MRTD REPORT

ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Planning & Protection

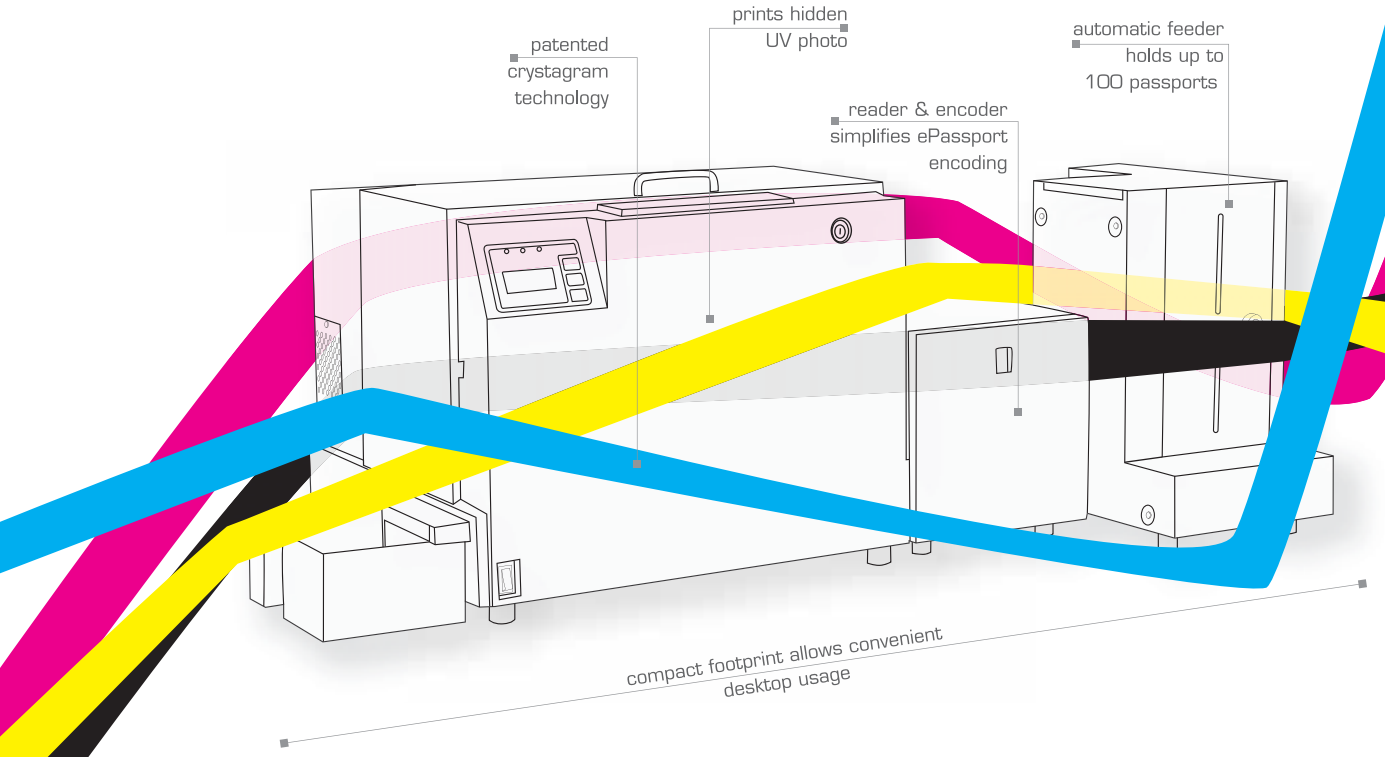
Providing a roadmap to States on the design and considerations of a robust, secure and flexible MRTD or eMRTD programme.

Also in this issue:
Malcolm Cuthbertson–MRTD Programme Guidance • David Philp on the ICBWG's Assistance for States • Arabic Transliteration by Mike Ellis • Robin Chalmers–Passports that Don't Read • ICAO Ecuadorian Mission • State Feedback: The Canadian Viewpoint • Fourth Symposium preview

Vol. 3, No 2

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

Secure your passport...



...with our E2000 passport printer.

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.

TOPPAN E2000 Passport Printer

ICAO MRTD REPORT
VOLUME 3, NUMBER 2, 2008

Editorial
Managing Editor: Mauricio Siciliano
MRTD Programme—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

The ICAO TAG/MRTD

The only international forum to achieve global interoperability on MRTDs and eMRTDs

The International Civil Aviation Organization (ICAO) Technical Advisory Group on Machine Readable Travel Documents (TAG MRTD), the ICAO Secretariat expert body in this area, is responsible for the development of specifications for travel documents with the goal of achieving global interoperability in this field.

In addition, the TAG MRTD seeks to advise ICAO Secretariat on technological issues related to the issuance and use of machine-readable travel documents.

Last May, during its 18th Meeting, the TAG/MRTD approved the work done by its working group and the work programme to be put forward for the coming year. During the last year, an extensive, thorough and complex programme has been achieved by this remarkable group of experts, which represents over 50 States.

In this issue you will read about some of the work achieved and recently approved by this group, notably the Transliteration of Arabic Names for use in MRTDs (page 20). You will also read about the TAG/MRTD approval for the creation of a new working group, the Implementation and Capacity Building Working Group, (ICBWG, see article on page four), which will, among other activities, increase the ICAO Secretariat's focus on providing field-proven assistance and expertise to nations that are now in the process of converting or modernizing their travel documents issuance process and, more importantly, updating their issuance systems.

What it is perhaps most remarkable about this ICAO Secretariat expert group is its exceptional and universal uniqueness: this is the only forum in the world able to research, discuss, draft and establish a common understanding on standards and specifications for MRTDs and e-MRTDs. There is no other.

This group has its foundations in an international convention (the Chicago Convention) adopted by 190 Contracting States, which provides the mandate to establish such standards and specifications. The group also benefits from a unique cooperative agreement achieved with the International Organization for Standardization (ISO), which provides for the technical support and integrity required to achieve sound international standards. Moreover, the work of the group and its success in implementing international standards relies on the cooperation and coordination with other International organizations such as INTERPOL, the United Nations Counter-terrorism Committee (UN CTC), the European Union (EU), the Organization for Security and Cooperation in Europe (OSCE), the Inter-American Committee Against Terrorism of the Organization of American States (OAS CICTE), the International Air Transport Association (IATA) the International Organization for Migration (IOM), and Airports Council International (ACI).

Thus, the ICAO TAG/MRTD is the only international forum that can truly propose and achieve the global interoperability required for the standards and specifications in this field, and it has successfully done so for over 30 years. Whether the initiatives or proposals come from a singular State, a small group of States or a region, the ICAO TAG/MRTD is the only rightful forum to which any such proposals shall be elevated to, in order to achieve any meaningful and significant international common understanding and standards.

Finally, the group also provides a forum for all ICAO Contracting States to establish and consider, in a "vendor-free" environment, their present and future needs for MRTDs and eMRTDs. Once these needs are established, the TAG MRTD, through its New Technologies Working Group (NTWG), issues a Request for Information (RFI) every three years in order to keep abreast of new and improving technologies from the vendor community. Relevant information gathered during the RFI process is summarized and shared among the 190 ICAO Contracting States, which is further considered when international standards and specifications are developed (thus, assisting States to put the "horses before the chariot" when it comes to adopting technology in this field.)

With the support of the Contracting States, the ICAO Assembly and the ICAO Council, the Secretariat and the TAG/MRTD will continue to be the unparalleled fulcrum on which this progress will revolve, and provide an unbiased and appropriate forum to continue and enhance it in the years to come—for the greater good of all the ICAO Contracting States. ■

Enjoy your reading.

Mauricio Siciliano
Editor

MRTD Compliance: Quality before Quantity

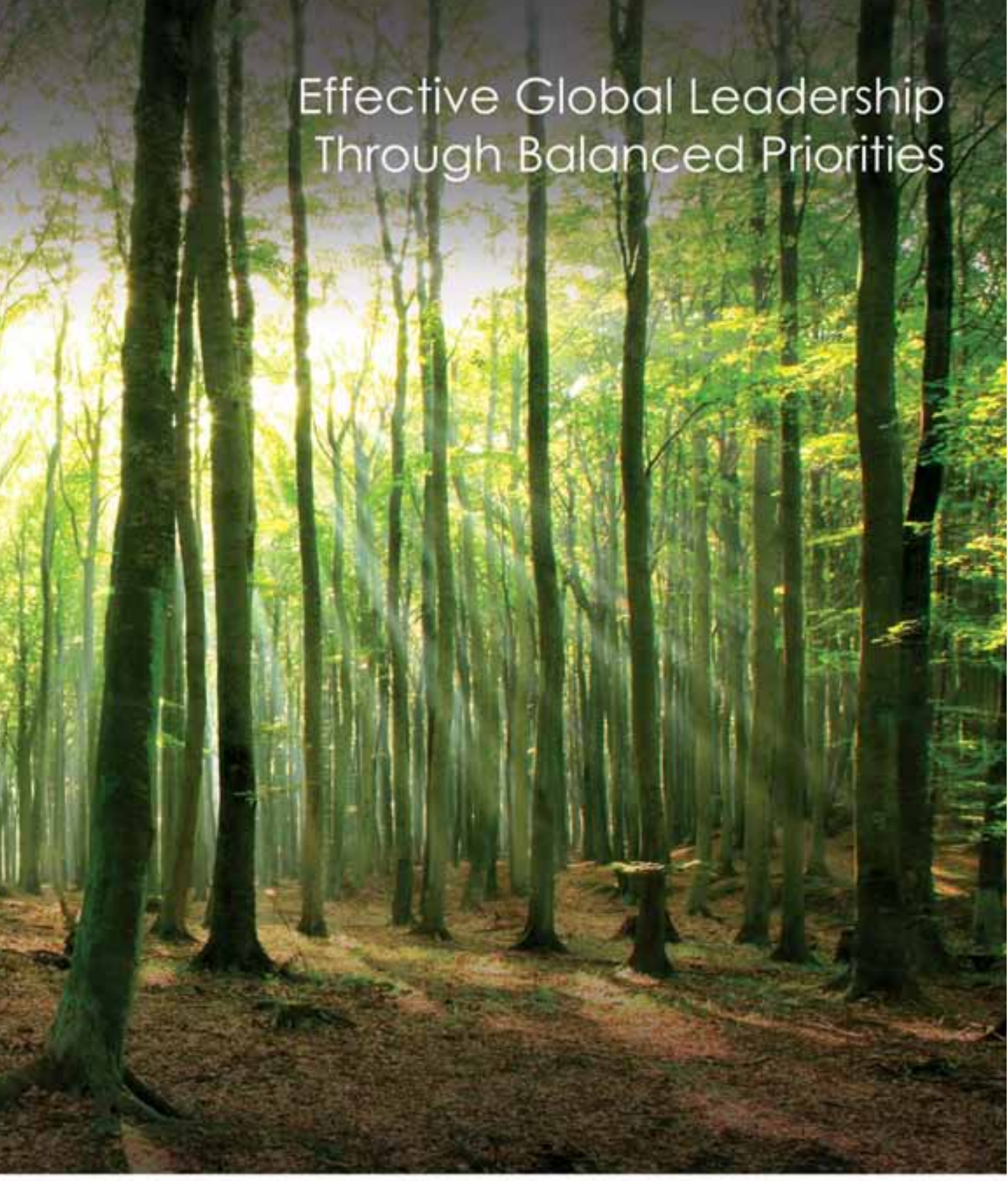
It was established this past May that the new Implementation and Capacity Building Working Group (ICBWG) should be convened to coordinate and promote special assistance to States still seeking to upgrade their travel documents to new MRTD standards. David Philp, Passport Manager for New Zealand's Identity Services division of the Department of Internal Affairs, and Chair of the new TAG MRTD Working Group, discusses the need for this new body and outlines the near and longer term goals that it will be establishing.

ICAO MRTD Report: **What was the motivation in developing the new ICBWG Working Group?**

David Philp: In 2004 ICAO had changed the minimum specifications for travel documents to require that by April 2010 all nations had machine readable passports. By 2007 there was a proposal to create a different structure for the MRTD advisory group with deliverables that would be more inline with the new results-focused business planning process that was sweeping through ICAO based on its new Strategic Objectives. In our area one of these was the providing of more in depth support for the universal implementation of machine readable travel documents.

The TAG recognized that to do this we really needed a dedicated focus group to begin to research and advance this area of endeavour at greater pace. The Secretariat continues to support that outcome and it understood that it needed to coordinate the resources and expertise of the Member States to push the programme forward. Although the 2010 date is no longer recommended for all nations (primarily due to the now very short timeframe remaining), the working group will be focusing on developing and coordinating field-proven assistance and expertise to the nations that are now in the process of converting their documents or who are soon to be embarking on the initiative to do so.

The working group was established therefore to help to take the programme forward at a greater pace. From my point of view as a chairman and from the Secretariat's point of view also a new level of priority will be assigned not only to the travel documents themselves but more importantly their issuance systems.



www.icao.int

The International Civil Aviation Organization

Portugal's RAPID system is an excellent example of MRTDs being very comprehensively integrated into newer and more efficient passenger throughput systems. Is that also something that the group is going to be looking at?

Yes it will. It will look to assist nations to develop border systems that will be particularly leveraged off the new capabilities and integrities presented by the newer passports.

And what additional tools and expertise do you expect the working group will be leveraging in the course of bringing this new assistance to States?

There are three primary areas where I see our work being implemented, mainly reflecting the range of backgrounds and technical expertise that our new members will be bringing to the table. The first of these will undoubtedly relate to technical and policy information that can be leveraged in the specifications and production of the actual document.

The second area will relate to the more fundamental project management assistance that can be shared with States just developing their programmes. There has been a great deal learned in this respect by the principalities who took it upon themselves to be the 'pioneers' in this area and it's in ICAO's interest not to see latecomer States to the MRTD process, often with less financial and human resources at their disposal, duplicating some of the errors in programme structure and management that several years worth of perspective has now provided us with the luxury to avoid.

Thirdly, all of this of course costs money and for some nations budget constraints are the greatest barrier. Therefore we'll be looking to partner with external donor organizations or countries who may be able to provide some of the assistance that will be required in this regard.

What are the current plans regarding how the Working Group will be structured and operated?

We're looking now to develop our own business plan that supports the ICAO business plan and its strategic objectives. Part of the requirements of the business planning process involves a detailed environmental scan of our industry and recent developments that will enable us to get a much clearer picture of the size and scope of the issues that are before us.

This type of detailed appraisal will also allow us to better identify and categorize those countries that aren't yet on the path to achieving compliance and to determine their capabilities and needs. This work has in fact already begun and I'm very much looking forward to these results.

Will this scan also let you develop a clearer picture of the complementary programmes that are going on in this sector… Helping you avoid duplication while identifying possible partners or collaborators?

Absolutely. There are quite a number of other organizations that have already established programmes of one form or another and we'll be looking to leverage off not only their experiences but also their skills… Particularly in the project management area.

And those organizations also have access to funding. That will be an important element I think. There's also quite a number of regional programmes that are active and show good potential for a variety of different types of collaboration and support.

And then additionally you've got organizations like INTERPOL that can provide some assistance and advice while also helping to ensure that countries report their lost and stolen passports. This is an ongoing problem in the world with literally millions of them out there and potentially in circulation.

That shapes up as quite a variety of stakeholders

I would expect the group to eventually have quite a large range of different participants—from governments and groups as have been mentioned but also through, for instance, the International Standards Organization. It will play a significant role in providing technical expertise and it also leverages its own unique and non-partisan partnerships with vendors.

My feeling is that the group will probably have somewhere in the region of 25 members before our first meeting in October. At the moment I've got about 12 or 13 with many others now firming up their particular availabilities and commitments.

Do you also see governments playing a key role in the group's activities?

Most certainly. One of the group's terms of reference is that, technically, it has to be chaired by a government representative. Given that our work is primarily aimed at assisting States, but also coordinating a much clearer picture of existing programmes and resources for all other States, we're finding a lot of government support. This is particularly true thus far from the more economically and technologically advanced nations, but we're also really trying to encourage a strong geographic spread at this point. Regional issues and concerns come into much clearer focus in this sector when the global picture is more accurately profiled and understood. We really need to ensure that we get adequate regional presence in order to be able to validate the quality of our data and to provide a better picture of more specific local conditions where required.

Do you think there's a body apart from ICAO that would be able to bring all these different types of stakeholders together and provide the forum that's going to be required for this working group to be effective?

ICAO is without a doubt the most suitable forum and tool for this purpose. There are a number of international organizations with resources and programmes now in play to assist us, but the world needs a body such as ICAO to coordinate the type of cooperation we'll be hoping to foster and leverage. We're also very keen to access ICAO's competence in the area of the development and provision of international training programmes.

Is the group's focus expected to be on increasing the number of compliant States or more on improving the quality of existing programmes?

We're not interested in simply rushing toward the 2010 deadline. It's been agreed that the focus should rather be on taking a measured approach and making sure the programmes that are put in place are robust and flexible. There are obviously a number of countries that still need assistance to get to level one, but the idea of the group is to provide detailed assistance to the states in developing their systems and processes.

As of today we've already started work on documentation, building off the work of the existing working group and developing guidance material on the secure issuance of travel documents, for example. We're also revisiting the current specifications for minimum security standards. It's most crucial at this stage that a solid bank of more general guidance material be developed that will be of significant practical and logistical value—while also capable of being tailored to the particular needs of States.

On a smaller scale, States will also need assistance with specific issues. In this instance we'll be looking to engage specific representatives from specific States and suppliers who have 'been there and done that,' if you would. I know from my personal point of view that, as New Zealand was one of the first countries to make the move to the new passport, we've had numerous visits from other nations hoping to learn from what we've done and how we've done it.

The Secretariat has limited resources in this regard but it is essential to establishing the type of framework that will be required. Once this is in place the international community can begin to work together and share existing expertise and new developments much more efficiently and meaningfully.

What sort of timeline are you currently working toward?

Currently everything is in draft form and queries were sent out in May 2008, shortly after I was appointed Chair, to some of the key personnel and government representatives whom I'd like to see participating. Our first meeting is currently slated for this October but I suspect that the group's membership will be more or less finalized somewhat in advance of that date. ■

The MRTD Game Plan

Important considerations for States planning to introduce or upgrade MRTDs and eMRTDs

As presented to the 3rd ICAO MRTD Symposium by ISO Task Force Member Malcolm Cuthbertson.

Newer chip-based MRTD security features are just a small part of what makes today's generation of eMRTDs the most secure and facilitation-friendly travel documents ever available to State passport officials. The ISO's Malcolm Cuthbertson outlines the issues and actions that need to be considered by States as they embark on the path to upgrading their travel documents to new MRTD or eMRTD standards.

This presentation is aimed primarily at those countries that are planning to introduce machine readable travel documents or ePassports for the first time. The subjects I'm going to discuss are first of all the evolution of the machine readable travel document (MRTD), its intended benefits, some of the market drivers that have got us to where we are today, and finally the security and personalization of MRTDs.

Although all MRTDs must conform to ICAO standards, that doesn't restrict countries, or groups of countries, from customizing their passports. As an example we could consider here the European Union, where their ICAO-compliant passports are required to have a burgundy coloured cover, a data page on page two, all the pages numbered, as well as specific security features.

I'd also like to highlight the facilitation and security aspects of these documents as I'm going to be going into in more detail on the balance—the fine balance—between facilitation and security in travel documents.

ICAO's only requirement, as has been discussed previously, is that all countries must have machine readable passports by April 2010. This is the first market driver moving this process forward. The other main drivers have been the U.S. Visa Waiver requirements for the 27 Visa Waiver countries (two failed to meet the 2006 deadline but all have now done so), and the European Union requirement that all member states have an ePassport with a facial biometric by August 28, 2006 (I'm afraid to say a number of those countries did not meet this deadline and still have a way to go). There is also the European Union fingerprint biometric requirement set for May 2009.

We need to note at this juncture that ICAO Document 9303 is a family of documents: Part One for passports; Part Two for Visas, and; Part Three for official travel documents or cards. I'd like to go into these in a little bit more detail.

Part One is currently split into two volumes: one for machine readable passports without added data storage, and a second volume for passports with additional data storage. Visas we will discuss a little later in this presentation. Part Three is split similarly to Part One.

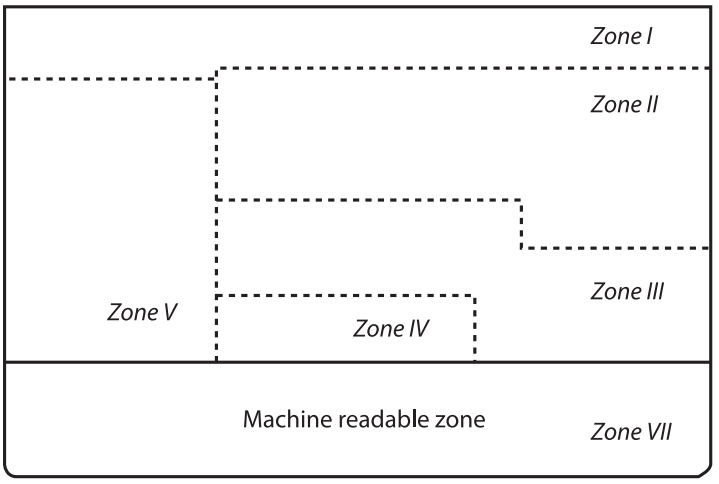
Part One—Volume One contains specifications on the photograph, the visual zone, and the machine readable zone. To enable the visual zone to be as flexible as possible, ICAO developed a series or a system of zones. Zone one is defined as the header, zone two as the personal data elements, and zone three for the document data elements. This was really to facilitate the task of immigration officers who were reading the passport, didn't have the facility to read the OCR, yet knew exactly where the data was. The specification is defined such that this content can all be on one page and in a sequence so that border control officials could extract the information as quickly as possible *(see Figure 1, left).*

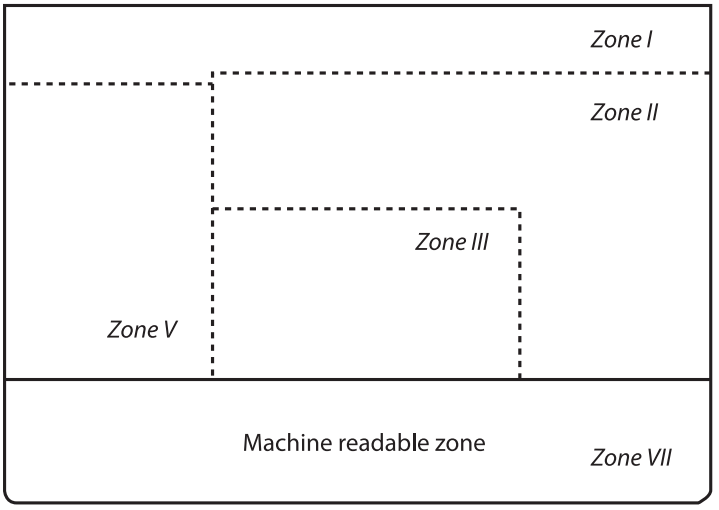
To provide as much flexibility as possible, field 13, for example, the optional personal data element provides that you can have a ghost image or a fingerprint—provided it doesn't obstruct the infield data. It doesn't always suit countries to digitally image the signature onto the data page, and so ICAO allows it to be in zone six—on the rear—or on the opposite page. To accommodate digital security or coded elements, provided they don't obstruct the photograph, zone five has been configured to provide space for these.

IMPORTANT CONSIDERATIONS FOR NEAR-TERM PASSPORT DEVELOPMENT PROGRAMMES

1. As well as ICAO Document 9303, States will also need to reference Chapter Three of Annex IX to the Chicago Convention for additional guidance and specifications.
2. Contracting States shall not extend the validity of their non-machine readable travel documents.
3. States shall issue a separate passport to each person regardless of age.
4. States shall begin issuing only machine readable passports (MRPs) no later than the April 1, 2010.
5. States shall make provision for any encoded data to be revealed to the holder of the document.
6. Non-machine readable passports issued after November 24, 2005 must expire as of November 24, 2015.
7. After 2015 there should be no non-machine readable passports still in circulation.

Figure 1. The Passport Visual Zones as defined by ICAO Document 9303, including possible variations.





With respect to different cultures and languages, the Qatar passport example provided *(see Figure 2, page 13)* is ICAO-compliant and you can see the Arabic text coming from right to left. This is one example of how ICAO has been able to accommodate these sorts of cultural and linguistic variables.

When we move into the machine readable zone we enter an area where there can be absolutely no flexibility *(see Figure 3, page 13)*. The OCR-B character set employed in the machine readable zone was chosen primarily because it had been field proven since the early '80s in applications such as bank cheques, and also because civil liberty and other privacy concerns are abated with OCR-B by the fact that you can also read the characters and content with the human eye—something not possible with magstripes or bar codes. Furthermore the Modulus 10 check digit at the end of each OCR-B numeric field isn't well understood by criminals and must be read at 950 nanometres in the B900 range. The check digit therefore helps provide some additional security despite the fact that it was originally designed for facilitation purposes.

Visa Issues

When we come to visas one of the questions in the forefront of most peoples' minds is "Why has a visa got to be globally interoperable? A country issues a visa and, in theory, it's only the country that's going to read that visa." Of course in reality that's not quite the case.

The Carriers Liability Act now requires that additional stakeholders and organizations, particularly airlines, must have access to visa information in order to ensure that a given passenger is actually entitled to travel to their destination. One eVisa method now under consideration for incorporating visa information into new generation travel documents is to

actually incorporate a contactless chip into the label, though this is not currently permitted due to possible conflicts with the passport's primary chip. A second method is the US or Australian technique of a paperless visa (the US version of which also utilizes a supporting label), and finally the option of including the visa in the actual passport chip. My personal view is that things now seem to be moving primarily toward the US/ Australian method of a paperless visa.

There are two types of machine readable visas for present consideration *(see Figure 4, page 14).* The Type A which is the American type and the larger of the two, and the Type B and smaller of the two, which was developed due to concerns that the Type A visa could cover the perfect numbering of the passport.

In both instances you'll note that the information zones on visas don't go

one, two, three—rather they are ordered one, three, two. The reasoning here is that on a passport the details about the person are most important—so they come first. In the case of a visa its the information about the visa itself that is considered most important; i.e. whether it's a transit visa, a work visa, etc. The machine readable information is ordered the same way on both versions, and as with the passport spec effort has been made to keep the visual zone as flexible as possible. One variation is that the machine readable area on the Type B visa is slightly smaller.

It's important when positioning these visas into passports that they are put in fairly accurately to the bottom left hand part of the page, and also that they're not skewed too much. Most of them will be read on lay-on readers, but there's still a number of swipe readers around, particularly in the airlines, and so care of placement remains a priority. Both the European visa and the

American Lincoln visa employ intaglio print, kinegrams, facial images, and additional measures which render them extremely secure documents.

Travel and ID Cards

Interoperability is also a concern for national ID cards or even driver licenses because these can currently be used, as in the European Union, for travel purposes. There are many variations of cards in circulation today, including ID Size One and ID Size Two, as well as a wide variety of functionality (some have contact chips, some do not) and information field zones (photos appear on the left or the right depending on the country, etc.).

Of primary concern in the present context is the fact that some cards still split essential data on both the front and the back of the card, and for facilitation purposes there is a movement now afoot to require all relevant information to be on one side for use with electronic readers.

Very few countries are now using ID Size Two cards any more, and of those that are I believe most have plans in place to change to the Size One standard in the very near future.

Although ICAO had previously indicated that technologies such as bar codes, magstripes and so on could all be made use of on identity cards, in the third edition of Doc. 9303 these other options have been whittled down and presently only contactless chips are permitted for ID cards that are also valid for international travel.

ePassports: Important Issues for States Designing New Documents

Presently there is just over 100 million passports being issued worldwide each year. The European Union, North America, Australia and so on for the developed world are responsible for about 50 percent of the passports issued each year. Therefore between the visa waiver countries and the European Union countries we can say that approximately half the world's passports are now being issued in e-format. 139 of the 190 ICAO Contracting States are now issuing MRPs. Of the 51 countries still not issuing them, 19 of these have MRP tenders in place. This leaves us with 32 countries still to initiate the upgrade process and a deadline of 2015 when non-machine readable travel documents will no longer be accepted.

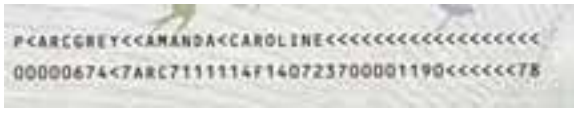
Where ePassports are concerned, 38 countries were issuing these with a volume per annum of 56 million at the end of 2007. This therefore accounts for half of the total new passport volume on an annual basis. By 2009 it's expected that there will be an additional 15 countries and another 23 million ePassports being issued annually. This leaves us then with a situation where 53 countries out of a possible 190 are now issuing ePassports, but perhaps more significantly almost 80 percent of the 115 million passports now being issued on an annual basis can be defined as ePassports.

For those countries planning to introduce ePassports, there are a number of issues that need to be considered. The first issue is between central or decentralized issuing, namely; "Is there a need to have a more centralized issuing process?" Centralization offers benefits including improved security, greater cost effectiveness and lower capital equipment requirements. Downsides include customer service levels that are not as high as a decentralized system allows for, especially with respect to embassy- or emergency-type issues. Decentralized systems pose higher security risks by requiring States to make allowances for the movement of blanks, producing more difficult audit trails, as well as necessitating higher numbers of staff in greater numbers of locations (meaning more difficult staff monitoring and therefore decreased overall system security).

Quite a lot of work has been done recently looking into the matter of emergency travel documents, and it has been maintained that States will need to have security features in their temporary or emergency documents comparable to their primary documents because of the principle that any system is only as strong as its weakest link. The validity period for temporary documents needs to be more than six months because some countries require more than six/less

Figure 2. A Qatar passport depicting Arabic text reading right to left. This is one example of how ICAO's specifications accommodate cultural and linguistic variables.

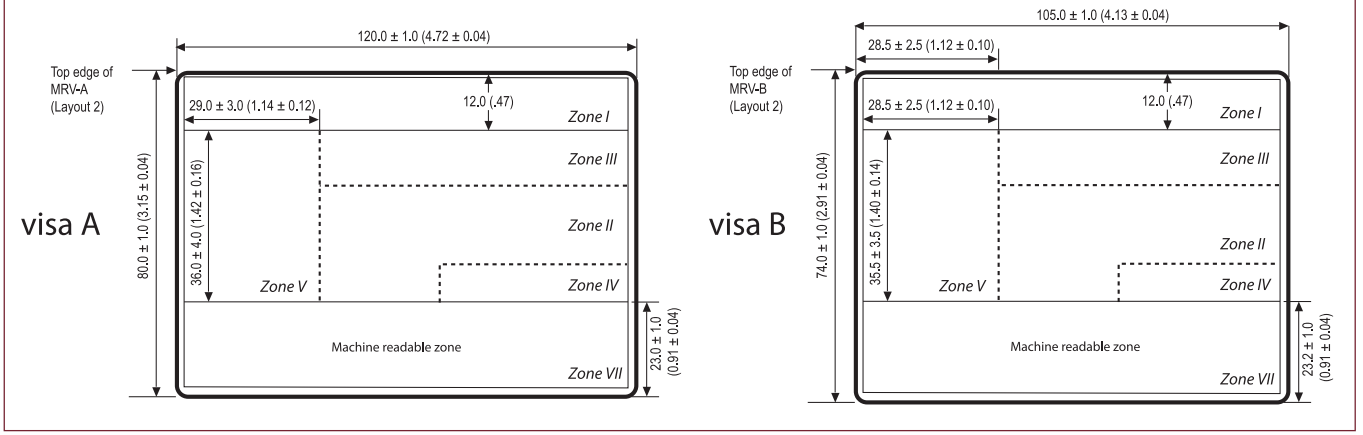
Figure 3. A sample of the OCR-B characters used in the passport's machine readable zone. As per ICAO Doc. 9303, II-2, machine readable information is contained in two lines of OCR-B text, each containing 44 characters.



than 12 months for related processes such as visa issuance. Temporary documents normally will contain eight to 12 pages and may have unusual cover colours (Canada has opted for a white version, Sweden for a pink shade) to encourage people to replace them with normal passports sooner than later. Germany, on the other hand, has opted to have their temporary documents look as much as possible like a real document to avoid possible confusion at foreign border control posts and unwanted suspicions aimed at its citizens.

Another issue that should be considered by newly issuing States is the personalization technology being employed and location options for the chip. There are a number of different personalization systems now available, including laser engraving, D2T2 printers, inkjet, laser engraving, and even a photographic system now being employed in Germany. It can be reasonably argued that laser engraving may be more suitable for centralized issuing whereas technologies like inkjet printing would be more appropriate for a decentralized solution. This is certainly true from a cost standpoint. States will note that Doc. 9303 leaves the location of the contactless IC, with its associated antenna, in the MRP at the discretion of the issuing State. It does, however, give guidance as to the optional

Figure 4. Type 'A' and Type 'B' visa specifications.



locations that are available and which are currently being used by Member States.

Other issues for newly issuing States to weigh include passport repatriation needs, the validity period of ePassports (whether, due to concerns over durability, there should be a requirement, as in New Zealand for example, to reduce the validity from 10 to five years), image capture, secondary biometric options, and waste levels (the unit cost of new generation ePassports is very expensive).

Where security features are concerned Appendix 1 to Section III in Doc. 9303 goes through the minimum requirements and includes a Glossary of Terms. Appendix 2 provides for machine-assisted document security aspects such as machine readability, kinegrams, and so on. These sections will not presume to tell you what measures you should or should not employ, but they will provide complete guidance on where the features you do choose should go on the data page. Most importantly from a security standpoint, as Barry Kefauver has previously detailed *(Editor's note: for the complete text of the relevant Barry Kefauver presentation, please see MRTD* January 2008 will be the information contained in Appendix 3 to Section III on the security of the issuing process.

Data Page Security

I'd like to move on now to specific issues related to the data page. Should the chip or the 'e' aspect of the ePassport become defective for any reason, it is important to note that the passport still remains a secure and valid travel document. It's important therefore that a lot of consideration continues to be given to the more traditional security features in the documents—in particular the data page—because that's the area that is most examined, contains all the personal data, and therefore which requires the most protection against counterfeit and fraudulent alteration.

Modern criminals using advanced desktop publishing tools (it's no longer the man with the hairdryer removing photographs in a dingy basement office) are now producing very sophisticated counterfeits. The importance of Level One features, such as multilayering, the protection of the photograph; not impeding the MRZ, and other aspects should all be employed to full advantage by States. I think that moving the data page away from the cover, which is recommended by ICAO, has been a very big step forward. Basically this last step has permitted States to incorporate all the security features that have been developed for currency (watermarks, special inks, holographic identifiers, etc.) into the passport.

I'm now going to go through some of the security features on a paper-based data page. The first thing that you notice is that the real estate on which to incorporate security features is rather small. You've got 125 by 88 millimetres to work with but the photograph takes up a reasonable area of that, which mustn't be obstructed. And there's 23.2 millimetres in the machine readable zone which equally needs to be protected and unobstructed. To get around the lack of space available document designers make use instead of various security 'layers' instead.
The base layer or substrate can be paper or polycarbonate, followed by a security layer and the various security printing and ink features that you can incorporate. Next comes the personalization processes (described in more detail earlier) and some of the digital security that can be incorporated, and, lastly, the number of laminates, particularly the new membrane laminates that are now available.

It's important to note therefore that passport security now involves designers and State clients moving beyond two-dimensional concepts and taking advantage of the new 'depth' in available security measures. To look briefly at the paper rather than polycarbonate option, in the first place passport security paper is UV dull, which normal paper isn't. It can be

chemically sensitized to protect against fraudulent alteration. You can select, and we would recommend, a different watermark to the watermark used on the visa pages to prevent page substitution, and the selection of a suitably complex subject for the watermark is very important (portraits, for example, are very good for this purpose). Visible or invisible fibres can also be incorporated into the paper, as well as numerous types of threads that have been designed for currency purposes.

Conclusion

In summary then, ePassport or chip-based security elements are not end in themselves. Traditional security is still very important and States need to maximize the security potential of the different layers that can make up the data page. However the security features we just noted above (fibers, etc.) were only what can possibly be incorporated into the paper substrate. Each separate layer offers similar options and it is of utmost importance that States strike a good balance between robust security and passenger facilitation/border control needs. Incorporating too many security features can confuse immigration officers and create new problems at border control points as a result.

It's important then to bring all these disparate parts together—the security print, the issuing systems, the laminates, the standards and so on. If these elements are not properly coordinated the determined criminal will definitely find the weakest link and go for that. Backing up what Barry Kefauver has said, at the moment the weakest link is definitely the breeder documents and the issuing processes. You can have the most secure passport in the world, but if it has been issued fraudulently you've wasted your money. ■

Advance Programme:

Fourth ICAO Symposium and Exhibition
ICAO MRTDs, Biometrics and Security Standards

ICAO Headquarters, Montreal, Canada, October 6-8, 2008

ICAO's MRTD Symposiums are the global forums for States, international suppliers and accredited experts in the fields of travel document issuance, production and regulation. As ICAO's 2010 deadline for implementation for MRP standards rapidly approaches, decision makers from all areas and disciplines in this field will be attending this event to provide input and guidance on the structure and operation of the future and interoperable travel document environment.

The following is an advance list of the itinerary and presenters at this unique global gathering. Readers who are interested in attending, exhibiting or otherwise participating in the upcoming ICAO MRTD Symposium should contact:

MRTD Secretariat
Phone: +1 514 954-8219, extension 8165
Fax: +1 514 954-5061
E-mail: MRTDSymposium@icao.int

MONDAY, OCTOBER 6

AM 08.00 - 17.00	Registration	09.00	Opening of the Exhibition
PM 14.00	Opening of MRTD Symposium		

1. Opening Statement by Secretary General of ICAO : Role of ICAO and objectives of the Symposium

Part I: MRTDs and Security

2. Keynote Address on International Security

3. Overview of the ICAO MRTD programme
An overview of the success of the ICAO MRTD programme and its evolution from MRP, to MRTDs (passports, visas and official documents of identity), to ePassports featuring the facial image as its globally interoperable biometric. This success is the result of joint work with the ISO through a special mechanism of cooperation whereby ICAO Standards are endorsed as ISO Standards. Secure and globally interoperable MRTDs and biometric eMRTDs meet today's challenging demands for improved security and facilitation.

4. A Brief History of the Passport
Progress from the early beginnings to our current environment featuring secure MRPs and biometric ePassports that are meeting evolving needs, including increased requirements for improved security and rapid clearance.

5. Threat Assessments and Risk Management
A number of countries have devoted tremendous work and funds to implement or plan advanced machine readable and electronic passport programmes. These initiatives are already paying dividends with respect to the integrity of the passport as a highly secure travel document, but that same success is accompanied by increased pressure on all attending systems and activities surrounding the issuance and inspection of travel documents.

There is a growing awareness that conscious and determined efforts are required to identify the risks in issuing and inspecting travel documents, particularly passports, and then defining ways in which those risks might be mitigated and managed. This presentation will address some of those risks and ways to manage them.

TUESDAY, OCTOBER 7

AM Part II : Secure Issuance and Reading of ePassports and Biometrics

6. Machine Readable Travel Documents - Identity Management and Protection Issues

- What threats exist to the integrity of MRTDs.
- What preventative steps can be taken to ensure that MRTDs are issued only to legitimate applicants.
- Importance of ICAO guidance on handling and issuance.

7. The German Experience: Incorporating the ICAO Facial Biometric and Second (Fingerprint) Biometric in ePassports as required by the European Commission

An overview of Germany's high quality biometric data collection through its 4,500 offices now processing applications for centralized production and personalization.

8. Importance of the ICAO PKD to Global Security

How the ICAO PKD works and an overview of the need for wider participation to ensure optimal effectiveness.

9. Analyzing the "e" in ePassports

An overview of the electronic security features of the ICAO-Compliant ePassport, viewed from the inspection systems perspective. The storage technology offers automated inspection systems the means to verify, through biometric technology, whether the person offering the passport is really the rightful holder. The "e" also offers powerful tools to check the authenticity and integrity of the document itself and the electronically stored information on the chip, confirming that it has not been modified. Topics of discussion will include the ICAO Public Key Infrastructure, certificate chains, certificate distribution mechanisms, and the use of keys and certificates in the inspection process. It is essential that automated inspection systems really use this technology and take full advantage of all that the "e" has to offer.

PM Part III : Border Security facilitated by MRTDs and ePassports

10. Improving Border Control Security with MRPs and ePassports and the continuing need for ICAO recommended physical document security features

ICAO has held a leading role for a number of decades in developing international standards related to the security and machine readability of passports and other travel documents, in particular the new ePassports and smart cards. The key to travel document security, even in the era of ePassports, is the requirement for MRPs to incorporate robust conventional physical document security features in addition to machine readability. This is essential to achieve secure and rapid facilitation of travelers through control points, both where high technology document verification equipment is available and where it is not. Examples are given of document security features considered to be most effective, and topics will address how the growing volume of ePassports (50 percent of current passports issued) is encouraging expanded use of biometric document reading systems for more secure inspection.

11. Automated Border Control systems to speed up passenger clearance

The use of ePassports and other biometric ID Documents in passenger clearance strategies, as reflected in ICAO's new Guidelines on eMRTDs & Passenger Facilitation.

12. Facilitation and Security: MRTD? ePassport? ABC? Or a better solution?

The challenge of immigration authorities worldwide is how to clear the ever-increasing volume of travelers efficiently. This means that the wanted and unwanted passengers must be identified speedily—by no means an easy task given the rapid passenger flow and increasing size of aircraft. Machine document readers, electronic documents and automated devices have been introduced to help achieve this goal but there is still room for improvement. This presentation will focus on what can and should be done.

13. Border Control Inspection: Security enhanced by MRTDs, Biometrics, Reading Systems and Automation

WEDNESDAY, OCTOBER 8

AM Part IV: Encouraging all States to introduce MRPs and upgrade to ePassports

14. ICAO programme to encourage cooperative efforts to assist States in introducing MRPs to meet the April 2010 ICAO Standard deadline, and to upgrade to ePassports

An overview of the ICAO UIMRTD programme and the role that the new Implementation and Capacity Building Working Group (ICBWG) will play in supporting the achievement of ICAO's business objectives. It will also outline the working group's proposed activities and how it intends to leverage off the expertise of government and private sector parties. An overview of what needs to be done to assist States with MRP introduction and ePassport upgrades.

15. IOM's assistance to States in introducing ICAO Standard MRPs and ePassports

- Role of IOM in migration and border management.
- Current priorities and collaborative approach with ICAO.
- Travel and identity documents for enhanced migration and border management.
- IOM's Travel and Identity Document Technical Assistance.
- Selected Project Examples.
- Recurrent Challenges.

16. How to Help States to introduce MRPs and ePassports

How to meet ICAO requirements for the introduction of MRPs and the upgrading to ePassports, including setting up a well balanced identity chain with reliable applicant registration and source documents. Expert assistance will be available.

17. Project Implementation: MRPs and upgrading to eMRTDs and ePassports

18. Concluding Summary Presentation

19. Concluding Remarks by Director, Air Transport Bureau, ICAO

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, 02088

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

Fax:
+38 (044) 561 2585

E-Mail:
edaps@edaps.biz

WWW:
http://www.edaps.biz

Arabic Transliterations for MRTDs

By Mike Ellis, TAG/MRTD

In response to security concerns raised by Interpol regarding variances in the manner that identical Arabic words and names can be spelled in Latin characters, the ICAO Secretariat requested that a work programme be initiated to prepare an "Arabic Transliteration Table" for Doc. 9303. Task Force 3 (TF3), of the ISO/IEC Working Group 3 (SC17/WG3), undertook this work approximately one year ago in liaison with ICAO's New Technologies Working Group (NTWG).

The ICAO Secretariat, through the TAG/MRTD working groups, has traditionally been active in following up transliteration issues and developing guidance for countries who desire to transliterate their national script into scripts that conform to the rules of ICAO *Doc. 9303, Machine Readable Travel Documents (MRTDs),* for entries in the Visual Inspection Zone (VIZ) and the Machine Readable Zone (MRZ) of MRTDs.

The TAG working groups have developed transliteration tables that have been incorporated into *Doc. 9303* and that give useful and sufficient guidance for many countries, in particular those with national scripts in the Latin and Cyrillic family. These general rules become more and more important as countries with scripts outside the Latin and Cyrillic family of scripts start to implement MRTDs.

Doc. 9303 states that if the name in the VIZ of an MRTD is in a font other than a Latin font, then a "transliteration" into Latin characters must be provided. Of course, the MRZ is limited to the (Latin) OCR-B characters 'A' to 'Z' and '<', so the Arabic font cannot be used there.

After analysis and discussion, TF3 decided to recommend that the traditional phonetic representation be continued to be employed in the VIZ. This phonetic representation is technically known as "transcription". However in the MRZ, TF3 recommends the use of a precise "transliteration" table to accurately represent the Arabic name.

The first point to stress here is that the representations of the name in the VIZ and the MRZ can be different. The VIZ is for human reading, so a phonetic Latin equivalent makes sense. The MRZ is for machine reading and subsequent database matching, so a more precise form of the name is required which may not be necessarily easily recognizable or pronounceable by humans. While we would like the two forms to be similar, this may not always be possible.

The Problem

The underlying problem is that the conversion of names from the Arabic font into Latin characters is dependent upon a number of factors that cause high degrees of variation in the transcribed result. These factors include the original language of the bearer (the Arabic font is employed not only by standard Arabic but also a number of other languages, such as Farsi, Urdu and Pashto), the skill of the translator, and the target language for the transcription (different Latin-based European languages have different sounds for Latin characters). Combined, these factors determine that a simple Arabic name, for example:

محمـــود عبـــدالرحيم

phonetically transcribed as say "Mahmoud Abdul Rahim", can have an enormous number of variations—57 of them for the first component of the name, "Mahmoud", alone (examples include Mahmut, Mahmud, Mahmood, Mehmood, etc.). No less than 145 variations exist for the second component of the name "Abdul Rahim" (e.g. Abd-al-Rahiim, Abdalraheem, Abd ar-Raheem, Abd al Raheem, etc.), but while not all influencing factors will always exist in every combination, on occasions when they did there would be no less than 8,265 possible transcriptions for this one Arabic name.

The Solution

To overcome this situation, TF3 has developed a new and more precise Arabic transliteration table for the MRZ. This table has been partially derived from the existing Buckwalter and SATTS standards, but because these standards contain Latin letters outside the range *A* to *Z*, a technique using *X* as an "escape" character has been developed. Thus the Arabic character "heh" would be transliterated as *H* and "hah" as *XH*.

The Arabic name mentioned above has only one transliteration under this framework: MXHMWD<EBDALRXHYM. While this might not appear to be particularly readable or pronounceable, for machine reading it represents an

unvarying and searchable transliteration of the original Arabic name. This is a major advantage for database matching in as much as a single query will now provide the results that used to require up to 8,265 separate searches. And for those systems that may still have to search the other variations, it is a major advantage to be able to reconstruct the original Arabic name and then to derive variations from that.

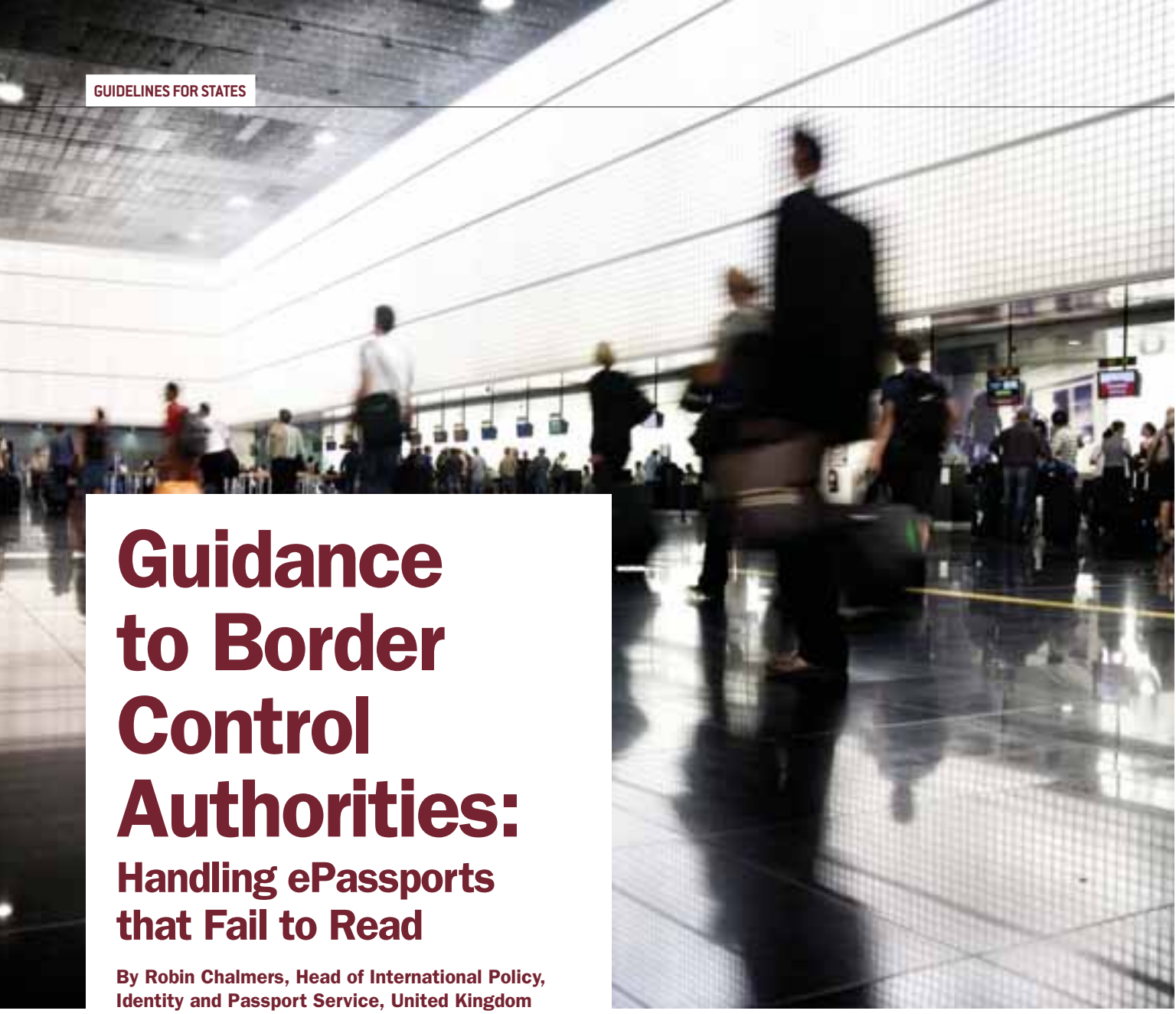
This major advantage of the being able to reconstruct the original Arabic name means that in countries using the Arabic font the original name can be machine read from the MRZ and displayed in the Arabic font. Thus MXHMWD<EBDALRXHYM maps into, and only into, its precise Arabic reflection noted above. Organizations such as Interpol doing database searches should find the conversion back to the original Arabic useful. If all transliterations of Arabic names follow this scheme, eventually the problem of having thousands of variations goes away. What's required at this stage is for the new standardization to start somewhere, and the passport is a good starting point.

Regarding the impact upon Advanced Passenger Information programmes (whereby governments require airlines to submit passenger information in advance), IATA, in a submission to FAL in Cairo, recently asked that governments only require airlines to submit the information recorded in the MRZ—so therefore there should be no negative impact or requirement for additional work based on our developments. For example, if the airlines instead were submitting a name from the PNR as supplied by the travel agent, there could be, and probably often is, a mismatch with the MRZ, so basically this IATA submission to FAL is the optimum solution.

Advice Sought

TF3 has constructed the new transliteration table based on the premise that the short vowels, the "harakat", are optional in Arabic names and often omitted. As well, it has not translated other diacritical marks such as the "sukun" and the "shadda" as of this point. Advice has been obtained from a number of international organizations, academic experts, and governments about the exact transliterations of the Arabic characters now being employed, but TF3's members are still soliciting any relevant input via their website at www.doc9303.com. Anyone qualified and interested in commenting on their work will receive a copy of the current transliteration table for their review and comment.

As of this writing a delegate from the UAE has submitted the report to the Technical Committee of the Gulf Cooperation Council, and it is hoped that a Middle-Eastern government will do the same with the Arab League. Feedback to date from Morocco, Algeria, Jordan, Tunisia, and Bahrain has so far been positive. ■



Guidance to Border Control Authorities:

Handling ePassports that Fail to Read

By Robin Chalmers, Head of International Policy, Identity and Passport Service, United Kingdom

Although it would be counter productive to penalize or delay a legitimate traveler due to a faulty or damaged chip in an eMRTD, this concern needs to be balanced against the unscrupulous acts of deliberate sabotage by fraudsters and other criminals. Robin Chalmers offers advice to States as they seek to define secure systems that will still be passenger-friendly.

An increasing number of countries are now producing ePassports and consequently border control authorities (and others) are increasingly being presented with such documents. ePassports constitute a significantly different document from previous passports as they contain a Contactless Integrated Circuit *commonly known as a contactless chip.* For the purpose of this guidance the terms 'contactless chip' or 'chip' should be taken as meaning contactless IC as per the 6th Edition of *ICAO Document 9303 (Part 1 – volume 2).* The chip contains the biographical details and image of the holder as shown on the biodata page. While the inclusion of a chip offers considerable benefits to the overall integrity of the document, it will inevitably introduce circumstances where the chip does not appear to be functioning properly.

Having developed an ePassport to make the document more secure and to enhance overall travel security through the use of biometrics, it would be perverse to penalize the genuine traveler as a result of a faulty/damaged chip about which they may have no knowledge. However care needs to be taken to balance this against the potential for fraudsters to disable the chip to prevent validation of the data taking

place. Consequently, it is important that some guidance is available to those that routinely inspect ePassports to assist them in determining whether difficulties in opening/reading/validating chips are potentially due to a fraud attempt or something much less sinister. It is also important that where documents cannot be read (e.g. due to damage) that they are withdrawn from circulation by the issuing authority.

The following guidance is intended primarily for the use of border inspection authorities. Consequently it aims to provide a fairly nontechnical approach to the ePassport, how it works and what problems a border inspector may encounter with such documents. It also sets out some of the reasons why problems may occur and also gives some practical guidance on what action to take.

Background

It has long been recognized that travel documents cannot provide a 100 percent guarantee that the holder of an identity document (Machine Readable Passport) assigned to that person by the Issuing State, is guaranteed to be the person purporting at a Receiving State to be the same person to whom that document was issued. Documents can be tampered with to change biographical data, the image can be substituted or a complete counterfeit document can be produced. The only method of relating the person irrevocably to their travel document is to have a physiological characteristic, i.e. a biometric, of that person associated with their travel document in a tamper-proof manner.

After a five-year investigation into the operational needs for a biometric identifier, which combined suitability for use in the MRP issuance procedure and in the various processes in cross-border travel, consistent with the privacy laws of various States, ICAO specified that facial recognition is the globally interoperable biometric technology. A State may also optionally elect to use fingerprint and/or iris recognition in support of facial recognition.

The introduction of ePassports provides a significant enhancement to the security of travel documents. The document holder's biographical and biometric data can be confirmed as being original to the document through the use of Public Key Infrastructure (PKI), which provides the means for machine assisted validation of this data. ePassports are, as a result, difficult to alter or counterfeit without detection *providing* Border control authorities carry out a proper document validation process in the course of the examination of the traveler.

The ICAO specifications require that digitally stored images are used, and these are "onboard" i.e. electronically stored in the travel document. A high capacity contactless Integrated Circuit chip is the electronic storage medium specified by ICAO as the capacity expansion technology for use with ePassports in the deployment of biometrics.

All ePassports that meet the minimum requirements set out in *ICAO Document 9303 (Part 1 – volume 2)* should carry the following symbol on the front cover of the passport, either near the top or bottom of the cover:

Both issuing and any receiving States need to be satisfied that the data stored on the chip has not been altered since it was recorded at the time of issue of the document. Names and other personal details of the passport holder that are stored on the chip reflect the information that is presented in the MRZ on the datapage. In addition, the privacy laws or practice of the issuing country may require that the data cannot be accessed except by an authorized person or organization. Accordingly, ICAO has developed specifications regarding the application and usage of modern encryption techniques, particularly interoperable Public Key Infrastructure (PKI) schemes, to be used by States with their Machine Readable Travel Documents (MRTDs). The intent is primarily to augment international document security through machine-assisted means of authentication of MRTDs and their legitimate holders.

It is not my intention to go into detail on how PKI works in this guidance. It is sufficient to say that PKI provides a means by which border inspectors can authenticate, through machine-assisted means, that the data that was placed on the chip when the passport was issued by the issuing authority has not been changed. The combination of the assurance given by PKI and the visual check of the document's physical security features will provide added security value.

However to do this, the inspection process needs to include not only a visual inspection of the data page and reading the chip in the passport, but also an information validation procedure. This should be a normal part of the automated inspection process carried out by passport readers equipped to deal with ePassports.

It is critically important for both border inspectors and the holder of an ePassport that the technology works. The potential for a chip or its associated antenna (which is used in the chip/reader communication process) to be damaged during production of the passport is a concern. Issuing authorities are aware of the importance of the need for the contactless chip to be protected not just against physical tampering but also casual damage including flexing and bending. Extensive durability testing has taken place in the course of the

development of ePassports to ensure that they are 'fit for purpose'. These checks can include but are not limited to impact testing, bending and twisting, putting through a washing machine cycle, and deep freezing.

Great care is taken with ePassports to avoid damage to the chip or the antenna in the production process. Checks are carried out at the end of the process to ensure that the chip is operating effectively. Additionally, a number of countries provide facilities for holders of ePassports to check them after they have been issued. It is also common in some countries for the chip to be checked at the point of delivery to the document holder.

Most countries advise recipients of ePassports that it is important that the document be treated properly. In some cases a printed endorsement appears on the page that carries the chip, requesting border authorities not to use it for entry/exit stamps. Although this may suggest that there is concern over the durability of the chip/antenna, this is not the case. It is simply there to alert the holder and border inspectors of the need to treat the document with appropriate care.

Given that the introduction of chips in passports is a new use of this technology, some concerns have been voiced as to how robust they are given that, unlike chips used in credit cards, etc., those used in ePassports need to be able to continue working over a much longer period (i.e. the maximum normal validity period for a travel document). Indications are that the level of faulty chips is extremely low and that detection of faults is happening prior to the book being sent out of the production facility. A number of issuing authorities have obtained warranties from malfunction from their chip manufacturer for the life of the passport (up to 10 years in some cases). As a result, it is very unlikely that a newly issued ePassport will contain a defective chip.

However, it is not just the passport issuers and producers that need to be aware of the need to take care with the production of ePassports. It is also essential that those inspecting ePassports at the border be properly trained in the operation of passport readers to avoid operator error and the possible misconception that a chip is malfunctioning when it is not.

Apart from the inherent physical protection of the chip in the book, protection of the stored data from alteration and unauthorized access is achieved through two methods method specified by ICAO: *Passive Authentication* and *Basic Access Control (BAC)*.

Where the face is the only biometric stored on the document, Issuing States primarily use the BAC mechanism in order to prevent unauthorized access to the chip data. This means that access to the chip data is not possible without the inspection system (i.e. the reader) 'proving' that it is authorized to access the chip, which is achieved from information taken by the reader from the passport MRZ.

Where BAC is being used, information from the MRZ is critical to the successful reading of the chip. If the MRZ is damaged, or of poor quality, the reader may be unable to access the chip (this might be the case, for example, where the document has been folded or has been mishandled or significantly abused—impacting on the readability of the MRZ). However the border inspector in such cases can enter the MRZ data manually and this should normally result in the chip contents being displayed for comparison with the document biodata page.

Border Inspectors should be alert to the possibility that failure to open the chip could mean that the second line of the MRZ has been fraudulently altered. Extended Access Control (EAC) has now been developed to provide additional protection to chip data (particularly in relation to fingerprint data), however the EAC protocols still require BAC to be successfully achieved before switching to the advanced access protocol.

An ePassport may be read at various points in a journey: on arrival at border control, exiting a country or in transit. At any one of those points the chip may fail to read. It is therefore important that guidance exists setting out suggested reasons for such failure—noting any telltale signs of attempted tampering and suggested guidance on the action to be taken. This should help achieve a degree of consistency in the treatment of such cases and ensure that genuine travelers holding ePassports are not unduly delayed should the chip malfunction (or appear to do so). Nevertheless, it is acknowledged that where the chip has failed to read it would be expected that the document and its holder would be subject to greater scrutiny by border control officials.

Finally, it is recommended that as States commence the issuance of ePassports they ensure that specimens are provided to other states so that these may be tested against a range of passport readers. In this way it should be possible to quickly identify any particular problems with documents/readers.

It is also important where chips are found to have a problem in the border inspection process that border control authorities raise this issue with the relevant passport issuing authority in order to highlight the problem and develop remedial action.

Interpreting Reader Results

ePassports present significant obstacles to the fraudster if they are read and validated fully against the Public Key Directory or similar facility using the Passive Authentication mechanism as defined by ICAO. As the document contains a chip in which the data has been digitally signed by the issuing authority, any change to that data will be highlighted through the reading *and* validation process at border inspection. Consequently, there may be attempts to disable the chip so that the inspection system is unable to read/validate the information contained in it or alter the second line of the MRZ so that the data on the chip cannot be accessed. In such circumstances a change to the biodata information in the book might go unnoticed, as it would not be confirmed as genuine through reading/validation of the chip. Consequently, the physical security features contained in the book remain an essential and very important feature of the inspection process carried out at border control. It is important that those who are required to examine passengers holding ePassports fully understand the technology of the inspection systems that are deployed by their governments at ports of entry. Border control authorities are likely to replace existing passport readers for new inspection systems designed specifically for ePassports, for example by moving from a 'swipe' to a 'flatbed/full page' reader. Border Inspectors used to 'swiping' passports may initially be unfamiliar with 'flatbed' readers and this can lead to difficulties reading ePassports and possibly lead to the reader being unable to detect the chip.

Border Inspection authorities should ensure that staff are sufficiently trained to ensure that where an ePassport fails to read, it is unlikely to be due to operator error. Errors can also occur where the chip takes longer to open than might be allowed by the border inspector or where the book has not been placed properly on the reader.

"Given that the introduction of chips in passports is a new use of this technology, some concerns have been voiced as to how robust they are given that, unlike chips used in credit cards, etc., those used in ePassports need to be able to continue working over a much longer period (i.e. the maximum normal validity period for a travel document). Indications are that the level of faulty chips is extremely low and that detection of faults is happening prior to the book being sent out of the production facility. A number of issuing authorities have obtained warranties from malfunction from their chip manufacturer for the life of the passport (up to 10 years in some cases). As a result, it is very unlikely that a newly issued ePassport will contain a defective chip."

Upon reading a chip-enabled document, the reader should normally display the image from the chip next to the scanned image from the biodata page. These images should be similar. If the image is missing, a second attempt should be made to re-scan the biodata page, preferably on a different reader to eliminate a problem caused by a malfunctioning reader *(see Figure 2, above).*

There will also be cases encountered where the ePassport reader detects that a chip is present but cannot display the chip image. There are a number of reasons why the chip data may not be displayed. Some of the reasons may be quite innocent—for example an error in the issuing process, or a problem with the inspection reader software. However as mentioned in the introduction to this guidance, issuing states take great care to ensure that when the passport book leaves the production facility that the chip is in working order. Over a period of time of course the chance of some damage occurring to the chip may increase. Where there is a problem reading/validating the chip data, border inspectors should examine the document and the passenger presenting it carefully.

A table is attached in Annexe A page 28 setting out a number of causes that may lead to difficulties in reading a chip. Recommended actions are also provided for each scenario. This

table has been designed specifically to provide a simple and nontechnical explanation of possible reasons for difficulties encountered reading an ePassport. Consequently it is a high-level view of the common reasons for problems reading the chip and may not be comprehensive.

Where a problem has been identified with the chip it will be up to national authorities to determine the appropriate action to be taken. This will depend on whether the problem is encountered either on departure from or entry to the issuing state or a foreign state. In some situations it may be appropriate to withdraw the document at the point of entry, especially if the holder is returning home from an overseas journey and does not require another document immediately. However, at the very least if the holder of the document has been allowed to enter or depart, it is recommended that he/she be advised to contact the passport issuing authority about the problem before their next overseas journey.

Detecting attacks on chips

ICAO does not specify the location of the contactless chip in ePassports. Consequently they can be found in end covers, the middle of the book, or within the data page. In most cases the chip and its antenna are not visible as they are 'sandwiched' between substrates. Nevertheless, and as mentioned earlier, many states indicate where the chip is located by a printed endorsement on the relevant area of the book.

In order to disable the chip, a range of attacks may be used. All of these are designed to prevent the inspection system from communicating successfully with the chip. It is inappropriate to provide examples of attacks on ePassports in this guidance. However it is recommended that border inspection authorities provide guidance to staff on a controlled basis that illustrates the type of attacks that might be made against the chip. It is recognized that, given the relative newness of ePassports, there are very limited examples of documents where the chip has been attacked. Nevertheless examples of guidance do exist and may be used as a basis for individual countries to develop their own. Further help may also be available from other sources where contactless chips are used.

While the failure of the inspection system to read the chip *may* indicate that there has been an attack on the chip or the antenna, border inspection authorities should not make a decision on the traveler's eligibility for entry

based solely on this factor. The inclusion of the chip in ePassports is an additional security feature of these new documents and failure in this one area by itself should not be sufficient reason to refuse entry. It is acknowledged that chip failure may lead to the traveler and the document being subject of a more rigorous examination. However a sensible balance needs to be struck based on the border inspector's overall consideration of the document and holder's reasons for travel.

Conclusion

The introduction of ePassports is a major step forward in providing a much higher degree of assurance on the genuineness of travel documents to border control authorities. While the inclusion of chips adds additional levels of security to the document, it does not in any way devalue the importance of the document-specific features that will continue to be a key component of a passport's overall security.

The contribution that chips can make to border control security is further augmented by the contribution they can make to easier passenger processing. It is now clear that a number of governments will be capitalizing on the opportunities presented by contactless chips to assist with throughput at border controls.

It is important therefore that ePassports are seen as a positive and helpful step forward in document security and passenger processing by Border Inspection authorities. This will be aided by having those who handle ePassports on a daily basis receiving an appropriate level of understanding about the documents and their technology. It is hoped that this guidance will go some way to providing that level of understanding. ■

Annex A

ISSUE	POSSIBLE REASON	RECOMMENDED ACTION
No response	- Reader communication fault. - Antenna damaged. - Chip damaged.	- Inspect passport carefully, especially MRZ and physical security features (Care: MRZ may have been tampered with). - Check reader/try different reader. - If everything else appears valid allow entry subject to normal immigration examination. - Advise holder to contact issuer on return to home country.
No chip data found	- Error by issuer. - Passport placed in Microwave to remove data (this might be verified under examination). - Passport issued as an emergency document.	- Inspect passport carefully using physical security features. - If everything else appears valid allow entry subject to normal immigration examination. - Advise holder to contact issuer on return to home country.
Chip data verifies but does not validate	**Care:** could be fraudulent passport	- Inspect passport carefully using physical security features and compare data on data page with chip data. - Check with issuer that passport record exists and that passport data is correct. - If correct allow entry, if not, conduct further investigation and potentially refuse entry.
Holder's image does not match printed image, yet all other details appear correct	**Care:** could be substituted chip or any of the following: - Photo substitution on booklet - Wrong photo stored - Digital photo in chip changed/ substituted	- Inspect passport carefully using physical security features and compare data on data page with chip data. - In secondary check with issuer that passport record exists and that passport data is correct. - If correct allow entry, subject to normal immigration examination. - Advise holder to contact issuer on return to home country. - If not, conduct further investigation and potentially refuse entry.
Digital Signatures do not compute correctly	**Care:** could be a forgery - Incorrect Document Signer Certificate attached to passport record.	- Inspect passport carefully using physical security features and compare data on the data page with chip data. - In secondary check with issuer that passport record exists and that passport data is correct. - If correct allow entry, subject to normal immigration examination and advise holder to contact issuer on return to home country. - If not, conduct further investigation and potentially refuse entry.

ICAO Assistance to Ecuador on MRTDs

In accordance with the International Civil Aviation Organization (ICAO) programme for Universal Implementation of Machine Readable Travel Documents (UIMRTD), a three-person team of experts visited Ecuador during the week of August 13, 2007. This team was composed of Malcolm Cuthbertson (UK), Barry Kefauver (US) and Mauricio Siciliano (ICAO ATB—Team Leader). The purposes of the mission were to examine the passport programmes in Ecuador in the context of security, system integrity, compliance with ICAO standards and specifications, and to make recommendations for enhancements as appropriate. The team was received with great hospitality and a warm and open willingness to share aspects of all of the issues, both positive and negative, in the spirit of Ecuador's commitment to improvement.

The ICAO Technical Cooperation Bureau, in coordination with the Air Transport Bureau, organized and fully financed a high level expert mission to Ecuador in order to verify and identify the State's technical assistance needs with respect to the modernizing of their systems of issuance for secure travel documents such as passports, ID cards (cédulas de identidad), visas, elections IDs, legalizations and refugee documents, etc.

Although Ecuador has already met the ICAO mandate for April 2010, the Government is continuing along the path to improve and modernize its ID management systems and passport issuance process—specifically the system for generating their "breeder" document to determine applicant eligibility for the Ecuadorian passport. In this sense, the team and the resulting report focus a great deal of attention on the national ID processes and the systems of civil registry—all of which are fundamental to passport determinations. The issues examined ranged from procedures, to facilities, to the modernization and automation of the office and staff equipment.

A key factor played by ICAO during this visit and assistance process was to serve as a forum and fulcrum to a common ID management and issuance project for the different local authorities that are involved with ID and travel document issues. There are a number of key local entities that are associated with the Ecuadorian passport, and in a larger sense, identity management activities in general (Ministry of Foreign Affairs, Department of Immigration, Border Police, Ministry of Tourism, Civil Registry, etc.). This assistance project made it possible for these organizations to come

together under a harmonious and unified commitment to the common purpose of moving Ecuador into the forefront of international identity management.

The report also recommended that this close collaboration must be shaped by and around a national security strategy and comprehensive integrated management focus. In this sense it was recommended that the implementation of this project should be allocated to and overseen by a champion at the highest level of the government, within the aegis of the President and directly reporting to the Vice President, if required. Because the proscribed goals require a well coordinated series of carefully planned and executed initiatives, the management and leadership of the champion must be carried out with the total commitment from the top—namely the President and Vice President. In order to effect the myriad changes needed and to bring Ecuador into the forefront of multilateral leadership, this high-level foundation and support is critical.

Malcolm Cuthbertson (third from left), Barry Kefauver (fourth from right) and ICAO's Mauricio Siciliano (fifth from right) with officials from Ecuador's passport and immigration leadership.

Members of the ICAO team reviewing documents and procedures with Ecuadorian officials.

Along with this overall policy and strategy, a second major area of the ICAO team's focus is the crucial contributions that civil registry and national identity programmes play in forming the foundation for related initiatives such as the passport. A number of recommendations were directed to enhancements in these areas.

Other recommendations were offered in the areas of application, personalization and issuance procedures, the use of biometric identifiers to verify and confirm identity, improvements for the passport booklet, including security features and passport printing and production, and finally improvements in the passport personalization process and in the border control processes. ■

Canada: MRTD Commitment and Progress

A traveler pauses at a NEXUS kiosk equipped with iris recognition technology. The NEXUS programme expedites border clearance for low-risk, pre-approved travelers between Canada and the United States.

With the number of countries still using non-machine readable travel documents (non-MRTDs) growing smaller year by year toward ICAO's 2010 MRTD implementation deadline, the *MRTD Report* will be devoting its attention in coming issues to highlighting the work of specific countries their MRTD implementation efforts.

In this first instalment of the *Report's* national profiles, Leslie Crone, Director of the International Programmes Division, Policy & Planning Bureau, Passport Canada, provides a testament to the importance of the new ICAO standards and Canada's role in developing and implementing them.

Leslie Crone

The process of establishing the new MRTD standards that are now leading the world toward a more secure and efficient travel document and facilitation system has taken over a decade now, and Canada is one of several countries that have played important roles in the work of the ICAO New Technologies Working Group that has coordinated and guided much of the research and reporting that have informed these important efforts.

"One indication of the commitment that Canada has made to the work of ICAO in this area is probably best reflected by the fact that Gary Macdonald, the Director General for Policy and Planning for Passport Canada, was the first Chair of the New Technologies Working Group," begins Passport Canada's International Programmes Division Director, Leslie Crone.

"Besides investing Gary's time I represent Passport Canada at the meetings," Leslie continued, "and we also have representatives from Citizenship and Immigration Canada and Canada Border Service Agencies participating as well. Canada has a strong understanding therefore of the importance of the work that the NTWG has been and continues to conduct, and we'll be continuing to commit the time and expertise available to us in order to assist ICAO in developing standards and implementation guidelines that are both practical and effective."

Canada currently has 16.4 million passports in circulation for a total population of some 33 million inhabitants. The country produced 4.8 million passports in its last fiscal year and has been producing MRTD-compliant documents since 1985.

It is an irony of technological progress that countries or regions who come later to a process can often leapfrog early adopters. So it is that Canada, despite the fact that it continues to play such a key role in developing the more contemporary eMRTD standards now being implemented, finds itself looking to a near future when it will be adapting its own document to the newer biometric security functionality of ePassports.

"A pilot programme is planned for later this fiscal year when Canada's diplomatic and special-issue passports will be ePassport-compatible," Leslie commented. "Public sector advances are often tied to longer budgetary cycles and this has very much been the case with our own programme. The Government of Canada has indicated that our own national ePassport programme will receive its funding and get fully underway in 2011."

On the importance and authority of the ICAO Document 9303 standards that she and her colleagues have helped develop, along with the many other State representatives and specialists who have participated in the work of the NTWG, Leslie is unequivocal.

"It's a testament to the quality and practicality of this work that everything we do in Passport Canada must submit to being able to qualify itself as 'ICAO-compliant," Leslie remarked. "The international travel document environment is one that demands very high levels of interoperability and shared coordination between global players for purposes of practicality and efficiency and, in that respect, the label 'ICAO-compliant' is the highest standard that a State can seek to attain." ■

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

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

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

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

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

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

Biometric system An automated system capable of:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Laser-perforation A process whereby images (usually personalized images) are created by perforating the substrate with a laser. The images may consist of both text and portrait

images and appear as positive images when viewed in reflected light and as negative images when viewed in transmitted light.

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

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

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

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

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

Metallic ink Ink exhibiting a metallic-like appearance.

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

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

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

Multiple biometric The use of more than one biometric.

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

One-to-many Synonym for “Identification”.

One-to-one Synonym for “Verification”.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UV Ultraviolet light.

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

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

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

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

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

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

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.

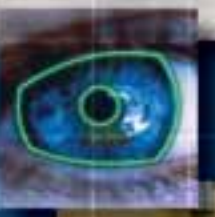
We offer a complete range of secure solutions that are tailored to local markets, and we deliver what you want where you want it with the support of a strong network of local partners.

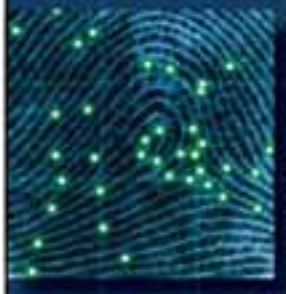
Gemalto relies on 120 years of experience in secure printing, and our unique expertise in digital security means we provide innovative, trusted solutions that you can count on.

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

Do You Know Who's Traveling?





Your Global Secure Identity Solutions Provider

In this era, visually checking documents is no longer enough, you need the complete identity verification solution, which only L-1 Identity Solutions provides. Our solutions are designed to improve security and operations on a flexible and scalable platform. We provide the capability to integrate many modules into a unified system, to be independently deployed, or to be fully integrated into existing systems!

We offer "one-stop identity shopping":

- **Backward File Conversion / Digitization / Scanning** of existing paper records
- **Identity Proofing** – Ensure the person is who they claim to be, and their documents are authentic.
- **Multi-Biometric Enrollment** – (ABIS), including face, finger, and iris
- **Secure Credential Issuance** – e-Passports, National IDs, Drivers' Licenses, proximity ID cards utilizing RFID technology and other secure credentials
- **Biometric Solutions** – face, finger, or iris

L-1 IDENTITY SOLUTIONS

VIISAGE
SECURE CREDENTIALING SOLUTIONS

www.L1id.com

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