call out a few of the measures that any passport system can derive benefit from. I'm not pompous enough to presume to tell anyone here what their specific system may or may not need, but in a general sense I would offer these points for your consideration with respect to what might be termed 'best practices'. One might expect that the first and second bullets would currently be employed by all issuers—they are not. Certain aspects are now being carried out—but in truth

precious few and far between. The risk analysis management program can be carried out in-house, via contractors, or using a combination of the two. I urge, strongly, that all issuers at least begin to take responsibility for some of these requirements. My personal advice would be to employ a process where consultants are used to objectively identify the challenges, vulnerabilities and threats, while the issuers themselves assign probabilities of compromise, chart the likely effects and impacts of successful attacks, and assess the likelihood of these scenarios becoming a reality.

Please note that there is no single formula that can work for all countries all the time. The security and related measures must be tailored to the specific context and characteristics of a particular issuing authority. Standards and best practices can point the way, and case studies can also be shared between issuers to help identify successes and failures, but in the end each issuer has got to develop and structure systems and procedures which meet their own requirements.

I've provided this list of best practices that were developed by the Smart Card Alliance *(see Reference Slide 7, page 12)* specifically with respect to chips, but I was struck by the fact that it can almost be directly applied to the use of biometrics as well. I'm associated with the ISO SC37 Biometric Group—where we're now working on privacy issues. These areas of focus, best practices if you will, are very useful for those of us who are now implementing biometric systems.

REFERENCE SLIDE 5: RISK ANALYSIS FRAMEWORK

- For example, Frontex, an EU organization specifically intended to conduct risk management analyses.
- To identify key threats and risks to border security.
- To provide the Member States' border guard services with systematic and immediate early warnings.
- To identify the most appropriate potential locations for the positioning of technical border control equipment.
- To identify the need for joint operations.
- To assess the most effective focus for Border guard training programs.

The six areas of focus in this list *(see Reference Slide 8, page 12)* call out the themes that were developed at a recent Border Control Summit. This list is not presented in order of priority. Issuers need to determine which biometrics they wish to employ, separately or together (fingerprints, fingerprints and face, etc.), and the associated costs and pragmatics of implementation. I won't go into further detail on these areas except as concerns the bullet on information sharing. Civil registry systems are especially critical in this regard as a wide variety of entitlement—particularly passport—decisions now revolve around the information contained therein.

Finally, a few areas of longer term consideration:

Chips: I think we've done a great deal of work with respect to the 14443 contactless chip. We've certainly learned a lot. But there are also new lessons emerging with each new deployment. That's why any Supplement to 9303 is something to keep your eye on because if there's one place where these lessons will be collated and shared, it will be in an ICAO 9303 Supplement.

Enrolment Systems: This is THE current and most pressing area of vulnerability afflicting most of the world's issuing authorities.

Biometrics: I think the area of biometrics has begun to realize some of its long-promised potential. I think we've come quite a long way with the use of biometrics, not as a panacea, but as a tool—a long way from the hype that emerged during the aftermath of 9/11. I think that now, finally, biometrics are beginning to realize their promise.

Inspection Systems: This is the least mature area of focus and certainly where the rubber hits the road. We CANNOT allow another eight year timeframe for inspection system development with respect to OCRB; we must move much more quickly.

The bottom line is that the new generation of passports is the most secure travel document the world has ever seen. This should prove invaluable in shoring up the integrity of our border control programs—meaning that attention must now be focused on the systems for entitlement judgments and identity management. ■

REFERENCE SLIDE 6: BEST PRACTICES

- The fundamental first step for system integrity is to conduct a comprehensive risk analysis and THEN construct a risk management profile; this is particularly critical for assessment of the biometric data collected and its uses.
- Use standards to define requirements that must be addressed as minimum specifications both for technical soundness as well as adherence to quality control.
- Insure that all aspects of the biometric system(s) are thoroughly understood by all involved, especially the staff on the line and those affected by its administration.
- Make extensive use of the tools of technology, e.g., rules-based adjudication software.
- Overseas issuance is higher risk with inherent differences of culture, infrastructure, external pressures.
- Fraud prevention programs-detection, deterrence, follow-up, information sharing.
- Database linkages and data sharing are multiplicative in impact and become especially powerful tools when combined with biometric data.
- Monitor and audit document inspection processes as well as document issuance and entitlement authorizations.

REFERENCE SLIDE 7: SMART CARD ALLIANCE RFID BEST PRACTICES

- Implement security techniques, such as mutual authentication, cryptography and verification of message integrity, to protect identity information throughout the application.
- Ensure protection of all user and credential information stored in central identity system databases, allowing access to specific information only according to designated access rights.
- Notify the user as to the nature and purpose of the personally identifiable information (PII) collected—its usage and length of retention.
- Notify the user about what information is used, how and when it is accessed and by whom, and provide a redress mechanism to correct information and to resolve disputes.

REFERENCE SLIDE 8: ISSUES FACING BORDER CONTROL TODAY

- Biometrics.
- Enrollment and other systems.
- Profiling.
- Information sharing.
- Privacy and data integrity.
- New visions.

A Guided Evolution

WE TAKE FOR GRANTED THAT PASSPORTS AND RELATED TRAVEL DOCUMENTS ARE THE MOST RELIABLE MEANS OF ESTABLISHING BEARER IDENTIFICATION, BUT THE TRUST THE WORLD PLACES IN THESE DOCUMENTS WAS ONLY MADE POSSIBLE BY A LONG AND DETAILED PROCESS INITIATED AND MANAGED BY ICAO, OFTEN IN CLOSE PARTNERSHIP WITH THE ISO. MARY MCMUNN, FORMER CHIEF, FACILITATION SECTION AND MANAGER OF THE MRTD PROGRAM, DESCRIBES THE ORIGINS AND AMBITIONS OF THIS WORK, THE LEGAL AND REGULATORY BASIS FOR ICAO'S IMPORTANT ONGOING ROLE, AND THE CHALLENGES THAT REMAIN AHEAD.

MRTD Report: How did ICAO originally become involved with setting the standards surrounding machine readable travel documents (MRTDs)?

Mary McMunn: ICAO took the initiative on MRTDs and continues to do this work because civil aviation has three major, vested interests in standardized secure travel documents. The first of these vested interests relates to international air travelers and the fact that they need to carry passports or internationally-accepted IDs for inspection by immigration and customs officials. These border controls take place in airports and hence are integral to the international air travel system. This fact is recognized in the Chicago Convention in articles 10, 22, 23 and 37, which together require compliance with passport regulations and address the need for standardized procedures to facilitate air transport-related border control activities and prevent unnecessary delays. Article 37 to the Convention specifically provides the mandate that ICAO develop and maintain standards for customs and immigration formalities, which the Organization has provided for in Annex 9.

How did this responsibility evolve specifically into the area of MRTDs?

Over the years ICAO has held, on a semi-regular basis, a "Facilitation Division"—a worldwide conference that meets to update and upgrade the provisions of Annex 9 based on new technological or regulatory developments. In 1968 this conference recommended that a "Panel on Passport Cards" be set up in ICAO to develop a standard, machine readable document for use by travelers. The reason for this was that wide-body aircraft were about to come on the scene, and it was foreseen that passenger numbers would increase dramatically as a result, not only in a general sense but also on a flight-by-flight basis, which would have serious impacts on airport and border control processes and infrastructures. At that time there were about 200 different styles and shapes and sizes of passports with every country doing its own in a unique way, and so immigration inspectors needing to make a decision in a reasonably short amount of time as to whether these passports were valid or not had a daunting task before them. Standardization and machine readability were seen as the solution to the problem.

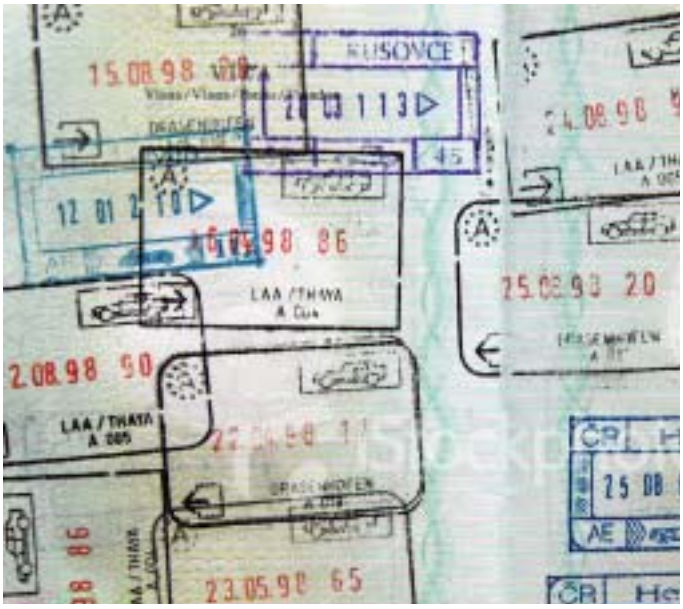
You mentioned three vested interests earlier—would you also like to touch upon the other two?

The second vested interest that I'd like to discuss is the involvement of the airlines in the document inspection process. National legislation in destination countries generally holds aircraft operators responsible for ascertaining that passports and visas are genuine and valid before allowing travellers to board an international flight. If an airline lets a passenger on a flight with an invalid document it can be subject to penalties and fines. A standardized machine-readable travel document facilitates the operator's inspection task and it also facilitates the collection of what has become known as advance passenger information, which is becoming a requirement of a growing number of major destinations to serve their national security interests.

This brings me to the third vested interest, which is the link with aviation security. All passengers are now required to show an ID at security checkpoints, and security officials must obviously be able to rely on an internationally-standardized document such as a passport to minimize opportunities for malefactors to use fraudulent documents, or somebody else's documents, to get on a flight. If non-standardized international or national ID-types were prevalent in this context it would obviously be difficult, if not impossible for security officials to carry out their responsibilities effectively.

This describes the originating context and mandates very well for our readers. Would you also care to shed light on more recent ICAO decisions or resolutions that helped to shape the development of the MRTD program since that time?

Following on the impetus that evolved out of the 1968 conference, and which progressed steadily during the ensuing decade as Contracting States began to understand and react to these new



needs, in 1980 ICAO published its first specification for what was called a 'passport with machine-readable capability'. This specification prescribed a document that looks very much like the machine-readable passport of today—a little bit less refined perhaps, but it had the same machine-readable zone of OCR characters and a photo of the bearer on the same page, as well as information about where the document was issued and the personal details of the bearer. In and around 1986 a partnership began to develop between the ISO and ICAO under the leadership of the Air Transport Committee, whereby an ISO working group would provide engineering consultancy to a new Technical Advisory Group regarding the physical composition of the passport, as well as guide the ICAO specifications through the necessary process to have them endorsed as ISO standards. The ICAO group in question was referred to as the TAG/MRP—the Technical Advisory Group on Machine-Readable Passports, and was comprised of passport and immigration experts from, as I recall, seven countries.

How did this partnership evolve over time? What sort of results emerged from the work of the TAG/MRP?

Over the next eight years the terms of reference of this TAG were expanded to cover visas and cards for international travel, as well as passports. The group was renamed the TAG/MRTD to reflect this change, and its membership began to grow. And so the specifications for machine-readable visas and international travel documents were developed and published, and specifications for machine-readable passports were updated twice during that time. In the mid '90s the liaison relationship between ICAO and the ISO intensified at the working level and ISO representatives began taking an active part in the technical working groups. This has been extremely helpful, both to the development of new technology specifications and also to resolving format issues in areas such as languages, presentation of names, transliteration of national characters, printing fonts, image quality and the arrangement of data in zones on the passport data page. The specifications for ePassports, featuring digitized data in contactless chips, have particularly benefited from this partnership due to their highly complex, technical nature.

And when did this move toward ePassport specifications begin?

In 1995 the TAG/MRTD started looking for ways to enhance the capability of a travel document to confirm the identity of the passport or ID card bearer. Photo ID in passports had served the aviation and security communities reasonably well up until this point, but with new technologies emerging it was felt that there might be a way to make identity confirmation even more robust. Considerable time, therefore, was spent studying possible options for biometrics and proposing specifications for an array of data storage technologies to supplement the machine readable zone, until finally we settled on the contactless chip.

The program got a big boost when the 1998 ICAO Assembly passed a resolution calling for increased international cooperation to protect the security and integrity of passports and other travel documents. This resolution has been updated and fortified in more recent Assemblies, especially in the wake of the security concerns that emerged after 9/11. The 2007 Assembly again resolved that ICAO was to continue its work in the areas of identity management and improving the security and integrity of passports.

How do you view the progress that has been made since this initiative began?

In 1997 fewer than 20 countries were issuing machine-readable passports. It was still a new concept to many States and viewed as being almost an expensive 'luxury' of developed countries. Since then, however, the number of countries increased very, very quickly, if only because countries were recognizing the compelling advantages of machine-readability and basic standardization, as well as the fact that, as countries went through the usual cycle of passport renewal and issuance, it simply didn't make sense not to incorporate these very obvious and increasingly more cost-effective improvements. Therefore by 2004 well over 100 countries were issuing machine-readable passports, and that's when the decision was agreed by all the Member States that issuance of machine-readable passports must become mandatory by 2010. By that time the consensus had been achieved that universal implementation of MRTDs was essential to the security of the international air travel system, but in as much as travel documents are now considered to be the most trustworthy method of establishing ID in virtually any context, I feel that our work has been very successful not only in meeting the needs of civil aviation and immigration/customs but also in bolstering aviation security.

Yet the big winners in all of this are the "peoples of the world"—the primary beneficiaries of ICAO work. Travelers now have

" We now have to address the processes around the development and issuance of the passport; namely the entitlement processes that determine whether or not a document should be issued to a particular person or not, as well as the circumstances under which the document is physically produced and issued—to make sure that fraud is not committed during these stages either. This represents a significant but not insurmountable challenge, and one that I'm sure will be addressed with the same expertise and resolve that has brought us to the point we're at today with respect to the document itself. "

readily recognizable, universally accepted travel documents, the best-ever protection against identity theft, and access to shorter inspection lines.

Could you sum up for our readers where we stand today and what you feel are the most important challenges that lie ahead?

ICAO needs to continue work in assisting states with implementation of the standards and produce additional guidelines, particularly in the area of what's come to be known as identity management. We can be very proud of ICAO's success in developing an advanced and secure document that soon will be issued by virtually every country in the world, but we now have to address the processes around the development and issuance of the passport; namely the entitlement processes that determine whether or not a travel document should be issued to a particular person or not, as well as the circumstances under which the document is physically produced and issued—to make sure that fraud is not committed during these stages either. There is also an ongoing need to upgrade and enhance inspection procedures at airline checkin, security and border control points, in order to make full use of the technological advancements in modern passports and ID documents. This represents a significant but not insurmountable challenge, and one that I'm confident will be addressed with the same expertise and resolve that have brought us to the point where we are today with respect to the document itself. ■

The IATA Simplifying Passenger Travel (SPT) Program

By Arundhati Gupta
Program Manager, IATA SPT

THE IATA SIMPLIFYING PASSENGER TRAVEL (SPT) PROGRAM WAS INITIATED IN RESPONSE TO A "PASSENGER FRIENDLY FLOWS RESOLUTION" ADOPTED AT THE IATA ANNUAL GENERAL MEETING (AGM) IN 1997. ITS GOAL THEN AS NOW IS TO IMPROVE PASSENGERS' TRAVEL EXPERIENCE. TRENDS AT THAT TIME SHOWED STRONG AND CONSISTENT GROWTH IN AIR TRAVEL, AND STAKEHOLDERS WERE OF THE COMMON VIEW THAT NEW AND INNOVATIVE MEASURES WOULD HAVE TO BE IMPLEMENTED TO COPE WITH THIS CONTINUOUS GROWTH IN TRAFFIC.

The Simplifying Passenger Travel program's vision was modified after September 2001 to include a strong focus on security aspects, while still endeavoring to enhance and streamline the overall end-to-end passenger travel experience *(see Fig. 1, below)*.

FIG. 1: THE SPT VISION

To measurably improve the passenger experience and enhance security by:

- Implementing new technologies.
- Sharing information amongst service providers.
- Enabling more efficient controls and services.

SPT Board and Interest Group

SPT is comprised of a board representing the various stake-holder groups and a separate "SPT Interest Group" that includes a broad range of public and private entities. IATA, acting as the secretariat, manages the SPT Program and is supported in its day-to-day activities by an elected chair and vice chair. The current SPT Secretariat is made up of Program Manager Arun Gupta and Program Director Georgina Graham. The current Chairman of SPT is Kevin Molloy of Vancouver International Airport, while the Vice Chair is Nina Mitchell of IATA.

The SPT board acts as the keeper of the SPT vision and consists of international organizations representing all industry

stakeholders. IATA is one of 13 organizations that make up the permanent SPT board membership.

The SPT Program has built a unique and multi-sectoral membership consisting of airlines, airports, control authorities, ground handlers and technology suppliers—all working toward the common goal of simplified and secure passenger processing. Together this group is committed to make the SPT vision a reality.

The active involvement of government border control agencies in the SPT work program is considered an essential component of the SPT's success. Government agencies of Australia, Austria, Bahrain, Canada, Chile, France, Hong Kong, Japan, New Zealand, Netherlands, United Arab Emirates, United Kingdom and the United States all participate in the ongoing work, and are full members of the SPT Interest Group (SPTIG).

Ideal Process Flow

SPT advocates the use of technology to automate key parts of the airport process, freeing up valuable resources, reducing costs and quantifiably enhancing security. In this regard the SPT Interest Group has developed the Ideal Process Flow (IPF), a high level schematic of the passenger experience describing the 'ideal' way of completing the steps involved in air travel, from the moment a passenger books a flight to their arrival at destination. The IPF is based on existing international standards, the sharing of data and use of emerging technology. A complete copy of it can be downloaded from the SPT website at: http://www.spt.aero/about.

The principal objectives of the Ideal Process Flow are to:

- Provide guidance to stakeholders involved in developing passenger
- Promote streamlined passenger processing through a real-time automated exchange of data between service providers.
- Increase security through better identification of passengers.
- Stress the importance for collaboration among all stakeholders.

The IPF defines each step of the passenger process, including departures, transfers, arrivals, and the movement and control of checked baggage. It considers both the experience of the passenger and the roles and responsibilities of government authorities, airports and airlines that may be involved in the journey.

Ideal Process Flow (IPF) Model

The IPF assumes that a passenger will have the choice of making a reservation online, and then checking in for the flight using a web site, a mobile device or a kiosk. He will use an ePassport that enables his identity to be checked using a biometric. His details will be automatically sent to government authorities that require passenger information for the journey (departing state, transit state(s) and at destination). To enhance aviation security, the airline will receive an automated real-time response to board the flight (or not), based on pre-departure data submission.

Once at the airport, to ensure that only bonafide passengers enter the restricted area, the passenger will authenticate his identity by means of a biometric identifier. At the boarding gate, a boarding token and biometric authentication confirms that the passenger has the "right to board" and is the person to whom the boarding token was issued. Additionally, the automated boarding control process will ensure that all persons who have checked baggage have actually reported to and physically boarded the flight.

Similarly, on arrival, a biometric comparison is used to authenticate the passenger's identity, allowing for automated and fully secure self-clearance processing at the border.

The use of technology and improved workflow in the example above demonstrates how the passenger's journey can be improved, security enhanced and manual intervention reduced. The IPF provides a win-win solution in responding to increased traffic passing through a constantly evolving airport environment.

Realizing the Vision

There have been many trials conducted on various elements of the travel process by a number of stakeholders as part of the SPT program. These 'proof of concept' trials have been a critical

EDAPS

CONSORTIUM

The new passport that Ukraine started issuing to its citizens in july of this year combines multiple features – not only does it have an interesting graphic background design, but its production employs state-of-the-art digital technologies.

The new document has a high level of security, and it fully complies with the international civil aviation organization (ICAO) requirements for machine readable travel documents.

The main feature of the passport is its personal data page made of multilayer polycarbonate and located inside the passport booklet pursuant to Doc 9303 guidelines. The advantage to using a new material is that, in addition to the traditional methods of document protection (background interlace patterns, guilloche, micrographics, secure ink), one can use brand-new methods of recording the owner's data. This primarily affects the main biometric identifier – the owner's facial image, which is recorded onto the page by laser engraving, and is then duplicated by laser perforation. The resulting black-and-white image has a high resolution, which provides a clear view of all facial features and makes the image easy to perceive. In the process of engraving the polymer structure undergoes irreversible changes, which makes the data impossible to counterfeit. This is the primary security measure undertaken by the government to prevent counterfeiting.

EDAPS CONSORTIUM BEING A SYSTEM INTEGRATOR, DEVELOPS AND IMPLEMENTS COMPUTER-CONTROL RECORDING AND INFORMATION MANAGEMENT SYSTEMS IN ALL SPHERES OF GOVERNMENT AND PRODUCTION ACTIVITIES THAT ALLOWS US TO OFFER "TURN-KEY" SOLUTIONS UTILIZING STATE OF THE ART INTEGRATED PRODUCTS.

The EDAPS Consortium:

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

The passport's design deserves separate attention, since it reflects the image of its owner, the Ukrainian citizen. The new passport's graphic design is based on the Ukrainian national theme, which includes ornaments and heraldic images from various regions of Ukraine.

Each page is designed to reflect a particular region of the country. The pages are framed with a non-repeating design of ornaments, adorned with regional coats of arms.

The passport's background is filled with micrographics and special raster elements, added with specialized computer software.

Passport protection includes printing with secure inks visible in ultraviolet light for quick document verification, as well as inks with double security effect.

Both the new Ukrainian passport and the systems solutions developed and implemented by the EDAPS Consortium and the Ukrainian Ministry of Internal Affairs are in full compliance with the latest international requirements.

EDAPS will be able to implement in a timely manner any additional biometric identifiers whenever the world community and the government of the country issuing the passport approve the technical parameters for such additional identifiers.

WE CAN PROVIDE THESE SOLUTIONS AND PRODUCTS IN A VERY COST EFFECTIVE WAY FOR YOUR GOVERNMENT OR PRIVATE SECTOR PROJECT. CONTACT US TO LEARN MORE!

Address:
64, Lenina Str.
Kiev, Ukraine, 02098

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

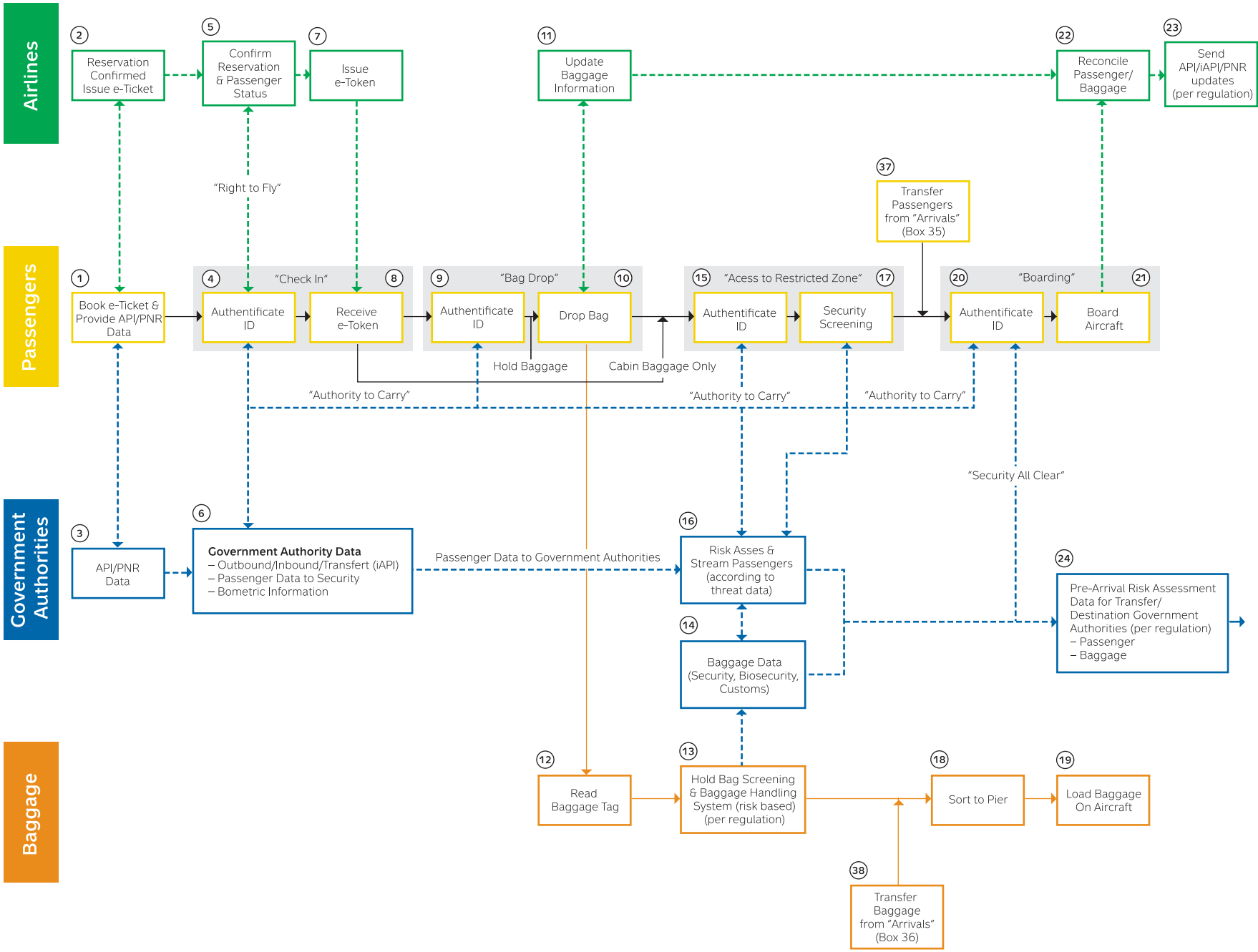
Fax:
+38 (044) 561 2585

E-Mail:
edaps@edaps.biz

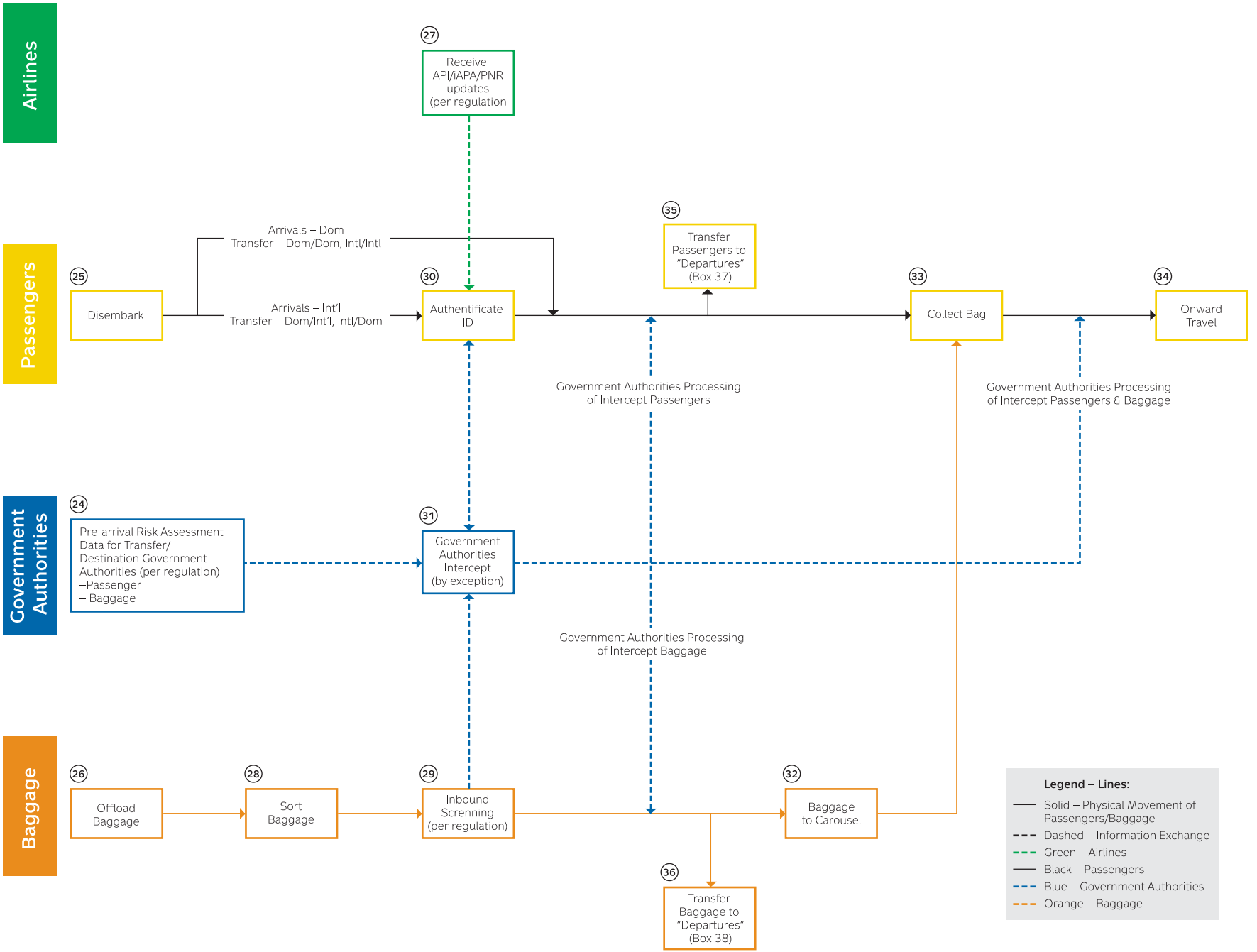
WWW:
http://www.edaps.biz

Fig. 2: Schematic of Ideal Process Flows for Departures and Arrivals

Departures – IPF v 2.0



Arrivals – IPF v 2.0



learning experience and have provided the necessary validation before these concepts could be rolled-out in a live environment.

SPTIG members from the United Kingdom and Hong Kong were among the first countries to test the concepts put forward in the Ideal Process Flow, by incorporating the new concepts and processes into the *miSense* and *SPEED* trials, respectively. The results have shown that multilateral co-operation between stakeholders is critical to the success of this sort of initiative. Feedback from passengers, staff and government authorities has been extremely positive, and lessons learned from the trials are of great value in supporting future development.

" SPT advocates the use of technology to automate key parts of the airport process, freeing up valuable resources, reducing costs and quantifiably enhancing security. In this regard the SPT Interest Group has developed the Ideal Process Flow (IPF), a high level schematic of the passenger experience describing the 'ideal' way of completing the steps involved in air travel, from the moment a passenger books a flight to their arrival at destination. "

Stakeholders acknowledge the need to achieve a critical mass of users in such initiatives. They also realize that educating the traveling public about the changing airport environment and the opportunities and benefits that new technologies can offer will be essential in efforts to strengthen passengers' acceptance of newly-introduced automated processes. Without such broad public acceptance, government agencies will be less likely to adopt the new processes as part of their normal operating activities.

Breakthroughs in international agreements on technologies, such as ICAO's adoption of facial recognition as the globally interoperable biometric for integration into passports and other machine readable travel documents (MRTDs), global adoption of IATA's e-ticket mandate, enhanced reliance on CUSS (Common Use Self Service) terminals, the introduction of bar-coded boarding passes and RFID baggage tags are all individual but significant steps toward achieving harmonization in an entirely new airport environment.

Success of these new technologies is almost entirely dependent on broad public acceptance, which can only be realized in the presence of adequate and internationally-agreed standards. Many of the necessary standards exist today, while others such as real-time, passenger-by-passenger interactive Advanced Passenger Information (iAPI) and government access to airline reservation records (PNR Access), have yet to be developed and internationally agreed. In the absence of such standards it will be difficult to ensure that the various elements of the IPF, as well as the technologies that will be introduced to make those processes work, will be able to be implemented in an efficient and globally-interoperable manner.

SPT will work collaboratively with ICAO and control authorities worldwide to promote the establishment of such standards and the adoption of the IPF as a model for the industry.

One of SPT's next steps will be to establish proof of interoperability between two or more countries (including airports, airlines and control authorities) collaborating on a cross-border trial. This next-generation trial will demonstrate that the use of pre-travel data collection, biometric passports or other e-tokens, automated check-in, baggage drop, security and boarding and bilateral or multilateral border control agreements can, and will, expedite a passenger through all aspects of normal border clearance processing on both inbound and outbound legs of a journey.

It is the goal of all SPT stakeholders to develop appropriate and efficient solutions that promote simplified and automated passenger travel. The fulfillment of this goal depends on collaboration between all industry stakeholders, the development and acceptance of international standards and international cooperation in the implementation of exciting new processes.

For additional information about the SPT Program and membership, please visit their website at: www.spt.aero. ■

The ICAO PKD: 2007 Year in Review

VALIDATION IS ESSENTIAL IF STATES ARE TRULY GOING TO CAPITALIZE ON THEIR ePASSPORT BORDER SECURITY INVESTMENTS, AND A PUBLIC KEY DIRECTORY (PKD) IS ESSENTIAL TO VALIDATION. ROSS GREENWOOD, ASSISTANT SECRETARY OF AUSTRALIA'S PASSPORT BUSINESS IMPROVEMENT AND TECHNOLOGY BRANCH AND 2007 CHAIRPERSON, ICAO PKD BOARD, ARGUES FOR THE BROADEST POSSIBLE IMPLEMENTATION OF A SCHEME OF ePASSPORT VALIDATION, AND FOR ICAO TO ACT AS THE LOGICAL BROKER FOR THE PUBLIC KEY DIRECTORY THAT FORMS THE SECURITY BACKBONE OF AN EFFECTIVE ePASSPORT SYSTEM.

The ICAO PKD commenced operating in March 2007. This article records the progress that has been made in the first year of the ICAO PKD.

An essential element in the introduction of ePassports is the implementation of a global system for ePassport validation achieved via the exchange of Public Key Infrastructure (PKI) certificates. The system is privacy enhancing. It does not require or involve any exchange of the personal data of passport holders and the validation transactions help combat identity theft.

The business case for validating ePassports is compelling. Border control authorities can confirm that the document held by the traveller:

- Was issued by a bona fide authority.
- Has not subsequently been altered.
- Is not a copy (cloned document).
- If the document has been reported lost or has been cancelled, the validation check can confirm whether the document remains in the hands of the person to whom it was issued.

As a result of these abilities, Passport issuing authorities can better assist border control authorities in all participating countries in identifying and removing bogus documents from circulation. The validation features noted also enable more effective identity automation and warning list checking of ePassport holders. Without PKI or alternative database validation checks, as well as traceable criteria to highlight lost and stolen passports, any such automation would be higher risk.

ePassport validation is therefore essential if States are truly going to capitalize on the investments they make when developing ePassports, both to contribute to improved border security locally as well as safer air travel globally. Because the benefits of ePassport validation are collective, cumulative and universal, the broadest possible implementation of a scheme of ePassport validation is desirable.

The exchange of PKI certificates (and the exchange of the certificate revocation lists that are the essential recovery layer in the system) must be reliable and timely. The emerging consensus is that this exchange cannot be achieved by other than electronic means, and that the system of ePassport validation must operate on an open ended, indefinite basis.

Engagement with Border Control Authorities

The primary beneficiaries of a global scheme of ePassport validation are border control authorities. While there is a broad acceptance of the importance of ePassport PKI validation in the passport issuing community, however, awareness of the issues is less developed within the border control community.

Around 40 States are now issuing ePassports. The number of ePassports in circulation globally is estimated at more than 100 million. For the early adopters of the technology, up to 40% of their traveling citizens can be expected to be ePassport holders. Traffic across borders is now approaching volumes where the large systems-integration investments required to support ePassport validation are viable. Once the tipping point is reached, demand for a central brokerage to support the exchange of ePassport PKI certificates will increase.

In the meantime there remains a communications challenge, and the PKD Board is now putting greater effort toward engaging with border control authorities. This is, however, a short term issue, as the growth in ePassport circulation will inevitably bring the question of how best to achieve ePassport PKI validation to the fore.

During 2007, members of the PKD Board and others engaged on their behalf were active in promoting the ICAO PKD in IOM's IGC, in the IATA-CAWG, in the OSCE, in the APEC Business Mobility Group and in a number of other fora where border control authorities meet.

Technical Design

After the technical design of the ICAO PKD was finalized, the United States made it a requirement for participation in the US-VISIT program that the Document Signing Certificate public key (C_{DS}) be included in ePassports. Subsequently, most ePassport issuing countries decided to include the C_{DS} on the chip in their ePassports.

Germany had been vocal in advocating changes to the design of the ICAO PKD, seeking new technical parameters that would improve security and simplify validation. The PKD Board finalized a compromise agreement with Germany on a European proposal for a modified approach to ePassport validation in October 2007. The changes, once implemented, will both improve and simplify the ICAO PKD, and their adoption has been the single most important achievement of the ICAO PKD during 2007.

Participation

The ICAO PKD currently has 8 members, of which 4 are active in uploading their ePassport certificates and revocation lists (Singapore, New Zealand, Japan and Australia). It is expected that Germany and the United States will commence certificate uploads early in 2008 and the United Kingdom later this year. Canada is not yet issuing ePassports and as such is not a candidate to upload certificates in the near term.

Early participation in the ICAO PKD has brought significant benefits for States who, in the early stages of ePassport implementation projects, have been able to learn from the experience of the early adopters. With annual fees becoming payable only after certificate uploads/downloads commence, membership ahead of ePassport implementations is expected to become more common, and Germany's membership is expected to be influential on other States.

Cost of Participation—Registration and Annual Fees

A number of countries have indicated that the ICAO PKD registration and annual fee costs are an impediment to membership. The fees that were initially set were not ideal in terms of being an incentive for early membership by larger States that are critical to ensuring a viable global scheme.

Subject to ICAO Council agreement, it is proposed that Registration Fees be reduced from USD 85,000 to USD 25,000. Annual fees are set by the PKD Board and in future will be set to recover the forward budgeted operating costs. A system of credits against future annual fees will be introduced to deal equitably with excess fee collections that will result from additional participants joining the PKD during the period after the level of annual fee has been set. Annual fees will therefore vary according to the number of participants. It is estimated annual fees could reduce to USD 20~30,000 per annum when the level of 20 participating States is reached, with the final cost levels to be determined once the terms of the operational contract are confirmed with Netrust, the external service partner.

Supporting ICAO in the Performance of their Broker Role

The PKD Board believe that a central broker is essential, and that the broker role must be able to be sustained and be trusted by the broadest range of States in order for the collective, cumulative benefits of the ePassport PKI validation system to be realized. ICAO is therefore the logical broker.

The ICAO PKD Board is responsible for operational and financial oversight. Success will rely on the Board being seen to be effective in this role.

ICAO appointed a dedicated staff member in September 2007 to ensure efficient and effective coordination of the uploads that are critical to the ePassport PKI validation system, and the newly appointed staff member is working in close consultation with the PKD Board.

Performance of the Third Party Service Provider

Netrust, a Singapore based company, was engaged by ICAO to build and operate the validation service. The close operational oversight of the PKD Board to date indicates that Netrust are thoroughly professional and competent in performing their role.

ICAO PKD—The Future

The Report of the 2007 ICAO Assembly urges those States issuing ePassports to join the ICAO PKD. The number of ePassports in circulation is approaching the tipping point where border control authorities will reap returns from investments in ePassport PKI validation. The PKD's founding participants, and the new members that have joined during 2007, believe that a central broker minimizes the volume of exchange of certificates and that ICAO, as the global agency responsible for travel document standards, is the logical broker for achieving a sustainable global scheme.

For all of these reasons, membership in the ICAO PKD is expected to grow strongly in 2008. ■

Profile: Chilean Identification Process and Immigration Control

WITH ONE OF THE WORLD'S MOST COMPREHENSIVE AND BEST-MAINTAINED CIVIL INFORMATION REGISTRIES AT ITS COMMAND, AS WELL AS A LAB NOW CONFORMING ITS BIOMETRIC RECORDS TO NEW ICAO STANDARDS, CHILE IS BECOMING A GUIDING EXAMPLE OF HOW STATES CAN ORGANIZE THEIR CIVIL INFORMATION SYSTEMS TO ENHANCE BORDER SECURITY AND ADDITIONAL NATIONAL NEEDS.

*The MRTD Report wishes to thank **Walter Montenegro Tapia**, Chief Information Security Officer, Civil Registration and Identification Service, Chilean Ministry of Justice; **Héctor Ulloa**, Deputy Commissary, Chilean Criminal Investigation Police; **Fernando Moya Castro**, Deputy Commissary , Chilean Criminal Investigation Police, and; **Marisol Cabello Moscoso**, Diplomatic and Official Passport Department Head, Consular Service Directorate, Chilean Ministry of Foreign Affairs, for their contributions to this submission.*

The Chilean Civil Registration and Identification Service (SRCel) is a public agency, functionally-decentralized with its own budget and legal status, and operating under the supervision of the President of the Republic of Chile through its Ministry of Justice. The SRCel service is composed of 15 Regional Directorates, 473 offices throughout the Chilean territory, an Internet office (www.srcei.cl), 13 mobile stations equipped with state-of-the-art satellite technology that bring citizens closer to the government, and 1 shipping office which travels the whole length of Chile's southern channels.

The SRCel assists 70 Chilean consulates working on-line with it to provide identification services, as well as working in coordination with the Ministry of Foreign Affairs, through the Diplomatic and Official Passport Department, for the issuance of said documents. Its main users are all Chilean citizens and foreign residents—who currently add up to approximately 16 million people.

Since 1884, the main duty of the SRCel has been to keep updated and fully operational a number of Chilean citizen registries (presently 26 types), including: birth; marriage; death; convictions (criminal records); motor vehicle permits; records of arrest; intestate actual possessions; DNA, and, most important of all; the identification registry.

The data volume handled by the SRCel is measured in millions of entries, with identification being the foremost category

accounting for over 16 million biometric entries (ten fingerprints plus one facial image per citizen). This information has been collected from nearly 100 percent of Chile's population.

Unique National Identification Number

Due to the large amount of citizen information that it must maintain according to law, since 1973 the SRCeI has established a unique national identification number or *Rol Único Nacional (RUN)* for each inhabitant of Chile. Any citizen-related statistical information is managed via their unique number, and it is also used for additional administrative purposes and activities such as the exercise of citizen rights, tax obligations, etc.

The unique national identification number is a lifetime identification given by the SRCeI to each person, upon registration of his/her birth. It is widely recognized and facilitates the conduct of private activities—as it is required by all public administration bodies, the Superintendency of Banks, insurance companies, public limited companies, stock exchanges, the Superintendency of Social Security, and any other public or private entities within the national territory.

Both the registration and identification activities of the SRCeI, facilitated by the unique national identification number, have created a synergy between such applications, permitting a fluent communication as well as a complementary interaction between them.

Products and Services

Besides updating the records as required by Chilean law, the SRCeI provides a number of services to supplement the use of identification and registration systems. Such services are directed to the citizens, police forces and additional private and public entities.

The main services rendered include:

Mobile stations for the issuance of certificates, identity cards and passports: These stations may operate either on- or off-line, within or without the Chilean territory, and with full autonomy to generate a document (in the same way and with the same tools as if they were a typical SRCeI office). Apart from these mobile stations there are also additional offices capable of issuing civil registration certificates, but these need to operate on-line with the SRCeI's central systems. Two types of technologies are available to assist in this regard: EDGE GPRS for locations with cell phone coverage, and; satellite technology for more remote locations. These services are available at hospitals, prisons, rural schools, Chilean communities abroad and remote Chilean locations, among others, and in both cases secure connection (VPN) with the SRCeI is required and achieved.

On-line supply of information to third parties: Another service provided is on-line information which is made available to entities having entered into an agreement with the SRCeI, such as the police forces (Carabineros and the Criminal Investigation Police), the law enforcement system, regulatory agencies (customs, treasury, internal revenue service), ministries, the State Defense Council, municipalities, concessionaires, health insurance companies (ISAPRES), among others.

Support to the criminal procedure reform: This system fully integrates the civil registry with the identification services by providing useful, segmented information to police forces and prosecutor's offices. According to the user's profile and by entering the unique national identification number (RUN), civil data may be obtained such as a person's name and surname, place of birth, parents, children, vehicle ownership, previous lawsuits, etc.

Identity verification system: This service is mainly used by police forces, which may verify, through on-line consultation with the SRCeI, the true identity of a person by simply entering the RUN-AFIS search parameter of that person. Currently this service is being extended to private companies, such as banks, in order to prevent frauds in the financial system.

Internet Office: This office provides services like civil registration certificate sales, the blocking of identity cards or passports and on-line verification of status updates for these and related requests. Certificates issued by the Internet Office bear an electronic signature. Chile already has a special law on electronic signatures, which makes a distinction between simple and advanced signatures. Advanced electronic

signatures are used on electronic documents requiring legal validity, and permits to validate, through the Internet, the accuracy of the document and the competence of the issuer anywhere in the world.

Status of System and Other Developments

At present, the SRCeI is going through a bidding process for a new identification system. With the selection of a successful bidder expected by the second half of 2008, the implementation should take approximately 18 months. The new system will be aimed at substantially improving identification procedures, and in particular switching from the present machine-readable passport to the newer ePassport. To this end enhanced technology and administrative processes must be developed to conform to ICAO standards and to enhance interoperability with other countries. The security of our current identification card will be also improved to make it consistent with these new standards In an attempt to provide a more accurate service, the SRCeI is currently setting up a biometric laboratory designed primarily to validate the current identification database and conduct research to determine whether the facial images and fingerprints now held by the SCReI conform to ICAO standards. The new lab will also set algorithm benchmarks for 1:N searches through the ID database and extrapolate response and performance times for all 16 million stored entries, improve the current search algorithms or propose more effective alternatives, and conduct on-line biometric validation tests to support other state agencies.

" As the information provided by the SRCeI is, in most cases, highly sensitive, service access is restricted through high security levels. Additional laws, regulations and decrees are also in place to help reduce threats to information integrity, availability and confidentiality. This is true for each process and system used by the SRCeI, whether for civil registration or identification purposes. "

As the information provided by the SRCeI is, in most cases, highly sensitive, service access is restricted through high security levels. Additional laws, regulations and decrees are also in place to help reduce threats to information integrity, availability and confidentiality. This is true for each process and system used by the SRCeI, whether for civil registration or identification purposes.

In addition to the foregoing services, the SRCeI keeps a close link with police forces through cooperation agreements, especially as regards identity control systems. The Chilean Criminal Investigation Police is entrusted with crime investigations and is the primary organization responsible for border control—supervising the entry and exit of individuals and the stay of foreigners in the national territory. This police force is currently detached to 82 emigration and immigration control posts for air, sea and land transit.

Technological Applications for Migration Control

In the discharge of its duties, the Chilean Criminal Investigation Police has introduced technology aimed at identity and document verification in support of the tasks performed by border control officials. This technology is based on state-of-the-art equipment designed to take advantage of the benefits afforded by the Chilean identification system. The system includes document verification by means of travel document authenticators equipped with electronic passport readers, determination of a document's validity and term, and the maintenance of databases of lost and stolen passports.

With respect to passport control, connection through the I-24/7 Interpol system with the Stolen and Lost Travel Documents (SLTD) database has recently been successfully implemented. The system makes use of fingerprint readers allowing access to national registries and facilitates the comparison of facial biometric features, which increases certainty about the identity of a passenger.

As emigration and immigration are dynamic processes requiring an adequate balance between the highest possible security standards and the expedited movement of people and goods through national borders, the Criminal Investigation Police have developed a comprehensive control system that balances these seemingly opposing objectives. This is primarily achieved through the establishment of specific high-risk categories that engage the full information resources available to the State when required, while lower-risk individuals can be expedited through a more streamlined procedure. ■

The EU's Path to Interoperability

THOUGH QUANTIFIABLY MORE COMPLEX FROM A LEGAL AND REGULATORY STANDPOINT THAN SIMILAR RESPONSIBILITIES FACING NON-EU STATES, THE EUROPEAN UNION'S PATH TO A 'SINGLE PASSPORT' AND SHORTLY TO A BIOMETRICS-BASED AND INTEROPERABLE ePASSPORT STANDARD, HAS PROCEEDED WITH ADMIRABLE PACE AND BENEFITED IN PART FROM ICAO STANDARDS ESTABLISHED IN THIS AREA. SYLVIA KOLLIGS, OF THE EUROPEAN COMMISSION'S GENERAL JUSTICE FREEDOM AND SECURITY DIRECTORATE, PROVIDES HER PERSONAL ACCOUNT OF THE EU'S COURSE UNTIL NOW AND ITS MOST SENSIBLE NEXT STEPS.

Footnotes may be found a article end on page 32.

At present, the commonly referred to "European Passport" is established on the basis of resolutions on the introduction of a passport of uniform pattern,[1] which are legally non-binding and which are comparable to political declarations by Member States.

The first of these resolutions was adopted in 1981 by the representatives of the governments of the Member States meeting within the Council (although outside the community framework) indicating that the creation of a uniform passport model "is likely to facilitate the free movement of nationals of Member States" and that Member States were "anxious to promote any measures which might strengthen the feeling among nationals of the Member State that they belong to the same community".[2]

On 8 June 1999 the German Presidency presented a draft resolution on the introduction of minimum security standards to protect EU travel documents from forgery, which was once again adopted as a resolution of the representatives of the governments of the Member States meeting within the Council on 17 October 2000. On this occasion the Commission made a statement in relation to the legal basis, considering that such a proposal should fall under community competence.

In its 2000/2001 annual work program the Commission included a proposal on making European travel documents more secure. It was multi-purposed: creating a "European Passport" with harmonized lay-out and common security features, a harmonized identity card for those Member States, issuing ID cards, a uniform format for residence cards delivered to EU citizens and members of their family, a uniform format for residence permits for third country nationals, an amendment to regulation (EC) No 1683/95 on a uniform format for visas, and introducing a photograph of the holder. Finally, the proposal also called for a standard form for affixing the visa issued by Member States to persons holding travel documents which are not recognized by the Member State. The objective was to have the same specific format and security level for all EU issued travel documents, making them more secure and facilitating border controls.

During the same time period, the Treaty of Nice was negotiated and Article 18 (3) was introduced into the Treaty. It stated: "Paragraph 2[3] shall not apply to provisions on passports, identity cards, residence permits or any such other

document or provisions on security or social protection." This removed the legal basis for the Commission to present proposals related to such issues for European citizens. The Commission consequently decided to reconsider the situation in relation to the presentation of proposals and in the end presented only the proposals related to third country nationals.

Following the events of 11 September 2001, enhancing security features in documents became a priority. Subsequently, the Commission presented three proposals: first, amending Regulation (EC) No 1683/95 laying down a uniform format for visas introducing the need for a photograph produced in accordance with high security standards; second, introducing a standard form for affixing the visa issued by Member States to persons holding travel documents that are not recognised by the Member State drawing up the form; and third, relating to a uniform format for residence permits for third country nationals. This made the joint action, adopted in the framework of cooperation among Member States, legally binding. At the same time a photograph of the holder onto the sticker version of the permit became mandatory. These proposals for regulations were welcomed by Member States and were rapidly adopted in February and June 2002.[4-5-6]

When the above-mentioned proposals were adopted, Member States saw a need to further enhance the security of travel documents by adding biometric elements. In a statement at the informal meeting of ministers in Santiago de Compostela on 14 to 15 February 2002, the Commission expressed its willingness to adopt such a proposal, but made clear that it would concentrate only on harmonizing the security features of the passport and, for legal reasons, would not alter the layout.

At the informal Justice and Home Affairs Ministers' meeting in Veria on 28 to 29 March 2003, Member States reiterated the need for a Commission proposal to integrate biometric identifiers into the uniform format for visas and residence permits for third country nationals. The Commission undertook to present a proposal, while emphasizing that a coherent approach should be taken in respect of all travel documents, including the passports of EU citizens.

Finally, the European Council of Thessaloniki, in June 2003, confirmed that "a coherent approach is needed in the EU on biometric identifiers or biometric data for documents for third country nationals, EU citizen's passports and information systems (VIS and SIS II)", and invited the Commission "to prepare the appropriate proposals, starting with the visa," In September 2003, the Commission presented two proposals on the integration of biometric identifiers into the visa and the residence permit for third country nationals.[7] As requested by the European Council of Brussels, a political agreement on the latter proposals was reached in the Council on 27 November 2003, At the same time, the mandate was given to the technical committee, created by Article 6 of Regulation 1683/95 on a uniform format for visas, to start working on the development of implementing these measures.

On 12 December 2003, the European Council of Brussels invited "the Commission to submit in due time a proposal for the introduction of biometric identifiers in passports."

The second step of the implementation of the Thessaloniki conclusions, the harmonization of the security features of the European passport (including the insertion of biometric identifiers), was presented shortly afterwards,[8] thus avoiding different solutions in each Member State together with an inevitable lack of interoperability.

Aim of the Proposal Related to Rendering Passports More Secure

It was neither the objective of the proposal to harmonize the layout of the passport format, nor to identify whether the passport had been issued to the right person in the first instance, as only Member States can verify the identity of an applicant at the time of issuing the passport.

Rather, the proposal was aimed at rendering the passport more secure via a legally binding EU instrument on minimum standards for harmonized security features. It would accomplish this while establishing a reliable link between the genuine holder and the document by introducing biometric identifiers.

> **" By June 2009 all EU Member States have to issue their new passports with a contactless chip —including the facial image and two fingerprints of the holder—protected by Extended Access Control. This is a major step forward in making the passport more secure by linking the holder to the document. "**

Minimum standards, which were set out by legally non-binding resolutions, did not seem to reach sufficient harmonization, as they were subject to different use and interpretation of the security features. Member States did not integrate all elements set out in the resolution and, in any event, during the five-year implementation period adopted industry would have produced new security features rendering the resolution of 28 October 2000 out-of-date. With respect to the photograph, it was noted that six Member States were still affixing it on the personal data page and were not integrating it during the personalization process by printing. This presented a high risk of falsification as it could easily be substituted.

Another important reason for the Commission to bring forward enhanced common security standards was to ensure that passports did not lag behind those standards already achieved by fixing the technical specifications for the uniform format for visas and for residence permits for third country nationals. Both uniform formats are constantly under review so that their high-quality standards parallel new technical developments and discoveries in the area of document security. The biometric identifiers for these documents had already been established (facial image and fingerprints). In order to ensure coherence and to avoid dishonest persons turning to the less secure passports of EU nationals, security aspects of the latter document had to be upgraded.

Finally, it was also believed that common security features would make it easier for border police to identify fraudulent documents. They could check some visible security features, present on all passports of the EU, and only in doubtful cases would they be bound to increase scrutiny. Because of the vast variety of security features in use at the time, border police had to check each passport against 25 national passports, which in turn contained different features and were of different quality.

It was also established that the biometrics to be integrated in the new passports should correspond to ICAO recommendations for them to be interoperable worldwide.

Legal Basis

Article 18 (3) prevented the Commission from presenting a proposal on a harmonized "European Passport." The objective of the proposal on harmonized security features and biometrics for passports, however, is to combat the use of false documents. Furthermore, the introduction of a biometric identifier, the facial image, enables the border police to make a thorough comparison of the person and the digital photograph. This makes border controls more efficient. Such a measure can be based on Article 62 (2) a) TEC.

In this respect, the legislative proposal could not go beyond the scope of this legal basis. The security of passports is important for reasons relating to external border controls: on the one hand, bona fide citizens will pass more smoothly through border controls; on the other hand, those who use forged or fraudulent passports will greatly decrease their chance of entering the territory of Member States. This is based on two basic elements of our area of freedom and security. For these reasons this proposal was based on Article 62 (2) a) TEC.

Minimum Security Standards and Choice of Biometrics

The Commission proposal was based on the security standards which were adopted by the representatives of Member States, meeting within the Council, in their resolution on minimum security standards for passports and other travel documents of October 2000. They were slightly "upgraded" in view of the technical developments relating to visa and residence permits. The proposal therefore set a harmonized, high-security standard for passports within the European Union. As in the resolution, the Commission sets out the minimum standards and will not prevent Member States from going further if they wish to do so.

> **" In June 2003 the European Council of Thessaloniki confirmed that "a coherent approach is needed in the EU on biometric identifiers or biometric data for documents for third country nationals, EU citizen's passports and information systems… "**

In accordance with the European Council conclusions of Thessaloniki, a coherent approach has to be taken regarding the introduction of biometric identifiers into the visa, the residence permit and the passport. The proposals in relation to visa and residence permits provide for two mandatory biometric identifiers: the facial image and fingerprints. Therefore, the proposal for European passports could only include the same mandatory biometric identifiers in order to ensure the coherence requested.

When choosing the most appropriate biometric identifiers, the results of the work of ICAO, which had taken the lead in the development of international standards in this respect, and the feasibility study on the visa information system (VIS), were taken into account.

It was also important not to lose sight of the need for a proper balance between the reinforcement of security and due regard for the individual rights of the persons concerned, notably the right to data protection and privacy, as guaranteed by Directive 95/46 EC and the national laws transposing it.

Standards and Technical Specifications for Security Features and Biometrics

The proposal on standards for security features and biometrics in passports and travel documents issued by Member States was adopted, after consultation with the European Parliament, on 13 December 2004 (Regulation (EC) No 2252/2004). As this measure is considered to build upon the Schengen acquis, all Member States except the UK and IRL participate. Norway and Iceland are associated, as will be Switzerland in due course.

Ministers agreed that the first biometric identifier, the facial image, should be implemented at the latest within 18 months, and that the second biometric identifier, also mandatory, at the latest

36 months after the adoption of the relevant technical specifications. These technical specifications were to be adopted by the Commission assisted by the committee created by Article 6 of Regulation (EC) No 1683/95 laying down a uniform format for visas (Article 6 committee), which is composed of Member States' experts.

The technical specifications were established in two parts: the first part relating to the integration of the facial image on a contactless chip in the passport; the second on the integration of the two fingerprints. The reason for the split was that the fingerprints were considered to be more sensitive data than the facial image and their protection should be ensured not only by basic access control (BAC), but extended access control (EAC). The EAC was not yet developped, and it was assumed that more time was necessary for this to be done.

The first part of the technical specifications was adopted by the Commission on 28 February 2005[9] and therefore biometric passports—including the digital image—were to be issued by all Member States at the latest on 28 August 2006.

Regarding the fingerprints, there were several technical issues to be solved, including the Extended Access Control chip protection profile and the certificate management policy. It therefore took much longer to establish the required technical specifications. In order to ensure interoperability, the experts of the Article 6 committee work closely with the relevant ICAO committees and working groups and are interested in developing and using common standards for EU passports.

The second part of the technical specifications, related to the secure storage of the fingerprints, was adopted on 28 June 2006[10] so that Member States have to implement them in their newly issued passports at the latest on 28 June 2009.

However, this work has not yet ended: all passports still need to be made interoperable. The Brussels Interoperability Group (BIG), a subgroup of the Article 6 committee was created for this purpose. Its task is to ensure the interoperability of all EU passports and the correct implementation of the technical specifications.

As some Member States have experienced problems with children's fingerprints, there was a request for introducing common exceptions from the requirement of fingerprints. On 18 October 2007, the Commission presented a proposal for an amendment of Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.[11]

The proposal aims to introduce exceptions from the requirement of taking fingerprints for children under the age of 6 years and for persons not able to give fingerprints, as well as the principle recommended by ICAO of "one person-one passport." The proposal is currently under discussion in the European Parliament and the Council.

Future Developments

By 28 June 2009, all EU Member States have to issue their new passports with a contactless chip—including the facial image and two fingerprints of the holder—protected by EAC. This is a major step forward in making the passport more secure by linking the holder to the document. The second step, which for obvious reasons should happen in parallel, is the equipping of all border posts with adequate readers.

Day-to-day experience in using the new technologies, however, still lies ahead *(ed. Note: for a profile of a new border control passenger throughput system, please see the article on Portugal's RAPID technology on page 32)*, and it may result in certain shortcomings. One concern is that with the use of biometrics in travel documents subsequent controls may focus only on the biometric features, when in fact they should be used in combination with the other security features built in the passport.

Another question is public acceptance. Citizens have to pay an increased fee for the biometric passport. They may agree that security has its price. The use of the biometric passport could, however, also be made more attractive through its use to facilitate border controls. Faster border passage systems such as a registered traveller system are currently being examined by the European Commission and some projects were already presented by Member States.

Furthermore, a new treaty, the Treaty of Lisbon, was recently adopted. It re-inserts the legal basis for the Commission to present a proposal in relation to passports: "If action by the Union should prove necessary to facilitate the exercise of the right referred to in Article 17b (2) a (free movement of EU citizens), and if the Treaties have not provided the necessary powers, the Council acting in accordance with a special legislative procedure, may adopt provisions concerning passports, identity cards, residence permits or any other such document." After ratification, the Commission may present a proposal on harmonizing passports in order to facilitate free movement, giving a real "European passport" to European citizens. ■

Footnotes

[1] OJ C 241, 19.9.1981, p.1.

[2] OJ C 241, 19.09.1981, p. 1-7.

[3] Paragraph 2: "If action by the Community should prove necessary to attain this objective" (free movement of citizens) "and this Treaty has not proved the necessary power, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1" (free movement of citizens).

[4] Regulation 334/2002: OJ L 53 of 23.02.2002 p.7.

[5] Regulation 1030/2002: OJ L 153 of 15.06.2002, p. 1.

[6] Regulation 333/2002: OJ L 53 of 23.02.2002 p.4.

[7] COM (2003) 558 final.

[8] COM (2004) 116 final.

[9] 28/06/2006. ©(2006) 2909. Commission Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States. http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm

[10] 28/02/2005. ©(2005) 409. Commission Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm

[11] COM (2007) 619 final.

A RAPID Success

THE PORTUGUESE RAPID SYSTEM REPRESENTS A BREAKTHROUGH IN PASSENGER THROUGHPUT, EMPLOYING STATE-OF-THE-ART CAMERAS AND LIGHTING IN AUTOMATED GATES TO PROVIDE ACCURATE AND EFFICIENT FACIAL RECOGNITION VIA ePASSPORT BIOMETRIC DATA—DOING SO MORE QUICKLY AND MORE EFFECTIVELY THAN HUMAN FACE-TO-FACE BORDER CONTROL VERIFICATION. THE ICAO MRTD REPORT IS GRATEFUL TO PORTUGAL'S DEPUTY DIRECTOR, SERVIÇO DE ESTRANGEIROS E FRONTEIRAS, MR. CARLOS GONÇALVES, FOR THIS COMPREHENSIVE UPDATE ON THE SYSTEM AND HIS ACCOUNTS OF ITS RECENT SUCCESS.

The Portuguese Electronic Passport (PEP) project was an incredible success story. Enabling a border control security breakthrough by promoting massive use of the country's new ePassport to cross the Schengen area at all the Portuguese international airports and seaports, the project's success has been facilitated by a new automated border control system, known as RAPID, which uses facial recognition technology to perform the same passport checks as a human immigration officer—in less than 20 seconds.

The RAPID system first went into service at Faro airport, serving the Portuguese Algarve region in the spring of 2007. Eventually rolled-out to all Portuguese airports and seaports, RAPID was inaugurated in Lisbon in August of last year, providing those travellers with biometric ePassports the opportunity to skip queues at border control. Travellers with ePassports can now walk up to an eBox gate, hold their biometric passport to a reader, and step through to a designated spot and look into a camera. If their identity is confirmed, the smart gate opens and they are allowed to cross the border without ever seeing a border control official.

In order to increase the global security of travellers and citizens, a large number of States have already issued millions of biometric ePassports to their citizens in the past few years. As additional countries continue adopt biometric technology to strengthen border controls and the security of their travel documents, RAPID can be seen as the first practical border control innovation for ePassport holders, no matter where they have travelled from or are travelling to.

The RAPID system was conceived by the Portuguese border control authority—Serviço de Estrangeiros e Fronteiras (SEF)—and was designed and produced by Lisbon-based company Vision Box. This is the first system worldwide to allow the automatic control of passengers who hold electronic passports, thereby removing the need for direct human action.

RAPID combines the operations of reading and checking electronic passports with an innovative feature for assessing the biometric data which operates an automatic door-opening device. On first pass this feature checks the authenticity of the ePassport, validates all data stored in the chip, and then cross-references data against the Schengen Information System and SEF's own databases. On second pass it appraises the passenger's identification by establishing a comparison between the photo stored on the chip and the image of the passenger captured at moment of presentation, automatically opening the passage door when both images meet the prescribed biometric criteria.

Faro airport was home to the original installation of the RAPID system. The experience gained at Faro was assessed by a team of experts and researchers from the Algarve University in order to guarantee an independent evaluation of the performance of the system.

RAPID allows for the entry of one passenger at a time, automatically adjusting the reading camera to the subject's height. It provides a significant boost to the efficiency of border control by reducing process times to an average of less than 20 seconds. The system is usually installed with several gates operating in parallel, providing traveller throughput rates that dramatically reduce the burdens confronted by border control employees, as well as the wait times previously experienced by passengers.

The original Faro installation was assessed by a team of experts and researchers from the Algarve University in order to guarantee an independent evaluation of the performance of the system. The choice of Faro airport was based on the fact that more than 80% of passengers travelling through it are either British or Irish passport holders, with an estimated 2.5 million UK citizens visiting Portugal every year.

Previous experiences with Portuguese ePassports, during which live enrolment-based processes were adopted by the

SEF, had already concluded that good enrolment rates guarantee good identity verification. The fact that most of the test population was coming from the United Kingdom, where the enrolment procedures for facial images for passports are not based on live enrolment standards, also allowed evaluators to assess the system under a worst case, warranty-less scenario for facial recognition systems to perform a successful live-match-to-chip operation for identity verification.

During the evaluation process, several aspects of the proof of concept were refined for assuring compliance with SEF requirements, namely False Acceptance Rates (FAR) and False Recognition Rates (FRR). Initially stated respectively as 1% and 7%, the figures obtained during the evaluation were in fact better than these levels. The currently operating RAPID systems come in at 3% for FFR.

RAPID is equipped with an integrated supervisory station that allows immigration and border officers of SEF to reliably monitor passenger identity and travel document validity. A single officer can easily supervise the operation of 5 to 10 gates simultaneously, providing back-up when needed for exceptional cases and guaranteeing the passenger flow with high quality-control standards.

It is recognized that the ePassport-based automated facial recognition verification, which achieves maximum FAR factors on the order of 0.001, currently outperforms human accuracy (FAR factor of approximately 0.05). Furthermore, it is now known that human facial recognition generally falls quite short on ethnically unfamiliar faces. The high resolution images of the live subject and the improved consistency of lighting and camera alignment are also key factors that help to guarantee high performance rates at the RAPID gates.

The background expertise achieved with the Portuguese ePassport project had already allowed the development team to conclude that adjustable capture conditions for lighting intensity and camera height were important factors for efficient facial recognition and identity verification.

The RAPID solution also integrates various intelligent analysis features in a digital video surveillance system made available to the supervisory officer, enabling a decision making environment for complex surveillance and control procedures. This feature also presents remote and simultaneous display of live and recorded images, provides an intuitive tracking of people, integrates cameras, sensors and alarms in interactive maps, and gives access to on-line content analysis with graphical alerts. The RAPID eBox gates are modular, present a very small footprint, and are compliant with high security requirements such as the DIN 18650. They allow a minimization of queuing time through better passenger flow, are integrated with several information systems (SEF, Schengen, etc.), enable a cost reduction for passenger handling and provide the user with a Self-Service Positive Experience.

Above the gates an explanatory video on continuous loop is presented to travellers on large monitor screens, providing instructions on how to use the system. Airlines flying to Portugal present the same video to travellers on inflight monitors.

No enrolment, additional application or registration is required to take advantage of the RAPID system. If a traveller holds a European biometric passport and is over 18 (Portuguese legal restraints), he or she can avoid the normal queues and make a beeline straight to the RAPID gates. Once inside it will take just a few seconds for them to securely cross the Portuguese border. ■

Document Security

Shifting Focus from the ePassport Itself

Part of a Series of Datacard Group White Papers for the Secure Document Issuer.

In the past, security threats have often focused on obtaining genuine passports after personalization, which could then be used by people modifying their appearance (look-a-likes) or by expert counterfeiters modifying the document. With ePassports this risk is virtually eliminated due to the securely-embedded biometrics stored within the chip.

The focus of future criminals will therefore shift to the other end of the supply chain, in particular the enrollment and issuance processes. The risks in enrollment alone are multiple, namely:

- Insecure and forged breeder documents allowing enrollment (i.e. an individual using a fraudulent MRP passport to obtain a 'renewal' electronic version—the legitimization of the fraudster).
- The subornation of enrollment officials through bribes or threats to allow enrollment.
- The capture and illegal use of enrollment equipment to submit details into the issuance systems.

Blocking these threats is no easy task. Setting up entitlement and credential checking as an on-line second stage process (outside of the control of the enrollment office) will go some way towards ensuring that enrollment systems are not a single point of failure for the system, however ensuring that the enrollment systems themselves are secure against attack, and that the communication between them and other government systems is secure, should be critical focuses for auditors.

With properly protected access control systems and secure (cryptographically protected) communications in place, it is then possible to use the enrollment station as the starting point in a tracking process for full and complete document management. This process should include not just the capture of the citizen's enrollment data but also complete information about the time, location and name of the authorizing enrollment officer. This data can be utilized for later investigative analysis if failures are detected.

Entitlement

Authorization to proceed with passport production is typically required at central management systems by approved authorization officers. These officials are also likely to be targets. Ensuring that software systems require multiple authorizations (and that the insertion of false requests is not possible) will require careful analysis of both the processes and the IT systems themselves. Again, providing audit trails for later analysis will be critical to identifying weaknesses in the systems.

Document Production

Once the request reaches the personalization center there are yet more threats to contend with. Machine operators could, if not controlled, insert bogus requests into the production process. As the passport specific cryptographic keys and certificates are added after the request for production is received, there is an opportunity to insert requests at this point (before the actual personalization takes place). Again, proper access control management and audit trails are needed for prevention and analysis. Well-designed systems will force a response back to the central systems, which should flag a mismatch between the requests generated and the passports produced. Ensuring that the centralized management systems capture and alert these issues is an important security measure.

At the personalization stage there are other threats, most notably when actual chip programming occurs. During this process— depending on the issuer and their setup—the data being personalized onto the chip may be transmitted in an unencrypted form. A properly equipped individual may be able to covertly capture this information that will include everything, including the private keys, needed to replicate a passport. It is possible to prevent this with the chip design, however only with a potential performance penalty.

Post Issuance

The above threats are all characterized by being relatively low-tech—the level of technical expertise needed to implement such attacks is not high and is easily within the reach of even modestly funded criminal networks. Other, more expensive attacks may involve assaults on the chip technology itself. Attacks on secure chip technology includes both non-invasive and invasive attacks—though modern chip technology is designed to defend against such attacks, one rule of thumb suggests that any system is vulnerable if enough money is spent on attacking it. On this basis, it is critical that the overall

ePassport model ensures that breaking the security of a single chip does not compromise the rest of the system.

Reinforcing the Weakest Links

Well designed issuance and identity management systems can, in a widely-networked world, offer significant levels of defense against any attacks. In particular, if management systems are well designed, it will be possible (albeit retrospectively) to identify illegal passports and to track the spread of counterfeit documents in a short space of time.

A key lesson in building the systems needed to defend against such attacks is that the introduction of chip-based biometrics alone will not provide the universal solution for border security. Important areas of focus include:

> **" Well designed issuance and identity management systems can, in a widely-networked world, offer significant levels of defense against any attacks. In particular, if management systems are well designed, it will be possible (albeit retrospectively) to identify illegal passports and to track the spread of counterfeit documents in a short space of time. "**

- Tracking and recording the details of the enrollment, management and issuance processes is vital to ensure that security breeches are minimized and that an audit trail is available leading to the source of any breech.

- Access control processes need to be implemented across the whole process with particular emphasis on avoiding single points of failure. The maintenance of high levels of physical and IT security at manufacturing and issuance sites is therefore essential.

- Data management systems, populated during issuance, need to be used to back-up border control processes. Where border control relies purely on individual biometric authentication to the passport chip there will be opportunities to use counterfeit e-passports to gain entry. Where possible, biometrics should also be checked against centrally held data.

- Countries need to look carefully at the approach used by the financial industry to analyze trends & unusual usage of credit cards. For example: where the same credit card is used in two different locations in a short period of time or suddenly starts to be used frequently when previously dormant, this is enough to trigger a warning and cause closer investigation. Similar techniques as applied to border control documents may help to prevent the wide scale successful use of high quality counterfeit passport documentations.

- Systems need to be designed to support frequent upgrade. As chip technology is advancing at a rapid pace, it is entirely reasonable to say that chips today will be significantly less secure than those available in ten years time. Systems need to support the introduction of new chip types and technology without requiring significant re-investment or major re-configuration. Any upheaval to the existing processes may present opportunities for security weaknesses to be introduced or taken advantage of.

- Finally, issuers should continue to integrate new features—electronic or otherwise—together with proven security print techniques, as visual inspection of these documents will not be forsaken (nor should it be) with the advent of the biometric chip.

Conclusion

As one set of risks is countered or blocked, the criminal will—should the economic imperative be high enough—find new ways of exploiting the system. No single line of defense will ultimately prove successful and, if security becomes dependent on such single lines of defense, may ultimately prove to be an exploitable weakness. It is clear that we already have the technology and methodologies to solve the problems listed above, but do we have the foresight to use them and the logic to deploy them in a holistic and pragmatic manner... If we do, then we should be finding some way to resolve the new problems associated with our new solutions, and achieve the delicate balance between our goals of security, interoperability and facilitation. ■

Do You Know Who's Traveling?

Assuring Traveler Identity at National Borders!

Identity Management is our Business

Protecting national interests by providing border control efficiency and convenience to the traveler, as well as maintaining the highest levels of safety and security.

New, compact B5000SC, with improved usability.

ID-Suite Borders

Fast, Proven, Automatic Authentication of Identity Documents.

- A hardware/software platform designed to automatically read and authenticate e-passports, driver's licenses, and ID cards that individuals use as proof of their identity.
- Supports Basic Access Control, Passive Authentication, Active Authentication and Extended Access Control.
- L-1's unique authentication technology adds security to any environment where the authentication of identity documents is crucial.

L-1 IDENTITY SOLUTIONS

VIISAGE
SECURE CREDENTIALING SOLUTIONS

L-1 Identity Solutions (NYSE: ID)
Learn more about our solutions at **www.L1id.com**.

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

The world turns to 3M for identification solutions

Whether you're protecting the integrity of ID documents or protecting borders, 3M can help. For more than 30 years we've been providing leading solutions that identify, authenticate and secure information on a global scale. Partner with 3M and experience a world of innovation that is driving secure identity.

Learn more at www.3M.com/security/ia/icao or call 1-800-581-2631.

3M