ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

MRTD REPORT

Stressing Security

As ePassport technology defies its critics and privacy groups begin to better understand the scope and purpose of the biometric chip, more and more States are continuing to implement the world's most secure solution to the interoperable travel document.

Also in this Issue: ePassport PKI and the ICAO PKD, Interoperability Overview, EAC Roll-out, In-House MRTD Training, CSCA Certificates Overview List, Maldives Implementation, ICAO's role in MRTD advancement

Vol. 2, N° 2

The E2000 ePassport Printer

20 years

100,000,000 secure passports and counting...

When you need the newest and most secure passport issuing solutions, talk to us.

Global Enterprise Technologies is the world leader in state-of-the-art passport solutions. With an international network of offices and affiliates and extraordinary resources and experience, we are strongly positioned to meet the needs of all clients, irrespective of size and issuing volumes, and wherever located.

As exclusive distributor of **TOPPAN** digital passport printers worldwide for over a decade, developers of our own proprietary software solutions with biometric modules, and with unparalleled integration experience, GET is proud to offer a wide array of unique passport printing solutions that can be designed to meet your specific needs. Our newest printer, the **TOPPAN** E2000 passport printer, is specifically designed to fully meet the requirements for ICAO/ISO ePassports and features on-line chip encoding, automatic book feeding and user-friendly operation.

With references in Canada, Egypt, Greece, Malaysia, Mauritius, New Zealand, Oman, South Korea, Tanzania, Zimbabwe, the United Arab Emirates and the United States of America, contact us to find out why our solutions are setting the standards for secure passports. Around the corner or around the world.

The E2000 Passport

GET. Into the future

Global Enterprise Technologies Corp.
230 Third Avenue, 6th floor Waltham, MA 02451 USA
Tel: +1 781 890-6700 Fax: +1 781 890-6320
www.getgroup.com

GET™

ICAO MRTD REPORT
VOLUME 2, NUMBER 2, 2007

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
Copy Editor: Robert Ronald
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.
Mr. 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.

Contents

3M Identification and Authentication

Applying ingenious technologies to protect your security.

More than 100 years of developing practical and ingenious products has made 3M one of the most trusted and respected companies in the world. Our technology expertise is broad and deep, which has allowed us to develop some of the most secure products in the industry. Products such as 3M™ Confirm™ Laminates, 3M™ ePassport Readers, 3M™ Identity Document Issuance Systems and 3M™ Border Management Systems. Find out more at **www.3M.com/security/mrtd.**

Local Service. Global Support.

www.3M.com/security

3M Security

Taking an Active Role

In a time when tremendous efforts are being made regarding the consistent and secure standardization of travel documents, the ePassport still has many faces. The world's aviation and security communities are continuing to finalize issuance processes that respect minimum quality standards, local regulations, citizen rights and worldwide interoperability requirements, but these goals are much closer now to being realized thanks to an unprecedented multilateral effort between State and industry experts.

For the last 30 years, ICAO has been the leader and primary forum for achieving world-class standards for ePassport documents. But setting the standards in this field is only one of ICAO's functions. The ICAO Specifications and Guidance Material (SGM) Section is also committed to continue developing, improving, educating and promoting worldwide implementation of MRTD and eMRTD standards and specifications.

During the TAG/MRTD 17 meeting held in ICAO Headquarters last March, the Secretariat committed to prepare and put into action a communications strategy that would see the Organization playing a more active role in informing and educating government administrations, private entities and the general public regarding the content of the MRTD Programme and its significant benefits for international air transport and national security agencies. This role is even more significant today in view of the present worldwide implementation of the ePassport, not to mention the troubling misinformation that has been generated by hackers and privacy groups who have made headline-grabbing but ultimately baseless claims regarding the threats that contactless chips pose to the security and privacy of the world's travellers.

In this issue of the *ICAO MRTD Report* we interview Mr. Barry Kefauver, formerly of the US Department of State, who currently chairs the ISO Task Force on new technologies of the TAG/MRTD on the security and privacy issues related to the ePassports. This is the first of a series of interviews, articles and reference materials that will address the specific and general concerns that have recently been brought forward at conferences and in the media. This body of reference will help to serve States, the media and the general public in more clearly identifying and understanding the actual issues and concerns currently being addressed regarding ePassport chip security and bearer privacy.

Should any of these issues be of particular concern to members of our readership, we would suggest that they contact the MRTD Programme Office by visiting the 'Contact Us' section of the MRTD web site at: http://mrtd.icao.int. Your input, concerns and requests in this field will be essential to help us build a comprehensive set of articles, information papers and presentations that will address these issues and reinforce the credibility and global consensus surrounding this important effort.

Finally, you'll notice that this latest issue of the *ICAO MRTD Report* has a new look and feel. This new approach is part of an overall re-branding of ICAO's magazines to help stress the central role that ICAO plays in the global aviation community, and to ensure that the Organization is clearly identified with the important work it carries out on behalf of all of aviation's stakeholders. We encourage any comments or feedback on this new design and focus and hope that these changes have helped to make the *MRTD Report* more informative and user-friendly.

Enjoy your reading.

Mauricio Siciliano
Editor

ePassports: The Secure Solution

THE ePASSPORT HAS ENGENDERED ITS FAIR SHARE OF HEADLINES SINCE ITS IMPLEMENTATION BEGAN SEVERAL YEARS AGO, MOSTLY AS A RESULT OF HACKERS AND PRIVACY GROUPS WHO HAVE MADE FANTASTICAL CLAIMS REGARDING THE THREATS THAT CONTACTLESS CHIPS POSE TO OUR SECURITY AND PRIVACY. **BARRY KEFAUVER**, FORMERLY OF THE US DEPARTMENT OF STATE AND CURRENTLY A CONSULTANT WHO, AMONG OTHER RESPONSIBILITIES, CHAIRS THE ISO TASK FORCE ON NEW TECHNOLOGIES, OVERSAW SOME OF THE EARLIEST ICAO AND RELATED PROCEEDINGS LOOKING INTO PASSPORT SECURITY, BIOMETRICS AND DATA STORAGE. HE ADDRESSES THE SERIOUS FLAWS IN THE CRITICS' APPROACHES IN THIS INTERVIEW WITH THE *ICAO MRTD REPORT*, AND DESCRIBES THE HUGELY SUCCESSFUL TECHNICAL AND MULTILATERAL ACHIEVEMENT REPRESENTED BY THE ePASSPORT INITIATIVE.

***ICAO MRTD Report*: There have been a number of statements made in recent months regarding what are described as 'privacy and security threats' associated with the new RFID or 'e' Passports. Would you like to address these briefly before we discuss the situation in more depth?**

Barry Kefauver: One of the biggest problems with the current crop of RFID naysayers is that most of their comments and observations, as unfounded as they may be, have gone unanswered in the media. Essentially we have tried to point out in rational ways where the holes in their critiques are, and they simply ignore the facts. This is in part due to the fact that some of them, Lukas Grunwald for instance, are focused on setting-up or are working for RFID security companies. To deal with the facts would blunt the bite of their old and tired arguments, diminishing their headline-garnering effects.

The media isn't totally to blame here, but the realities of contemporary news gathering are such that wild claims made by anyone calling themselves an 'expert' garner far more headlines than do the reasoned, deliberative responses to these claims. You'll see all sorts of headlines screaming about security and privacy flaws in ePassports, but often you have to get down to the second-to-last paragraph in the column to find the part referring to how the claims were later pointed out to be somewhat less than legitimate. Unfortunately, the media are not asking that crucial question, "so what."

As an example, I encountered Lukas Grunwald in an open forum at a secure documents conference this past May in London. This pattern of denial was clear from the get-go. His slide presentation would make one unfounded claim after another. When I and others in the audience would try to address such claims as comprehensively as possible, he would simply ignore the substance and go on to his next irrational statement. I offered several corrections to his erroneous slides at that conference in May, though I noted that the identical errors were still in his presentation slides in July. We try

to let these critics understand where the holes in their arguments are and how false the premises are that they're basing their positions on, but in the end business is business I suppose and their companies' vested interests rely on a certain level of misinformation persisting in the public domain. It's unfortunate for the technology's credibility and it does a tremendous disservice to the many IT, security and cryptographic specialists who took part in the lengthy and very diligent development stages of the ePassport. Perhaps that's simply part and parcel of how things work these days and we have to white-knuckle our way forward.

Where Grunwald and others like him see these chip-based passports as a toy to be brought into the laboratory and made sport with on the basis of impractical and questionable scenarios, I see them as globally-interoperable tools that have had to meet multi-variant international requirements in order to be able to function effectively within different countries, cultures and economies. One of the proposed 'must-dos,' for example, is 'hashing' the facial biometric (hashing, in this instance, involves using prescribed cryptographic algorithms to protect data); however, hashing the image in that way would make it useless in a globally-interoperable environment such as border control.

It's very important to consider all of the security features of a given ePassport as complementary. To highlight a specific, alleged deficiency of a document's printing, selected security features, bindery or contactless chip is to ignore the context that these documents are used within and to ignore the understanding that everyone developed early-on in the process with respect to biometrics being an additive and not a replacement security measure.

Let's discuss those security features for a moment and try to understand more clearly why the ePassport is as secure as its developers and supporters claim.

You have to realize that one of the most significant factors associated with the current generation of passports is that these documents, contactless chips aside, have more physical features to protect them than any other passport in history. Any of the new generation of ePassports currently in circulation have the most advanced and the state-of-the-art security features available built right into the documents themselves—basically passports are the best they've ever been and this is before we come to the chip and the myriad other security measures that have been developed around that technology.

« I would like to stress that the chip in an ePassport in no way replaces the wide variety of additional security measures inherent in paper passports, but rather enhances and strengthens these measures through the addition of biometric data to help tie the bearer to the document in ways that could not be done before. We studied the technologies available to us, we consulted the world's foremost experts in arriving at our conclusions and best practices, and in the end we have produced an exceptionally secure document that will assist border control and other officials for decades to come. »

Can we briefly go over the security features associated with the chip itself?

It's very difficult for me to be brief about the development of the ePassport. I get so wound up and there's so much there. Let's start by saying that the chip itself and what it represents are the result of over five years of agonizingly-detailed multilateral deliberation. The search for something to carry more information and enhance passports-as-they-were goes all the way back to 1995. ICAO issued a Request for Information (RFI) at that time to elicit new ideas and new technologies from industry that could allow passports to carry additional security measures, specifically the use of biometric data.

We discerned fairly early on that biometrics were really the only type of data that could provide passports with the additional security we were looking for, and the only technology that could truly tie the document to the citizen to whom it had been rightfully issued. It took a full year to simply assess the various factors to be considered that could be addressed and resolved multilaterally, based on the 125 or so criteria that needed to be established by the working group. The facial image was judged to be the one biometric that could satisfy all the different countries' requirements. The very first Technical Report to be generated by ICAO around this topic was the one reflecting the process and specifics surrounding the selection and endorsement of the facial biometric.

A little further down the road, in the context of the ICAO New Technology Working Group (NTWG), we discerned that the contactless chip would provide the only practical approach for incorporating the biometric information into the passport document. I need to stress here that this began pre-September 11, 2001, and that therefore, even before that tragic incident, the worldwide travel document community had become absolutely certain that this was something that needed to be done if passport security measures were going to remain effective and move forward.

At that point in time there had been an implementation of the contactless chip in a paper susbstrate (many, of course, had been used in plastic, ID-1-type cards prior to this) which was of interest to us due to the differing chip placement configurations that would be required and, of

greatest concern, the need for different countries to be able to incorporate the chips into their documents based on their current passport manufacturing processes. We reached some initial sense of general direction and purpose in 2000 regarding the chip, and then spent the next two-to-three years looking over the full range of storage media alternatives such as optical memory, high-capacity magnetic stripes, two-dimensional barcodes, etc.

Was any consideration ever given to contact chips in this regard?

This is one of those areas where one of the myths surrounding our selection of contactless technology crept in: namely, that we were in some way 'puppets' of the RFID industry and simply let them spoon-feed us along the path to an RFID future. Among the more far-fetched, there were actually a series of allegations made that we had selected the contactless chips so that we could launch satellites and keep track of individuals from space—which is patently preposterous. Individuals tried to make the analogy that this technology was in some way similar to the chips being used for inventory purposes at your local department store. The fact is that the genre of chip used for inventory control and the 14443 chip used in passports are completely different technologies, not to mention that both have very different performance and security attributes that were carefully considered in the early going.

I want to make it very clear here that we've had, and continue to have, the world's experts at our disposal regarding all of these decisions. To listen to Lukas Grunwald, who stated this point earlier this year at his presentations in both London and Las Vegas, the people who selected contactless chips and came up with the new standards were all "brain-dead", and only had 'politicians and printers' at their disposal for advice and expertise. Like most of what Mr. Grunwald comes up with, nothing could be further from the truth. Throughout this process we have consulted with chip experts, electrical engineers, IT experts, physicists, cryptographers, security specialists, card technology practitioners—basically the highest caliber of professionals across the board that could be brought to bear on these issues.

In 2004 we had a standing-room-only meeting in London where 130 cross-industry experts were on hand at a joint ICAO-ISO session where we presented for review what we were intending to accomplish vis-à-vis contactless chips and biometric passport data. We noted all the possible technologies and applications at our disposal and for three days these experts, from scores of companies and organizations, poured over the requirements of the travel document and border inspection functionalities and gave us feedback based on their own implementations in other industries, for instance banking. It was here that we refined our expectations and focused in on the ISO 14443 series chip due to numerous performance virtues, as well as the necessity for them to be read from proximity and the added security potential proximity-reading would provide.

And so what about those who now say that they can clone or copy these chips without the holder's permission? What are the actual risks posed by this ability they've demonstrated?

The ability to clone or copy the biometric information on a contactless chip, from a security and engineering standpoint, is a relatively trivial matter. We knew from the onset that cloning chips was feasible and rather simplistic, but what was important to us was to make sure that this cloning or other misuse would not jeopardize the overall security of the travel document. Cloning a chip is basically the electronic version of photocopying someone else's passport data page. Imagine going up to a passport inspector and attempting to present a photocopied data page of somebody else's passport, and essentially you have the security-threat equivalent of cloning a chip. You'd be laughed out of border control and escorted to the door, maybe by security officials, maybe by the nice men in white coats. Again, the rigour to be applied with cloning is the "so what" test. Cloning a chip has no impact on a passport's security or the bearer's privacy—it is a non-issue.

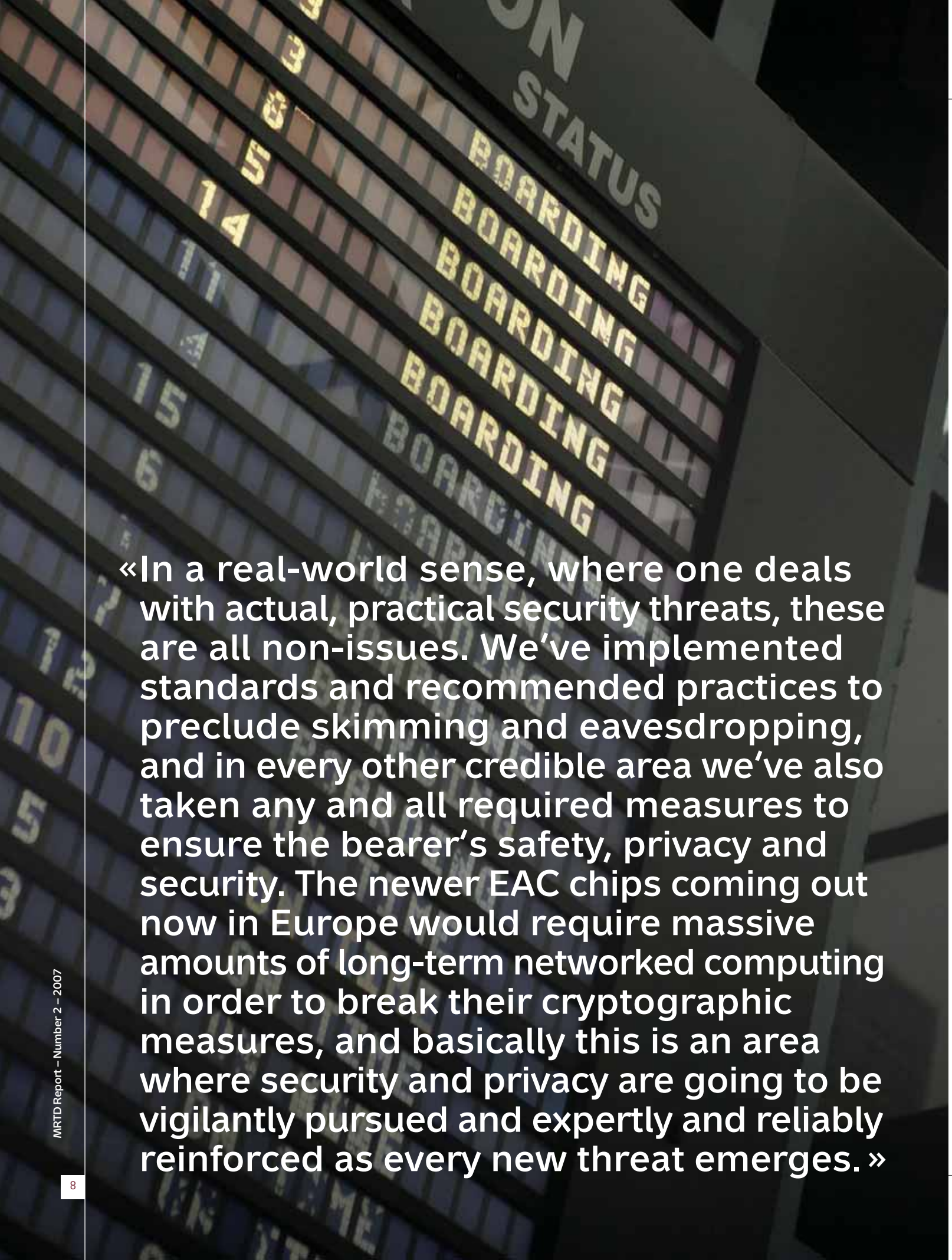
> « **We try to let these critics understand where the holes in their arguments are and how false the premises are that they're basing their positions on, but in the end business is business I suppose and their companies' vested interests rely on a certain level of misinformation persisting in the public domain. It's unfortunate for the technology's credibility and it does a tremendous disservice to the many IT, security and cryptographic specialists who took part in the lengthy and very diligent development stages of the ePassport.** »

The skimming threats (reading the chips from a distance) are also something that the worldwide travel document community has spent a great deal of time and money on over the past several years. It's been proven thus far that, indeed, you can access a chip from beyond the 10 cm range, but mainly what has been shown is that one can merely activate the chip, not necessarily read meaningful data from it. So, yes, a chip can be skimmed. However, the pragmatics of doing so must be considered to assess how much of a risk this represents. Sophisticated equipment, carefully orchestrated logistics of book placement, and rather precise circumstances are needed. At one example of this that I witnessed in a lab, the machine in question needed to be rolled in on train track rails and the level of power required to operate it was dangerous to humans. Not the kind of equipment that you could fit into a cigarette pack.

FIGURE 1: SUMMARY OF SECURITY RECOMMENDATIONS FROM TABLE IIIA-1, ICAO DOC 9303.

Threats (Counterfeiting)

Basic features		Additional features	
Paper substrates (5.1.1)			
▪ controlled UV response ▪ two-tone watermark ▪ chemical sensitizers	▪ appropriate absorbency and surface characteristics	▪ registered watermark ▪ invisible UV fibres/ planchettes	▪ visible UV fibres/planchettes ▪ embedded or window thread
Label substrates (5.1.2)			
▪ controlled UV response ▪ chemical sensitizers ▪ visible UV fibres/planchettes	▪ invisible UV fibres/planchettes ▪ non-peelable adhesive	▪ embedded or window thread	
Plastic/synthetic substrates (5.1.4)			
▪ security features providing an equivalent level of security in plastic ▪ as per paper or substitute		▪ optically variable feature (OVF)	
Security printing (5.2)			
▪ two-colour guilloche background ▪ rainbow printing anti-scan pattern	▪ microprinting ▪ unique biodata page design	▪ intaglio printing ▪ latent image ▪ duplex pattern ▪ 3-D design feature	▪ front-to-back register feature ▪ deliberate error in microprint ▪ unique design on every page ▪ tactile feature
Numbering (5.2.3)			
▪ unique document number		▪ perforated document number	▪ special typefonts
Inks (5.2.2):			
▪ UV inks on all pages ▪ reactive inks		▪ optically variable properties ▪ metallic inks ▪ penetrating numbering ink ▪ metameric inks ▪ infrared dropout ink	▪ thermochromic ink ▪ photochromic ink infrared ▪ fluorescent ink ▪ phosphorescent ink ▪ tagged ink
Photo-substitution (5.4.4)			
▪ integrated biodata page ▪ guilloche overlapping portrait ▪ secure laminate or equivalent		▪ OVF over the portrait ▪ digital signature in document ▪ embedded image ▪ secondary portrait image	▪ storage and retrieval system for digital portrait images ▪ biometric feature
Alteration of the biodata (5.4.4)			
▪ reactive inks ▪ secure laminate or equivalent		▪ chemical sensitizers in substrate ▪ secondary biodata image	▪ OVF over the biodata
Page substitution (5.5.3/4)			
▪ lock stitch or equivalent ▪ unique biodata page design		▪ programmable sewing pattern ▪ fluorescent sewing thread ▪ serial number on every page ▪ page folio numbers in guilloche	▪ index marks on every page ▪ biodata on inside page
Deletion/removal of stamps and labels (5.5.5)			
▪ reactive inks ▪ chemical sensitizers	▪ high-tack adhesives (labels) ▪ permanent inks (stamps)	▪ over-lamination ▪ high absorbency substrates	▪ frangible substrate (labels)
Document theft (5.7.1):			
▪ good physical security arrangements ▪ control of all security components ▪ serial numbers on blank documents ▪ secure transport of blank documents ▪ internal fraud protection system ▪ international exchange on lost and stolen documents		▪ CCTV in production areas ▪ centralized production ▪ digital signature ▪ embedded image	



«In a real-world sense, where one deals with actual, practical security threats, these are all non-issues. We've implemented standards and recommended practices to preclude skimming and eavesdropping, and in every other credible area we've also taken any and all required measures to ensure the bearer's safety, privacy and security. The newer EAC chips coming out now in Europe would require massive amounts of long-term networked computing in order to break their cryptographic measures, and basically this is an area where security and privacy are going to be vigilantly pursued and expertly and reliably reinforced as every new threat emerges.»

The bottom line is that yes, you can skim, but this is extremely impractical with Basic Access Control and other measures that States are now implementing using state-of-the-art cryptographic technology. If you look at the ICAO 9903 document's security measures *(see excerpt, page 7)*, you'll find a lot of the information there in much more arcane but important detail. Some countries are also using shields built into the ePassport cover that render the contents, quite simply, unreadable until authorized to do so. Now that Europe is rolling-out fingerprint data into their chips, necessary measures such as Extended Access Control technologies are additionally being used to make this data even more secure.

What were some of your early findings after you had settled on the 14443 chips?

At a watershed meeting over a two-week period in Glasgow, where the world's experts came together, industry and government discussed everything relating to chip security, passport manufacture and basically the entire panoply of issues that needed to be discussed prior to the serious testing getting started. Subsequently, at the Canberra meeting, which was really the first meeting where we started to put interoperability to the test in a targeted way, we invited a host of chip and reader manufacturers to come and be evaluated. It became apparent fairly quickly, however, that claims of 14443 compliance were confused, exaggerated and very misleading *(for a more detailed overview of the interoperability test meetings and their respective results, please see "Achieving Interoperability," on page 16)*.

What we were finding was that chips and readers made by the same company, used in the same plant, could be rolled out and would functionally be considered interoperable. Real problems became apparent, however, when we started testing one company's readers with another's chips, and vice-versa. Basically at this stage of development nothing was working in a manner that would be useful to us from the interoperability standpoint. What we discovered was that the 14443 standard had a lot of holes (known affectionately as 'doors' in ISO) that we were going to need to fill-in ourselves if our interoperability goals were to have a hope of being achieved. Fortunately we have been able to accomplish this.

What are some of the other security concerns that *MRTD Report* readers may wish to have reassurance or further information on?

Eavesdropping, whereby someone may wish to 'listen-in' on the data-exchange between a chip and a reader, is another area where much attention has been directed. Since this has been feasible for years, no one has ever shown much interest in actually doing this, but regardless there is enough consideration being given to a range of provisions, such as Faraday cages for readers, that are addressing this issue and rendering this a very low level threat from an overall security standpoint. Governments and others in general have had security provisions for many years designed to eliminate or minimize risks from unprotected or unauthorized RF radiating from PCs and other types of sensitive equipment.

Another area, albeit of a very low threat level concern at this stage, is the so-called ePassport as a beacon scenario. Here it's proposed that if unauthorized persons were to access the information on a chip, if they could get that chip's serial number, and if they had a list of manufacturers that used chips built with those serial numbers, then and only then this group might be able to identify a traveller's country of origin. Though very impractical and highly unlikely, the travel document community

nonetheless took this threat seriously, as we do with all threats, and has put measures in place to eliminate this concern. Another example of our commitment to insuring that privacy and data integrity remain uppermost in our minds.

To the privacy crowd the sort of 'so what' test cited earlier doesn't really matter, nor does it matter that someone can get far more useful information from a trash-can in your driveway, nor does it matter that many hotels, for instance, regularly ask for your passport and photocopy it for their verification and records, thereby duplicating exactly the same sort of information that a skimmer might find from a chip with much more expense and effort. But this doesn't keep ePassport critics and privacy mavens from dreaming up any number of far-fetched scenarios whereby terrorists could, for instance, follow around a bus with a chip skimmer trying to determine if there were enough of one nationality or another's citizens in it to warrant blowing it up.

In a real-world sense, where one deals with actual, practical security threats, these are all non-issues. We've implemented standards and recommended practices to preclude skimming and eavesdropping, and in every other credible area we've also taken any and all required measures to ensure the bearer's safety, privacy and security. The newer EAC chips coming out now in Europe would require massive amounts of long-term networked computing in order to break their cryptographic measures, and basically this is an area where security and privacy are going to be vigilantly pursued and expertly and reliably reinforced as every new threat emerges.

To conclude, I would like to stress that the chip in an ePassport in no way replaces the wide variety of additional security measures inherent in paper passports, but rather enhances and strengthens these measures through the addition of biometric data to help tie the bearer to the document in ways that could not be done before. We studied the technologies available to us, we consulted the world's foremost experts in arriving at our conclusions and best practices, and in the end we have produced an exceptionally secure document that will assist border control and other officials for decades to come.

Bringing together a unique partnership of government and industry, devoted to a common purpose, has brought us to where we are today. In my view, all of those involved can feel extremely proud about the effort that has been expended and the incomparable multilateral achievement that the ePassport represents. ■

Sdu Identification's passport concept ready for the future

Dutch passport

Finnish passport

Irish passport

Slovakian passport

Swiss passport data page

Integrated transparent Kinegram®

Binding technology®

ImagePerf/TLI®

Enrolment device

Sdu Identification is one of the leading developers of physical and digital high-end national identity documents world-wide. By means of system integration we realise secured end-to-end solutions to process the issuing of ID documents.

Research & Development has always been high on our list of priorities. We have developed a high-end passport concept in which the data page with integrated contactless chip technology is finished as a polycarbonate document that is incorporated into the passport booklet using a durable binding technology invented by Sdu Identification.

Moreover, our company has developed the concept for the current Dutch identity card. Also made from polycarbonate, it enables contact and contactless chip technology to be integrated. In addition to the graphic laser-engraved personalisation, ImagePerf/TLI® and a transparent Kinegram® are applied in the identity cards as well as in the passport data page.

Also the Dutch EU Residence Permits and the new Dutch driver licences are produced following this high-end identity card concept.

Integration of biometrics

Concerning the durability of a biometric passport, the most important requirement is that chip and antenna must function correctly during the lifetime of the passport. The best solution for security and durability is the ICAO compliant integration of a contactless crypto processor chip with an antenna into the polycarbonate data page. Biometrical information about the document owner is saved digitally and secured electronically in the contactless crypto processor chip.

Sdu Identification developed a biometric passport solution that is already in full scale operation in three European countries. The Dutch government as well as the Finnish successfully implemented this since August and the Irish government successfully implemented this since October 2006. Next to that Sdu Identification has been awarded with a contract for the production of biometric passports for Slovakia. Sdu Identification is also the supplier of polycarbonate data pages for the Swiss passport.

Secured storage of biometric data

The authenticity, integrity and contents of the chip are guaranteed by the use of a digital certificate and asymmetric keys. The retrieval of this information and the biometric identification of the identity of the document owner can take place at border crossings.

The Sdu Identification ePassport solution, consisting of a Philips 72 kB Smart MX micro crypto processor chip, operating system and Sdu ID_Applet, allows the storage of two types of biometric data, i.e. facial recognition and fingerprints and the following functionalities as far as specified by ICAO:
- Passive Authentication;
- Basic Access Control;
- Active Authentication;
- Extended Access Control.

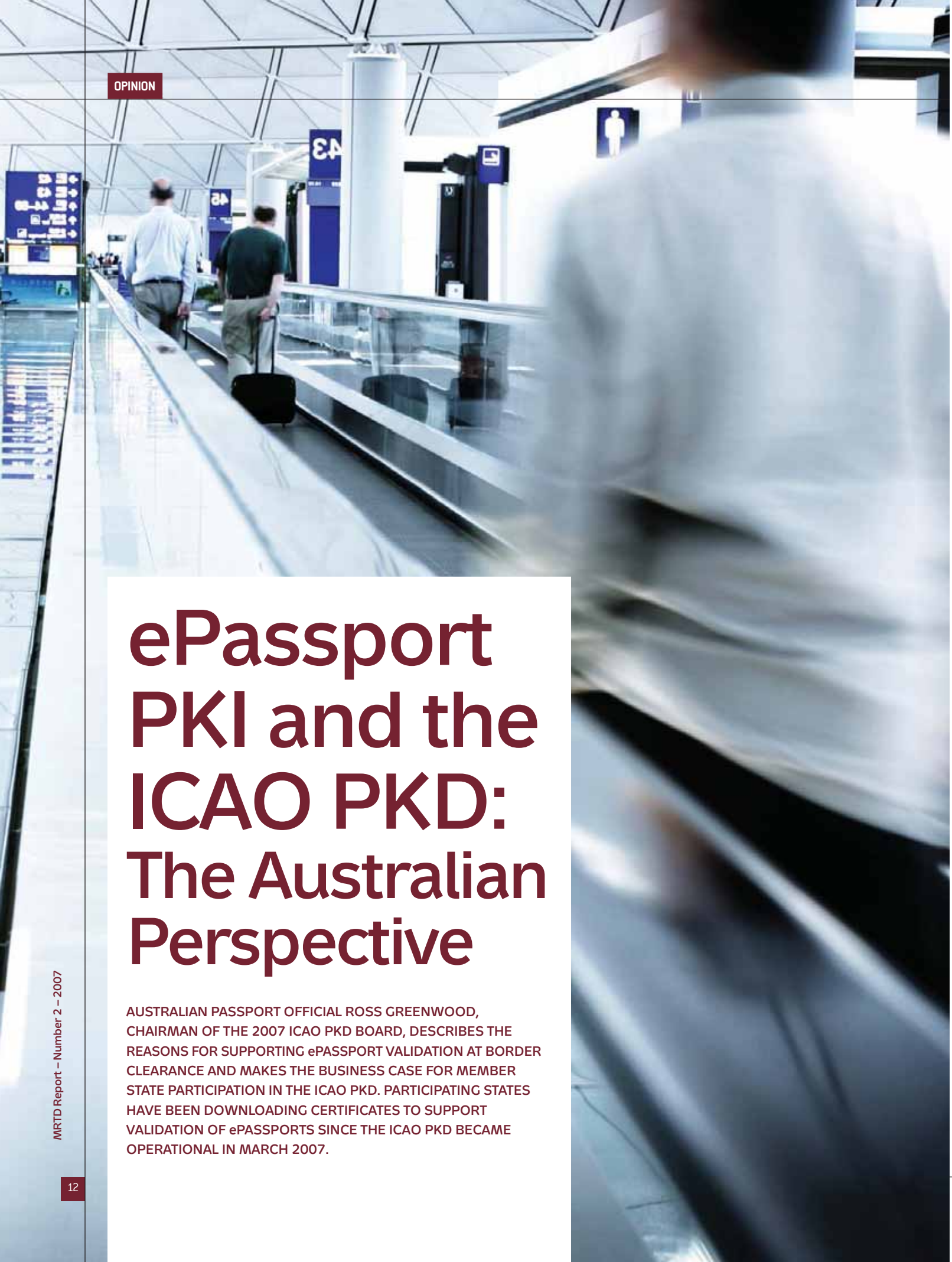
Enrolment device for recording of biometric data

For the collection of biometric characteristics (such as face or finger) of the applicant in an electronic way Sdu Identification developed an enrolment device and software. The enrolment device can be integrated as a front office device in every process where applications are digitised and plays an essential role at issuance of the travel documents.

Sdu IDENTIFICATION

PO Box 5300
2000 GH Haarlem
The Netherlands

Telephone +31 23 799 51 46
Fax +31 23 799 51 80
www.sdu-identification.nl
sales@sdu-identification.nl



ePassport PKI and the ICAO PKD: The Australian Perspective

AUSTRALIAN PASSPORT OFFICIAL ROSS GREENWOOD, CHAIRMAN OF THE 2007 ICAO PKD BOARD, DESCRIBES THE REASONS FOR SUPPORTING ePASSPORT VALIDATION AT BORDER CLEARANCE AND MAKES THE BUSINESS CASE FOR MEMBER STATE PARTICIPATION IN THE ICAO PKD. PARTICIPATING STATES HAVE BEEN DOWNLOADING CERTIFICATES TO SUPPORT VALIDATION OF ePASSPORTS SINCE THE ICAO PKD BECAME OPERATIONAL IN MARCH 2007.

ePassports improve the inherent security of travel documents by duplicating the biographical information and photograph from the data page onto a chip. As a result, provided the data on the chip is read during the border clearance process and compared to the information on the data page, any fraudulent alteration of the document needs to be achieved in two places.

However, the real improvement in document security of ePassports is the Public Key Infrastructure used to secure the information written to the chip, thus providing an opportunity to confirm that the information on the chip was put there by the issuing authority, and not subsequently altered. The ICAO PKD is a repository for current, validated ePassport public key certificates which are available for download.

The full border security and aviation security benefits of ePassports will be realised when validation of the PKI certificates for each ePassport becomes the pervasive practice of border control authorities around the world. If this can be achieved, border control authorities in all countries, by being able to readily identify and remove from circulation bogus ePassports, will assist passport issuing authorities to manage the integrity and reputation of the documents they issue.

To date, the ePassport PKI design and the design of the arrangements for exchange of certificates has largely been managed by the passport issuing authorities, the organizations responsible for generating the PKI certificates.

However, it is border control authorities who are the primary client for passport validation using PKI certificates.

The fundamental feature of any PKI application, including that for ePassports, is that:

- **Security** is guaranteed by "private keys" that are retained by, and known only to, the issuing authority.
- **Validation** is achieved by the exchange of "public keys".

The ICAO PKD has been designed to preserve a high level of data security, appropriate for the handling of the public keys associated with ePassports. It remains the responsibility of individual States to preserve the absolute integrity of the private keys associated with their documents, and to advise if and when this integrity is compromised.

Debate continues about how to optimise the ePassport PKI design to optimise security of the certificates—a conversation dominated by technical experts from the passport issuing authorities.

Less attention has been given to ensuring that the arrangements for the exchange of "public key" certificates are reliable, timely and efficient—the conversation of interest to the border control authorities who want to be able to validate all ePassports, from all the States that issue them.

A point lost in much of the technical discussion is that security in the exchange of public key certificates process is a second order concern, because the public keys in themselves contain no personal data, and no data that can compromise PKI validation. It is instructive that the "P" in the acronym PKI stands for "public."

Australia's view is that the challenge facing the ePassport PKI are:

1. Achieving agreement on the PKI design, to ensure security of the certificates, and;
2. Ensuring the most extensive possible sharing of validated "public key" certificates, from all ePassport issuing countries.

ePassport PKI and the ICAO PKD

Under the current design, the ICAO PKD contains Document Signer Certificates (C_{DS}), a public key, that have been validated by Country Signing Certificates (C_{CSCA}), a separate public key, that have not subsequently been the subject of a Certificate Revocation List (CRL). Under this design it is a requirement for States to forward the relevant public key certificates (i.e., C_{DS} & C_{CSCA}) and CRLs to ICAO to ensure that only validated, current C_{DS} are included in the ICAO PKD*.

Subsequent to this design being finalised, most ePassport issuing countries have decided to include the C_{DS} on the chip in their ePassports. If agreement can be reached for this practice to be mandated, there is scope to simplify the design of the ePassport PKI, and in turn of the ICAO PKD. This technical conversation will also need to resolve the divergent opinions that remain with respect to the distribution of public keys, in particular those associated with the Country Signing CA Certificates (C_{CSCA}).

Distribution of Public Key Certificates

Australia commenced production of ePassports in October 2005. At that point the ICAO PKD was not operational, and it was not

* The ICAO technical report on PKI for MRTDs states at 2.2.2 that "Country Signing CA Certificates (C_{CSCA}) are not part of the ICAO PKD service" but goes on to state in the next sentence: "The PKD however SHALL use Country Signing CA Certificates (C_{CSCA}) to verify the authenticity and integrity of the Document Signer Certificates received from participating States, before publishing," and at 2.2.1 states that "Each Country Signing CA Certificates (C_{CSCA}) generated by each State MUST also be forwarded to ICAO for the purpose of validation of Document Signer Certificates (C_{DS})." Certificate Revocation Lists similarly are required to be copied to ICAO.

clear when it would become operational. In order to manage the exchange of public key information until such time as the ICAO PKD commenced operating, Australia established a Local Key Directory (LKD) as a repository for the validated, current C_{DS} of all ePassport issuing countries.

The Australian Passport Office has operated its LKD based on the bilateral exchange by email of public key certificates since December 2005. E-mail was chosen as the only practical means of bilateral exchange of certificates because Australia's diplomatic representation in more than 80 countries falls well short of a presence in all the potential ePassport issuing States. In the period since December 2005, Australia has invested significant effort in establishing and maintaining e-mail contact lists, monitoring ePassport implementation timetables, and requesting and distributing public key certificates and revocation lists.

Our experience of distributing Australian public key certificates broadly reflects our experience in receiving them. Notwithstanding all efforts, few of the emails in which we distribute our public key certificates are acknowledged, most remain unacknowledged and a significant number fail. Successful transactions in one month are followed by failure or unacknowledged emails in subsequent months.

Australia's assessment is that bilateral exchange of public key certificates is unreliable, slow and inefficient. The reasons for this are that there are myriad practical constraints on bilateral exchange:

- The scale required to manage bilateral exchange of certificates is formidable—80 countries issuing ePassports x new CRL x new C_{DS} x new C_{CSCA} = a large volume of transactions for each border control authority to manage.

- The upload transactions are not straightforward:

  - Prior to public key certificates or revocation lists being loaded to a local directory, the credentials of the person and organization sending the certificate must be established. This is problematic because:

    - Contact persons change.

    - The names of organizations responsible for issuing ePassports change.

    - The organizational units responsible for managing certificate distribution change.

    - Sometimes even the organization itself responsible for passport issue changes.

    All these changes lead to changes in email addresses, or the alternative contact details required to ensure accurate addressing by other means.

  - Organizations receiving certificates will typically be involved in border control. Organizations sending certificates are involved in passport issue. Other organizations responsible for airport security may have an interest in receiving the certificates, and the foreign ministries that manage diplomatic communication channels must be aware of all changes in order to send certificates to the correct destination.

  - In order for public key certificates to be uploaded, datasets need to be assessed and tested as meeting specifications in order to be accepted for upload. Where the data set is rejected a bilateral communication is required to resolve the issue. This is a common occurrence.

In summary, as jurisdiction varies between countries, border control agencies receiving certificates are impossibly placed to maintain reliable contacts with the passport issuing organizations from other countries that are sending them.

Moreover, a system that relied on bilateral exchange of certificates between governments would exclude access to non-Government clients for ePassport validation, such as airlines, airport operators and the financial industry.

All of the foregoing suggests that the exchange of certificates is a process that can more simply, efficiently and effectively be done via a central point like the ICAO PKD.

Conclusions

The Australian Passport Office believes that validation of ePassports can contribute to improved security of travel. We therefore support extensive, reliable, timely and efficient exchange of "public key" ePassport certificates.

Australia believes that the ICAO PKD is the best vehicle to deliver this goal.

We want Australian travel documents to be secure. We want to assist other governments in identifying and withdrawing from circulation fraudulently altered or otherwise falsified Australian and other ePassports. Australia believes it is in the interests of all States that the scheme or schemes in place to support validation of ePassports grow in their coverage.

However, it is also the case that the ICAO PKD needs to change:

- The current design predates the widespread adoption of the practice of including C_{DS} on the chip in ePassports—there is scope to simplify the exchange of "public key" certificates, to redesign the validation process and to change which certificates are exchanged and how this is achieved.

- The current costs of participation are an impediment to expansion of the ICAO PKD. With the establishment phase complete and the ICAO PKD operational there is scope to reduce fees significantly as membership in the PKD increases.

The ICAO PKD Board and the ICAO Secretariat are working on these issues and engaging those with alternate views.

Many countries are now producing ePassports, but many fewer are reading data from the chips on ePassports at the border. However, Australia expects interest in validating ePassports and participation in the ICAO PKD will now start to grow as the number of ePassports in circulation makes the required investment in border processing hardware, systems integration and changed business processes worthwhile. ■

Achieving Interoperability

By Claudia Hager, MBA, Executive Director of the Austrian State Printing House (OeSD)

EVEN THE MOST SECURE OF ePASSPORTS IS ONLY AS USEFUL AS THE READER THAT CAN COMMUNICATE WITH IT. CLAUDIA HAGER, EXECUTIVE DIRECTOR OF THE AUSTRIAN STATE PRINTING HOUSE, OUTLINES THE EVOLVEMENT OF ePASSPORT/READER INTEROPERABILITY AND THE ISSUES THAT NEEDED TO BE OVERCOME BEFORE TRULY RELIABLE AND GLOBAL DATA INTER-CHANGE COULD BE ACHIEVED.

There were two primary preliminary considerations regarding global interoperability and the new generation of chip-based travel documents: the need for additional storage capacity for biometric data, and; an open platform for data storage and data reading. To satisfy both requirements, ISO 14443, applicable to contactless chips, was chosen as a globally interoperable medium that as an added benefit was not bound to a specific or proprietary vendor's application.

The standardized chip provides enough capacity to store a variety of raw biometric data types. Although ISO 14443 clearly specifies the chip's technical requirements, the standard also provides for flexible tolerances which can be implemented differently depending on a manufacturer's individual priorities. It was therefore of the utmost importance to test the various beta-version ePassports (with different chips, operating systems, chip locations and data sizes) and readers in multiple environments to judge the effect of these varying tolerances and more closely reflect the actual conditions of live performance.

The Road to Interoperability

During the last three years, several governments have hosted interoperability tests. Passport and chip manufacturers, operating system developers and reader manufacturers were invited to participate in live tests of their products in the designated area of application, namely border crossing. ePassports (or simply 'chip inlays' in the early stages of the test series) were cross-tested against each other under a variety of interoperability scenarios. The target was to benchmark the performance rates and isolate areas for improvement.

The first interoperability test was hosted in Canberra, Australia, in February 2004. The last and biggest test sessions were held in Singapore in November 2005, and in Berlin, Germany, in May/June 2006. Figure 1, below, gives an overview of all the interoperability tests performed during this period. The test sessions evolved from a series of general assessments on to

FIGURE 1

List of locations, number of chips (eMRTDs), readers and participants present at the various ePassport interoperability tests conducted since 2004.

	eMRPs	Readers	Participants
Canberra	10	6	–
Morgantown	100	18	150
Sydney	120	15	~100
Baltimore	~25	8	~20
Tsukuba	600	35	200
Singapore	140	40	240
Berlin	443	45	400

FIGURE 2

Evolution of interoperability test objectives.

Interoperability Test	Objective
Canberra	Examine compatibility of Type-A & Type-B and explore additional requirements that need to be specified
Morgantown	Research if ICAO specifications addressed all basic issues in multi-vendor condition
Sydney	Investigate incompatibility problems and test readability/usability for corrections of specifications
Baltimore	Determine the operational impact on primary inspection systems
Tsukuba	Test with standard equipment and measure reading speed/chip characteristics with scientific approach
Singapore	Promote interoperability between ePassports and ePassport readers including optional features
Berlin	Simulate border situations, no standard data sets allowed, focus on reliability of reading rather than speed

more focused measurements of specific abilities as the actual 'state-of-the-art' became more apparent. Figure 2 on the preceding page provides an overview of the objectives* of each of the tests and illustrates the progression that occurred.

In order to obtain comparable reading data, a common software platform called the Golden Reader Tool (GRT) was developed by the Essen Group (a group of specialists from UK, The Netherlands and Germany that met in the city of Essen in 2004). This software continues to serve as an interoperability testing tool for compliance with the ICAO specifications on the application and security level. The GRT has been constantly updated and provides comprehensive data related to the ePassport reading process.

An eMRTD read and accepted by the GRT can be considered as being compliant with the LDS and PKI standards defined in 9303 Part 1, 6th edition. The tool conveys additional information—such as the security mechanisms being applied and the data fields being utilized—as well as the facial and fingerprint images and MRZ data.

Apart from the widely employed GRT program, other testing software has also evolved. The Japanese test hosts developed proprietary "NMDA Test Software," and the hosts of the Singapore sessions also used their own "Interfest Test Software." Figure 3, below, shows the technological development of the samples and readers over the past two years and includes a glossary of applicable terms and acronyms used for this purpose.

FIGURE 3

Technological development of samples and readers over the past two years and glossary of terms and acronyms employed.

	Canberra	Morgantown	Sydney	Baltimore	Tsukuba	Singapore	Berlin
Reading	Poor	OK	OK	Not Satisfactory	Good	Very Satisfactory	Very Good
Data Set	–	Silver	Silver & 34k photo	Silver	Tsukuba	Orchid, Individual	Only Individual
Tool	–	–	–	GRT	GRT, NMDA	GRT, NMDA, Interfest	GRT (50%), individual
Read Range	–	2, 5, 10 cm, rotated	Rotated, upside down	–	0, 2 cm at four positions	0, 2 cm, Flip	0 cm
Eavesdropping	–	Yes	–	Shield Test	–	–	–
Bps Average	106 kbps	212 kbps	212 kbps	212 kbps	424 kbps	848 kbps	848 kbps
Time Average	> 30 sec	> 30 sec	30 sec	~ 20 sec	3 sec - 10 sec	2 sec - 5 sec	5 sec
SoD Test	–	–		–	Yes	Yes	Yes
BAC	–	–	–	–	Yes	Yes	Yes
AA	–	–	–	–	–	Yes	Yes
EAC	–	–	–	–	–	Yes	Yes

Reading The first line gives the general impression participants and organizers had from the test sessions.

Data Set In many tests a standard data set was provided to the participants in advance so they could all load the same data onto the ePassports submitted for testing. The advantage was the comparability of the data with the same image size on different chips, different operating systems, different antenna geometry and different chip locations in the passports that were tested. The disadvantage was that the readers had pre-stored the MRZ data for BAC-reading and therefore all reading parameters were adapted to the sample data set. Presenting an ePassport with different data still caused substantial problems for the reader. This was not a realistic border scenario where–hopefully–each ePassport has a different data set stored in the chip. Hence the last interoperability test in Berlin only allowed individual data in order to better simulate a border environment. A server for uploading the different public keys used by the passport manufacturers was available, however all passports had the public key stored on the chip.

Tool The type of reading software is listed here.

Read Range This was a set of tests measuring the position of the document and the distance from the reader antenna.

Eavesdropping Tests on eavesdropping were carried out and analysed.

Bps Average This shows the acceleration in reading speed over time, measured in kilobits per second.

Time Average Very generally, this line gives the average reading speed with/without BAC and different data sizes. Reading duration proportionally decreased when reading speed increased.

SOD Test The digital signature of the data was verified where indicated.

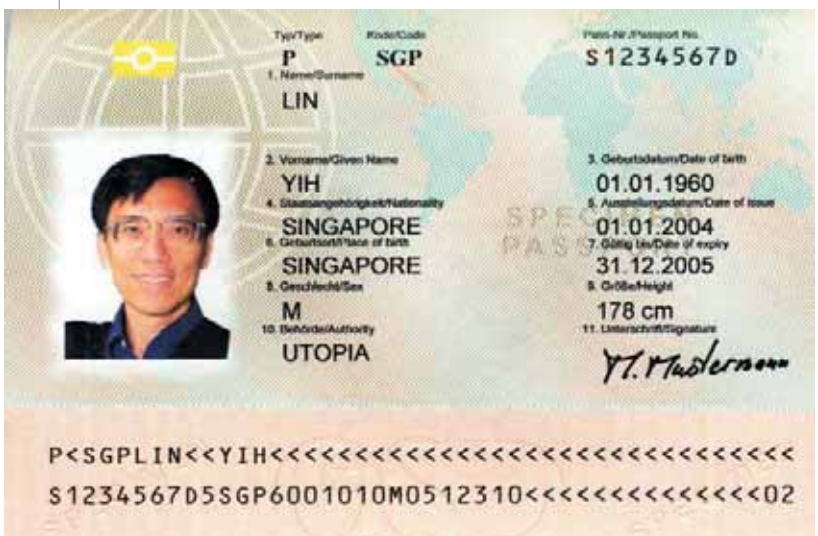
BAC A test of Basic Access Control was included.

AA A test of Active Authentication was included.

EAC A test of Extended Access Control was included.

* Information obtained from Mr. Junichi Sakaki (Co-chair ISO SC17/WG3/TF4) during interoperability tests in Singapore, November 2005, updated by Claudia Hager.

One example of a sample data set, in this case the «Orchid Data Set» used in the Singapore Interoperability Test.



In the test session in Berlin, GRT was once again the most commonly used software (used by about 50 per cent of the readers). Reading speed was around 5 seconds on average due to the greater number of security layers involved (at least BAC, often also AA). Only individual data sets were allowed in the tests and none of the previously used test data were employed. The outcome of the Berlin and earlier testing sessions and the major issues that emerged as a result of each are summarized in Figure 4 *(see table, page 19)*.

The organizers of the Berlin test also smuggled two wrongly-personalised passports into the group of test samples. One had an incorrect hash value, the other a faulty digital signature. This was an excellent means to detect those few readers that firstly verify the digital signature and secondly give a clear message in the user interface to the border officer about the cause of the reading error.

Analysis of Interoperability Issues

ePassport operating systems, antennas, chip integration and reader manufacturing have developed rapidly during the last three years. General and basic issues surfacing in the first test sessions were soon solved, while later tests focused on more detailed and specific questions.

It is important to note that all test sessions were followed by a detailed report which was distributed to all participants and which were then made available to the industry. The awareness

of the potential issues was highlighted and is reflected in the Supplements to the ICAO Doc.9303 Part 1, and huge improvements were obvious between each of the test sessions.

The results and findings of the Singapore and Berlin tests showed substantial improvements and fewer issues were spotted. Fifteen new reader manufacturers participated in these sessions; however it was clear that reader manufacturers who had already participated in earlier test sessions had more stable reading performance than newcomers.

After the last test session, it could be concluded that the maturity of ePassports had advanced to the implementation level, as field-proven experience has now demonstrated. For the reader manufacturers it can be generalised that those having the experience of previous interoperability tests and the background of border control processes performed extremely well. Thanks to the series of test sessions, the new generation of travel documents was globally and jointly developed and are now fit for the implementation process. ■

FIGURE 4

Summarized outcomes and major issues discerned during interoperability testing: 2004–2006.

Interoperability Test	Findings
Canberra	Need to specify 'Reset' time Antenna design has great influence on performance Power requirement too high OS implementations in early stage
Morgantown	Need to specify APDU Command details not correctly implemented Eavesdropping technically possible up to 10m Jamming threat with more than one chip
Sydney	Field Strength sensitivities Chip detection CBEFF & LDS format error
Baltimore	Slow reading speed Poor ergonomic usability Power problem SoD is not verified by readers
Tsukuba	Short File Identifier not used as specified 3 byte Le needs clarification BAC successfully implemented
Singapore	Antennae orientation can be an issue AA, EAC, BAC lite many variations
Berlin	Low quality MRZ (necessary for BAC) Type B sensible to field strength variations Shielded passports difficult to read Reader conformity tests are necessary

Moving to the Second Generation of Electronic Passports:

Fingerprint biometrics for enhanced security & privacy

Excerpts from the *Gemalto White Paper* courtesy of Eric Billiaert, Marketing Communications Manager, Identity, Gemalto, July 2007

The European Union has made it clear that a new security mechanism known as Extended Access Control (EAC) is necessary for access protection. EAC implementation is a complex affair and requires skilled handling and cooperation from all EU members throughout the migration process.

The new system requires the set up of a complete Public Key Infrastructure (PKI) and two new security mechanisms. This development has a significant impact on all major players, including governments, national printers, the ePassport industry and citizens.

As the industry moves forward and interoperability tests proceed unabated, it is clear that countries that have yet to broach EAC migration have a lot of work to do. Executed properly, EAC offers huge advances in more secure travel documents and tighter border control, but the deadline is fast approaching.

First Generation ePassports

In the aftermath of September 11, 2001, the US changed its entry requirements and required all countries participating in the Visa Waiver Program to start deploying electronic passports as of October 26, 2006. Subsequently, in December 2004, the European Commission (EC) passed the (EC) 2252/2004 regulation, calling for common technical specifications to enable biometric markers on travel documents. Then, on February 28, 2005, the EC adopted the first phase of the ePassport technical specifications, which set August 28, 2006 as the deadline for all member states to include a facial biometric image on ePassports.

Pioneering states such as Sweden and Norway were first to introduce a fully European- and ICAO-compliant ePassport using facial biometrics in October 2005. Twenty-three other US Visa Waiver countries met the August 28, 2006 deadline.

Second Generation ePassports

The second phase of the technical specifications from (EC) 2252/2004, which called for the use of fingerprints as a second biometric marker in ePassports, was adopted by the European Commission on June 28, 2006. The deadline for compliance is set for June 28, 2009. Under these specifications, when implementing fingerprint images on second generation ePassports access rights to read the fingerprints must be further protected by a security measure called Extended Access Control.

Extended Access Control

First generation ePassports are meant to be easily read. They have also been carefully designed to be tamper- and forgery-proof. The following security measures were implemented with first generation ePassports:

Passive Authentication (mandatory with ICAO)—Allows reader to check the authenticity of the data stored in the microprocessor. The data is digitally signed by the issuing country.

Basic Access Control (mandatory for phase one EU ePassports)—Prevents passport reading without the holder's involvement. To protect against skimming and eavesdropping, a key must be used to gain access to the microprocessor and the communication is encrypted. This requires that the passport be intentionally shown and optically read before access to the chip is granted.

Active Authentication (optional with ICAO)—Prevents the copying of the microprocessor. The readable data in the microprocessor contains a public key and the corresponding private key is stored in the microprocessor but cannot be read.

Extended Access Control (mandatory for phase two EU ePassports)— Limits access to additional biometrics to the issuing country and countries that have permission from the issuing country. This capability will be used to protect fingerprints, iris scans (optional) and other privacy-sensitive data.

ICAO recommends the use of EAC to protect fingerprints and iris scans, but leaves the definition of the actual mechanism up to the individual country. The technical specifications for the EU were prepared by the Brussels Interoperability Group (BIG) and approved by EU article 6.

Tightened Security with EAC

The chip authentication stage of EAC is based on a chip-dedicated Diffie-Hellman asymmetric key pair using either DH (PKCS#3) or ECDH (ISO 15946), the latter implementing elliptic curve cryptography. The public part of the key is digitally signed by the issuing country, while the microprocessor contains the matching private portion which can never be read out.

Through chip authentication, the terminal ascertains that the chip possesses the private portion, thereby identifying it as genuine and making chip cloning unfeasible. An attacker trying to the ePassport faces the practical problem of computing the microprocessor's private key given the public elements (which can always be obtained freely). Carrying out this task is commonly referred to as the Discrete Logarithm problem and requires massive computational resources even for practical key sizes.

A brute-force attack, where the attacker gathers as much computational power as possible and implements the fastest known discrete-log extraction algorithm (currently GNFS) would typically require 273 (respectively 2103) operations for a 1024-bit (resp. a 2048-bit) DH public key, and 2128 operations for a 256-bit ECDH public key. This represents several decades of unceasing computations over a large-scale computer network and by far exceeds the limits of practicality.

Extended Access Control consists of three phases: Basic Access Control (BAC), followed by; Chip Authentication, and; Terminal Authentication. Basic Access Control is used to prevent skimming and eavesdropping. This is achieved by encrypting the communications using a symmetric key obtained and created by reading the optical data in the Machine Readable Zone (MRZ). Chip Authentication performs the same function as Active Authentication in the ICAO standards, i.e., proving the microprocessor is genuine and thus protecting the electronic passport against cloning. It will also enhance the BAC security mechanism by replacing the encryption key with a totally random key. Terminal Authentication aims to prove to the microprocessor that the terminal is allowed to access the data on the microprocessor.

This access is granted through a chain of certificates, the root of which is the passport issuer. In other words, only the issuer of the passport controls who can access the data on the document. The introduction of EAC will not make the security mechanisms of BAC obsolete, but it will supplement them. In the future, the entire reading process for a biometric ePassport will always be carried out in three consecutive steps: Basic Access Control, Chip Authentication and Terminal Authentication.

How Does EAC Work?

In the Chip Authentication stage, when the reader authenticates the microprocessor, a standard PKI challenge-response process between the reader and the microprocessor is used whereas Terminal Authentication process is a somewhat more complex system.

To decode the encrypted data contained on an ePassport microprocessor, the border control authorities of the visited country must request authorization to access the passport holder's fingerprint data from the home country where the ePassport was issued. Friendly countries will have mutual agreements in place that enable their border control authorities to share information.

Subsequently, a specially adapted key agreement protocol will allow both the issuing and inspecting countries to generate the same secret and unique key, which is contained within every second generation passport, to access the information needed. Every second generation ePassport can use the secret key to establish a secure communication channel with an inspection system at a border control post and to prove that it is the original passport and not a counterfeit. The trustworthy public key allows the ePassport mechanism to verify the credentials presented by the inspecting party and then permit or deny access to biometric data.

The fact that with EAC the ePassport challenges the inspection system before providing sensitive data ensures that the passport issuer retains control over who is allowed to view the secure data stored on an ePassport's microprocessor, since each government controls the issuing of credentials to the border control posts of other states. Second generation ePassports are thus armoured against counterfeiting and can protect their biometric data more securely *(see Figure 1, below)*.

FIGURE 1

EAC Terminal Authentication

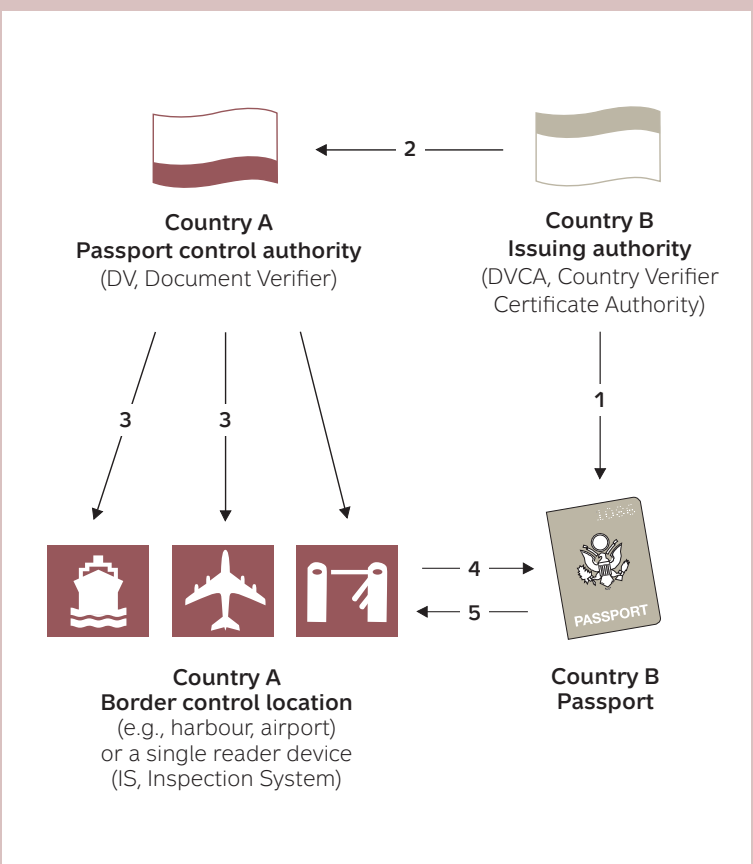
1. CVCA certificate from the issuing country is stored on the passport chip during passport personalization. This certificate will be used to verify the inspection system's certificates (access rights to fingerprint data) in the passport reading step.

2. Country B certifies (i.e., gives permission to) Country A's passport control authority to authorize their access to read the fingerprint data from Country B's passport.

3. Country A's border controlling authority certifies (i.e., gives permission to) its border control locations or individual devices (Inspection Systems) to have an access to read the fingerprint data from Country B's passport.

4. Country A's border control reader (Inspection System) shows Country B's passport its authorization to access the fingerprint data on the chip.

5. Country B's passport allows reading of fingerprints once the inspection system has proven its authorization from the Country B.



The Implications for Key Players

All players involved in enrolment, passport manufacturing, personalization and border control processes must consider that many complex competencies will be involved in second generation ePassport deployments, some of which are completely new. These competencies include the following:

- Cryptography and advanced authentication techniques.
- Implementing new EAC compliant operating systems on the microprocessors in use.
- Management of a PKI certificate authority, responsible for the registration of public keys, revocation of certificates, etc.
- Biometric data capture, storage and matching of configurations in accordance with both high security standards and strict privacy policies.
- Capture of enrolment data material, preparation and formatting.
- Authenticating individuals' identities with the appropriate government entities and verifying that the applicant provides valid ID credentials.
- Establishing a chain or network of trust, especially internationally.

The Impact on Enrolment

The most obvious requirement for second generation ePassports are the reader stations that will be installed for fingerprint collection at passport application agencies. The least visible element—to citizens—is how to protect fingerprint privacy all the way from enrolment to personalization.

As the purpose of EAC is privacy protection, security issues become apparent not only when the fingerprints are housed on the microprocessor, but also throughout the whole application and issuing process. Even the staff operating the passport

enrolment system must not have access to an individual's fingerprints.

To avoid heavy and expensive security mechanisms for enrolment stations, systems based on PKI technology have been developed and can conveniently be used to satisfy these privacy requirements. The system used for securing privacy for the whole issuing chain—from enrolment to personalization—is termed "end-to-end" privacy.

The Impact on Passport Manufacturing

When implementing second-generation ePassports, the biggest change for passport booklet manufacturers and security printers is the passport cover or datapage containing the microprocessor that meets all the interoperability and security requirements set by EAC. Compared to first generation ePassports, there is a vast set of requirements that needs to be fulfilled. First of all, a fully EAC-compliant operating system must be used. In addition, 32 KB microprocessors are not big enough. A minimum 64 KB memory capacity is needed as MRZ and passport holder data take up some 5 KB, facial images 20 KB, and fingerprints some 10 KB each.

There is also a requirement from the EU which stipulates that the operating system on the microprocessor must be security certified. This security certification must be done following the international Common Criteria process designed for evaluating secure IT systems. The context of the second generation ePassport evaluation—a document entitled the Protection Profile—has been developed by European national standard bodies and security organizations like BSI (Bundesamt für Sicherheit in der Informationstechnik) and DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) with support from the industry. It was endorsed in EU Article 6.

The purpose of the certification is to provide an independent 3rd party evaluation that guarantees that security mechanisms in ePassports' contactless microprocessors are robust enough to withstand even the most sophisticated intrusion attacks. Operating system and electronic datapage (paper, polycarbonate...) suppliers will take care of the operating system development and CC security evaluation, ensuring a smooth and convenient transition for passport manufacturers.

The Impact on Personalization

There are several new challenges facing personalizers, mostly centring around security and productivity. New data and keys must be prepared, requiring updates of numerous systems at the personalization site. Implementing EAC will require changes for the key management system,

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

Second Generation ePassports
Key Challenges for Governments and Border Control Authorities

- At the enrolment stage, to create the infrastructure to capture fingerprints.
- At the production stage, to ensure privacy and secure storage of personal data.
- At the border control stage, to adapt the infrastructure to biometric verification

as unique asymmetric Diffie-Hellman keys are to be generated for each passport and more certificates need to be incorporated on the microprocessor. It is also important during the personalization stage to protect fingerprint privacy before the data are securely stored on the passport microprocessor. This is achieved through end-to-end privacy between enrolment and personalization.

It is important to remember that, after personalization, readers used for passport quality assurance must perform both Chip Authentication and Terminal Authentication to verify the certificate confidence chain from the issuing authority (CVCA, or Country Verifier Certificate Authority), to get access rights to read the data from the microprocessor, and finally to confirm their accuracy. As in normal Terminal Authentication during border inspection, these certificates must also be renewed periodically.

Also, while some 25 KB of data were loaded on the microprocessor with first generation of ePassports, some 45 KB must be loaded on the microprocessor for EAC passports. This has an effect on productivity unless the latest personalization technologies are put in place to offset the expected time increases.

The Impact on Border Patrol

As with enrolment, the most visible aspect for users during border control is that new reader stations for fingerprint reading will be installed. Not only will fingerprint scanners be installed, but the entire border control reader must be compatible and equipped with the document authentication software linking to the passport controlling authority (DV, Document Verifier). In practice, this means that the whole reader system needs to be updated.

This in turn means that the whole PKI scheme required by EAC must be extended to the inspection system on borders in order to be able to propagate, verify, and revoke numerous certificates. In addition, the inspection systems at border control stations must be compatible with several algorithms such as RSA and elliptic curves in the various passports they'll need to process.

The amount of data read from the microprocessor will be twice as large compared to first generation ePassports. The EAC mechanisms and the enhanced security calculations on the microprocessor are to be performed as well, with all of these factors resulting in increased inspection times unless newer readers are employed. With top-quality readers and operating systems, the impact on reading times will still be less than three seconds compared to first generation ePassports.

The Impact on Governments and Citizens

EAC stands a good chance of success as long as governments support this evolution with an adequate framework of laws, manpower and infrastructure. In almost all EU countries, the introduction of biometric passports has legislative implications and regulations must be adapted or revised.

New technologies such as smart cards, biometrics and contactless technology have gained attention and their usefulness is becoming better understood, but questions of privacy and security continue to hold the prevailing political focus. Countries that have successfully tested eID schemes recognize the importance of safeguarding citizens' privacy and communicating the potential benefits of these new solutions, and public opinion and the activities of pressure groups can potentially influence how second generation ePassport mechanisms are designed and accepted during this development stage.

Uniquely, the EAC protocol requires authorization from the ePassport issuer to allow certain specific data groups to be read by specified groups of readers. Without this protection, anyone with the necessary technical skills could read all the

data on a passport. When implemented, EAC will have the effect of strengthening all the other security measures because the protocol will not operate as a stand-alone element.

EAC-equipped readers will link back to national Public Key Directories (PKD), meaning that the Passive Authentication need no longer blindly trust the document signer certificate held within the ePassport. Instead, this certificate can be validated against the country signer certificate in the PKD.

In such a scenario, governments will provide a second and more significant block of security infrastructure for the benefit of the citizens of the issuing countries. This enhanced security of digital identities eliminates the threat of identity theft, thus addressing privacy concerns, while increased service levels via automated gates and fast track lines can slash queuing times by a third.

The Current Status of Second Generation ePassport Implementations

In August 2006, Singapore implemented a biometric passport including fingerprints and a related security scheme. The implementation of BioPass—as the Singapore ePassport is known as—has gone smoothly according to authorities.

Some privacy concerns have been voiced over the introduction of biometrics in travel documents. The authorities have clearly stated that biometric technology will not restrict civil liberties, that it will make it more difficult for terrorists to assume false identities, and that it will also facilitate legitimate travel since accurate identity verification will be made easier. This is a national initiative.

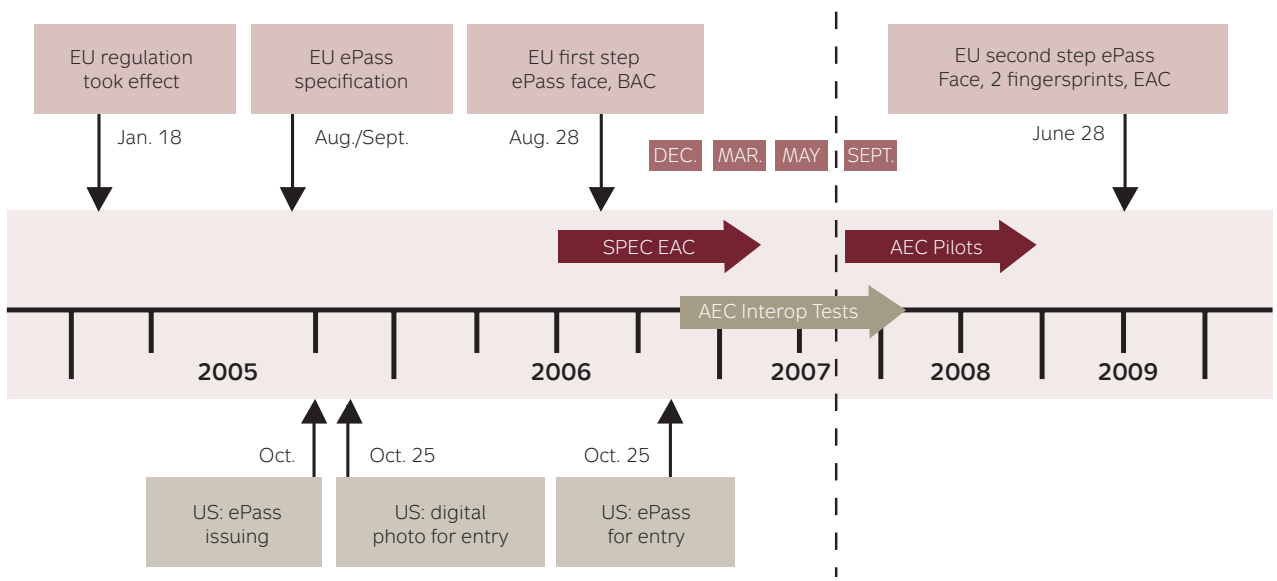
In the EU, the Brussels Interoperability Group (BIG) was formed in 2006 to resolve the technical issues related to the development, implementation and application of EAC in the member states. The group's tasks include finalizing the certificate policy for EAC, setting up a pilot implementation, and providing guidelines to EU member states on the implementation of technical specifications.

Preliminary EAC interoperability sessions were held in December 2006 in Italy to ascertain the level of common understanding of the EAC specifications. After this session, comments and clarifications were posed by countries and manufacturers to improve the previous specifications. In mid-March, 2007, an official interoperability session was held in Prague where all the EAC passports inspected with an official inspection system successfully passed the test. This proved that EAC interoperability is guaranteed on a local scale.

Nevertheless BIG members considered that more complete cross tests were necessary to enhance the interoperability of the global system. In May 2007, the Portuguese Aliens and Borders Service (SEF) in Lisbon hosted the interoperability tests performed by various European Countries set up by BIG of the European Com-

FIGURE 2

Timeline of International interoperability tests of EAC hardware and software solutions.



mission. The goal was to check the proposed EAC test suite specifications developed by the ad hoc group (participants from France, Germany, Joint Research Centre, The Netherlands, UK) with verification of the certificate update in the ePassport.

This was a new release for the majority of suppliers. Preliminary results of test suites illustrated firstly that the AFNOR-BSI specifications have been well defined and well understood by developers, and secondly that the four tools are well-advanced and therefore most of the ePassports were tested successfully. Two methods for certificate verification were used, and results should be considered as indicators of an advance in the two specifications (passport and test tools), taking into account that developers had only two weeks to prepare.

For countries and members of the industry this is good news, as a choice in test platforms means the availability of competitive tools. However, developing test tools with complete specifications does take time, and therefore a commitment for September 2007 is crucial. Pilot tests are set to begin in several countries by this time, and full-scale interoperability testing of EAC readers and passports between countries is planned to take place in 2008. For a more complete timeline please refer to Figure 2 on page 25.

Conclusions

In a world where international terrorists and criminals are becoming ever more sophisticated in their use of cutting-edge technology, it is imperative that national agencies charged with securing borders stay one step ahead by employing systems and processes that can foil any attempt to gain illegal entrance through border checkpoints.

The second generation of ePassports with fingerprint biometrics is one more tool that agencies can use in order to ensure that the person presenting a passport to a border guard is, in fact, the person represented on the travel document. Extended Access Control through the use of strong encryption and PKI-based public/private key pairs to ensure impenetrable data transmission will provide enhanced border security for years to come.

EU countries are expected to introduce second generation ePassports by mid 2009. To succeed with such a challenging but achievable goal, government agencies and state printers should liaise with global technology partners able to integrate the new document production processes. ■

Key Priorities per Sector

Passport Booklet Manufacturers

- Select new, higher performance microprocessors together with EAC compliant operating systems in inlays, in passport cover, in polycarbonate datapage.

Enrolment System

- Implement biometric data capture, storage and matching of configurations (in accordance with both high security standards and strict privacy policies).
- Install fingerprint scanners at passport application premises.

Personalization Site

- Update key management system for massive key generation and management of fingerprint end-to-end privacy.
- Update quality control stations with Inspection System and Document Verifier functionality so that they can simulate border control terminal authentication.
- Use state-of-the-art personalization technologies to offset personalization time increase and avoid throughput deterioration.

Governments

- Set up and manage a Public Key Infrastructure (PKI) certificate authority (registration of public keys, revocation of certificates, etc.
- Create a chain or network of trust, especially internationally.

Border Control

- Install fingerprint scanners.
- Update/renew the border control reading systems to be compatible to and equipped with the document authentication software with a link to the passport controlling authority (DV, Document Verifier).

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, Russia, Singapore, Slovenia, Sweden and the United States of America.

gemalto
security to be free

Aine Ni Fhloinn, Director, InHouse Training

eLearning for ePassports

WHEN ICAO WENT SHOPPING FOR THE IDEAL SOLUTION TO PROVIDE STATES WITH THE BACKGROUND AND KNOW-HOW THEY WOULD NEED ON MRTD ISSUES, AINE NI FHLOINN AND InHOUSE TRAINING HAD AN AFFORDABLE, CUSTOMIZED SOLUTION AVAILABLE FASTER THAN YOU COULD SWIPE A CHIP PAST A READER.

In April 2005, ICAO met with representatives from InHouse Training (www.inhousetraining.ie) to discuss the options available for online training and examination tools that could be developed to assist States and authorities with their implementation needs for ePassport technology.

In the course of these preliminary discussions, several key factors were noted that made it apparent that the online approach would be uniquely suited to the training needs surrounding ePassport learning requirements:

1. As e-learning only requires web facilities such as browsers and network access, participants are free from agenda and travel management.

2. Shared training provides for the enhanced communication essential for cross border communication, helping to both resolve interoperability challenges and increase the amount of feedback reverting to ICAO. This feedback is essential to the Organization's ongoing activities relating to the maintenance and development of standards.

3. For officials involved in implementation, eLearning (online standardised training) provides co-ordinated programs across diverse geographical areas, lower costs, ensured quality levels and improved vendor selection and relationships. Online testing capabilities offer further assurances relating to skill level attainment.

4. Vendors and implementers benefit from shared understanding because it leads to more effective and innovative products/services.

It became clear from these early discussions that ICAO needed to offer exceptionally affordable training that would support the Organization's inclusive international culture. In response to this need, but still cognizant of the fact that even online programs require development investment and hosting costs, Aine Ni Fhloinn, Director of www.inhousetraining.ie, suggested a novel solution.

"In an ideal world, learning would never be blocked by lack of funding," began Ms. Ni Fhloinn. "Though we may not live in an ideal world, online approaches often allow us to rethink traditional training and business models. Our approach was simply to de-couple certification (the result of a successful exam) and the quality learning experience that ICAO was seeking to provide. By providing the training free of charge, countries facing budget pressures could still participate equally—regardless of internal budgets."

By virtue of this approach, countries, vendors and individuals with more accommodating training budgets still retain the opportunity to become certified, but the need for certification doesn't create an obstacle to parties seeking merely to develop their

skills. On the merits of this approach and their excellent track record in providing quality e-learning courses, InHouse Training was awarded the exclusive right to use ICAO's logo in identifying and marketing their MRTD course.

The courses themselves were developed using 3D animation software and Adobe Flash technology. In effect, every animation sequence (each step in a unit) is a miniature movie. The course interface and all the artwork are original and designed to enhance the e-learning experience.

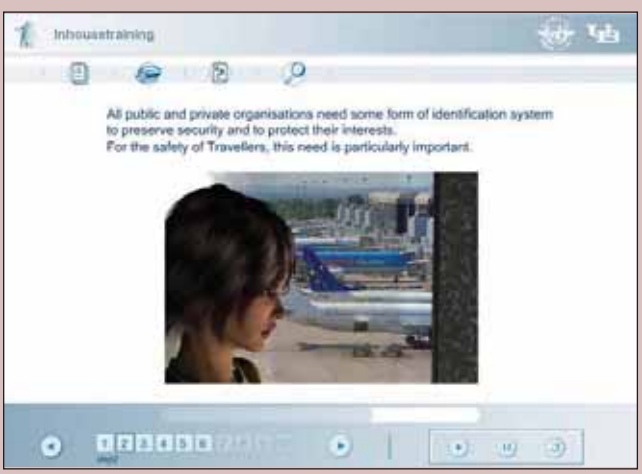
The animations used fall into two categories: 'photorealistic' for a primary story telling sequence (with characters); and 'silhouettes' for faster illustration purposes (bullet points). "This animation style strongly aids the learning process, including memory recall," commented Ms. Ni Fhloinn. "At the same time it makes for an attractive and very user-friendly course."

The exams themselves are open book and self-managed. The State University of New York University at Buffalo (UB) administers quality assurance and provide requested certifications for course exams. UB is one of America's oldest medical universities and has a history of research into identification technologies. It was the first university in the world to dedicate a research centre to the area of biometrics. Open book exams are suited to a working environment where continuous learning plays a role in everyday operations. As identification technology evolves, the learning habit (including accessing learning resources) is as important as the content to be learned. Self-managed exams support learning habits as well as a positive certification experience.

"The objective of our certification process is not to pass or fail individuals, it is to provide concrete, measureable results," continued Ms. Ni Fhloinn. "We believe Certification will be most useful for decision makers who need to benchmark companies and individuals offering MRTD-related products and services."

A free quick quiz that exactly replicates the format of a formal exam is available for all of the online training courses. The courses and exams are currently only available in English, but based on demand they will later be translated for the convenience of the broader ICAO community.

InHouse Training is looking forward to feedback and suggestions from all those taking courses and exams. Ms. Ni Fhloinn will be in Montreal this October and welcomes any interested parties to contact her while she's there (email: info@inhousetraining.ie). ■



The courses themselves were developed using 3D animation software and Adobe Flash technology. In effect, every animation sequence (each step in a unit) is a miniature movie. The course interface and all the artwork are original and designed to enhance the e-learning experience.

A free quick quiz that exactly replicates the format of a formal exam, is available for all of the online training courses. The courses and exams are currently only available in English, but based on demand they will later be translated for the convenience of the broader ICAO community.

How to Obtain CSCA Certificates:

The CSCA Overview List

By Sjef Broekhaar and Jan Verschuren, Ministry of the Interior and Kingdom Relations, The Netherlands

WITH THE INTRODUCTION OF E-MRTDS, A NEW PHENOMENON HAS BEEN INTRODUCED—THE DISTRIBUTION OF PUBLIC KEYS TO VERIFY THE INTEGRITY AND AUTHENTICITY OF THE INFORMATION STORED ON THE ELECTRONIC MEDIUM (CHIP). ACCORDING TO ICAO SPECIFICATIONS THERE ARE TWO LEVELS: THE COUNTRY KEY, INCORPORATED IN THE CSCA CERTIFICATE, AND; THE DOCUMENT SIGNER KEY (CONTAINED IN THE DS CERTIFICATE). FURTHERMORE, A CERTIFICATE REVOCATION LIST (CRL) IS ESSENTIAL IN THE VERIFICATION PROCESS.

ICAO currently requires that the CSCA Certificate be distributed by bilateral means, preferably via diplomatic channels. No other specific mechanism for bilateral exchange other than 'diplomatic exchange' is defined in the technical report.

Some countries have experience with this manner of distribution but face difficulties in order to find the right contact person in a ministry or organization. The NTWG was looking for a new solution for distribution of the CSCA Certificates and what follows is suggested approach. In the new solution the International Forum for Travel Documents (*IF4TD, see ICAO MRTD Report, Volume 1, Number 2*) will play a key role in indicating where and how the CSCA Certificates can be obtained. Since approximately 90 per cent of the countries issuing an e-MRTD are members of the IF4TD, this would be a logical step.

How does it work? In the members profile of a country or organization an extra field is integrated entitled: "CSCA Certificate." In this field the issuing body can add the following information: "How to obtain the CSCA Certificate," "Website," "Contact Person," "General e-mail address," "CSCA Version," "CSCA Verification Value Created by means of" and, if necessary, "Additional information."

The completed field in the members profile has to be sent to the Regional Representative of the IF4TD. This contact person will insert the information into a draft version on the IF4TD web site. When the information is entered the providing body is asked to check the details and, if they confirm the accuracy of the content, the information is published on the public site and made accessible to all members of the IF4TD.

As an additional measure, a hard-copy CSCA Overview List (COL) is created. The COL consists of the same fields as published on the IF4TD web site, as well as an extra check possibility, namely the fax number. The COL will be sent to ICAO Headquarters for publication on their web site: www.icao.int/mrtd.

The COL provides control authorities an overview with locations and contact points for requesting CSCA Certificates. The trust in the obtained CSCA Certificates can be improved if there are several different ways of checking their authenticity, therefore it is important to check first the authenticity of the downloaded COL from the ICAO web site. This can be done by checking the COL against the published one at the IF4TD web site or to request a copy of the COL by sending an e-mail to sjef.broekhaar@bprbzk.nl.

Secondly it is advised to use more than one contact point on the COL to request and verify the specific CSCA Certificate before using the Certificate in an Inspection System.

Countries or international organizations who are already issuing e-MRTDs and want to publish their CSCA Certificates can contact one of the authors: Sjef Broekhaar or Jan Verschuren, Ministry of the Interior and Kingdom Relations, The Netherlands (Sjef Broekhaar e-mail is noted just above). ■

CSCA CERTIFICATES OVERVIEW LIST–CONTINUED ON PAGE 34

Contact Points and Locations–Version 3, September 2007

Country	How to the Obtain CSCA	Contact Person	General E-mail Address	Fax Number	Website or LDAP Address	CSCA Version & Validity	CSCA Verification Value	Created By
Belgium	Request via e-mail to: luc.corbeels@diplobel.fed.be	Mr. Luc Corbeels	Josephus.hendrikx@diplobel.fed.be	+32.2.501.8701	N/A	Year: 2004 Version: 01	27 b5 ce 14 7b 1e 3b 9d 11 ff e1 7e 99 d9 99 82 c8 69 b8 58	SHA-1
Thailand								
Sweden								
Norway	Request via e-mail	Mrs. Ellen Thorvaldsen	pass.cert@politiet.no	+47.61.318.001	N/A	Year: 2005 Version: XX	2f b8 03 37 e2 59 54 85 70 49 42 05 e7 64 7f 2b dc bc c6 09	SHA-1
Australia								
Germany	Via website or e-mail	Mr. Dennis Kügler	csca-germany@bsi.bund.de	+49.22.8958.2722	www.bsi.de/csca www.bsi.de/csca	2005, serial: 00df; relative distinguished name = "SN=001" 2005, serial: 00df; relative distinguished name = "SN=002"	6e 7e be 85 98 e7 8f a1 b0 61 a6 12 74 a8 4f 9e d2 2e df c7 61 f0 c0 95 23 27 5f 9d 92 f9 83 bf 4d ef f5 34 35 6b 32 06	SHA-1 (of Public Key) SHA-1 (of Public Key)
New Zealand								
United Kingdom								
Japan	Via Diplomatic Channel in each country (primary method) or via general e-mail.	Ms. Noriko Nishimura	pki.passport@mofa. jp	+81.3.5501.8166	N/A	N/A	N/A N/A	
France								
Singapore								
Iceland								
Austria	Via website	Mr.Robert Gottwald	csca@bmi.gv.at	+43.1.90600.39709	www.bmi.gv.at/csca	2006 V3 Serial Number: 01 Valid from: 09-06-2006 till 12-09-2021	46 7b 29 82 26 4c 05 b1 16 37 2b b2 2e aa 7a 5b 32 db 8f fa 9c 70 5a db 85 71 c3 ac 06 b8 12 6c	SHA-256

CSCA CERTIFICATES OVERVIEW LIST–CONTINUED FROM PAGE 33

Contact Points and Locations–Version 3, September 2007

Country	How to the Obtain CSCA	Contact Person	General E-mail Address	Fax Number	Website or LDAP Address	CSCA Version & Validity	CSCA Verification Value	Created By
Portugal								
United States	Via Contact Person	Mr. Michael Holly	Ca-cst-pki-ops@state.gov	+1.202.663.2654	N/A	Year 2004 Serial Number (41 9e 65 23)	f0 2a 8c 1b 77 d3 42 a4 34 8b 7d 64 6c 88 f8 2f ba c2 40 15	SHA-1
Portugal								
Spain	Via LDAP site	Mr. Juan Crespo	oficinatecnica@dnielectronico.es	+34.91.890.2018	Ldap://ldap.dnie.es:389	2006 valid 20-07-2006 20-10-2021	ac 37 f5 8a 69 36 el ca b5 30 0b 08 eb 61 53 ba 7f 53 37 47	SHA-1
Finland	Via website	Mr. Tommi Rakshit	ePassport.Finland@intermin.fi	+358.9.1604 2223	http://www.fineid.fi/cp-csca/	2006 valid 12-06-2006 11-09-2016	e5 2f 6f 2d 9d 43 2f 88 1b 73 0e 71 02 ac f4 02 82 7b 92 c0	SHA-1
Netherlands	Via website	Mr. Jan Verschuren	agentschap@bprbzk.nl	+31.70.356.0066	https://www.bprbzk nl/echtheidsken-merken/csca	2006 valid 21-08-2006 30-08-2014	f2 8a 97 71 f4 fd bf 6d 65 ef fd 11 8b 5a e5 ce 26 68 87 f5	SHA-1
Greece	Via website	Mr. Georgios Dedemadis	csca@passport.gov. gr	+30.210.7296229	http://www.passport.gov.gr	2006 version 1 from 24-08-2006 24-11-2016	ec bc ad e3 9b 16 33 89 12 2e 04 66 78 89 e1 56 69 9c cb df	SHA-1
Lithuania								
Lithuania								
Luxembourg								
Slovenia	Via e-mail, In the near future via the website	Mr. Ales Pelan	csca-slovenia@gov.si	+386.01.4788.649	http://www.csca-si.gov.si/eindex.htm	June 08, 2006	3a 88 a2 88 91 dc b5 7e de 41 de f5 c4 e1 85 29 fe b9 dd 01 47 3b c8 5f 10 3e 27 78 b7 74 ff 52	SHA-256 With RSA Encryption (1.2.840.113549.1.1.11)
Poland	Via Diplomatic Channel in each country	Mr. Rafal Czarnecki	sekretariat.drr@mswia.gov.pl	+48.22.602.8215	N/A	2005, V3	19 35 7f 69 17 11 37 64 9b 67 c4 a0 d4 d4 3b 4f ec 19 c4 2a	SHA-1

Country	How to the Obtain CSCA	Contact Person	General E-mail Address	Fax Number	Website or LDAP Address	CSCA Version & Validity	CSCA Verification Value	Created By
Hungary								
Czech Republic	Via website	Mr. Libor Pokorny	pokorny@mvcr.cz	+420.974.816.823	http://www.mvcr.cz/kontakty/csca.html	24/07/2006 Version: V3. Serial Number SN=1	a8 96 7d c0 4a f6 92 c0 10 9a 5e d5 31 1e 56 b8 ca db c8 da	SHA-1
Switzerland	Via website or e-mail or LDAP	Mr. Roman Vanek	schweizerpass@fedpol.admin.ch	+41.31.324.14.10	http://www.bit.admin.ch/adminpki/00247/index.html?lang=de or admindir.admin.ch (port389)	2006, Version: 01	a2 b6 d6 63 b2 33 61 91 4d 30 b0 20 0b 88 68 16 76 1b dc 11	SHA-1
Andorra								
San Marino								
Ireland								
Liechtenstein								
Italy								
Hong Kong SAR								
Estonia	Via Diplomatic Channel in each country for now.	Mr. Helar Laasik	kma@mig.ee	+372.666.2721	N/A	Year: 2007	2f 86 7b e3 4a 1f f3 b6 5a 89 16 8c 4c b1 71 a2 c7 b7 5a 01	SHA-1

Country = EU Member State

Maldives Make Move to ePassport

FIRST SOUTH ASIAN COUNTRY TO IMPLEMENT ICAO-COMPLIANT BIOMETRIC TRAVEL DOCUMENTS

Seeking to reinforce its existing visa-exemption agreement with the UK and to enhance the security of its travel documents, the Maldives have become the first South Asian nation to make the move to the ePassport.

The move comes on the heels of recent US visa-waiver requirements concerning ePassports and the expectation that the UK with whom the Maldives currently enjoys visa-exemption. Making their document state-of-the-art with respect to general security and fraud-protection measures were also important considerations.

The Maldives made the decision last October to move to ePassport technology, setting themselves a very tight deadline to have the program up and running by their Independence Day on 26 July 2007. Despite the mere 10 months of lead time, Maldivian officials, together with their contractors, easily met their target.

"Fortunately we were able to implement the program on time and on budget," commented Aiman Ibrahim, Head of the Maldivian Travel Document Section. "To help offset some of the production costs—due to the low volumes we require—we bought chips and passports from our partner (Oesterreichische Staatsdruckerei (OeSD) and thus enjoyed the benefit of their economies of scale."

OeSD re-designed the passport layout, leading to a harmonic visual combination of Maldivian art and tradition combined with a variety of overt and covert security features. The new ePassport did not only impress the president at the inauguration ceremony, but also all the citizens that have applied for the new travel document so far.

Apart from the OeSD for the document itself, other suppliers for the Maldivian solution included Iris Corporation for the chip inlays and chip personalization, as well as NXP (former Philips) for the chip. The chip itself features a 72kB storage capacity, which fulfills the requirements for storing both a facial image and two index fingerprints as biometric identifiers, as well as full security mechanisms.

The passport data is protected by Passive Authentication, Basic Access Control and Active Authentication—thus surpassing current ICAO requirements. The ePassports are securely personalized in one central location in the capital city of Male.

Maldivian officials expect to issue 20,000 of their new ePassports per year for the next three-to-five years. ■

DATACARD GROUP

SECURITY, EXPERTISE AND EXPERIENCE

SECURE IDENTIFICATION SOLUTIONS FOR A CHANGING WORLD

To issue secure travel documents and ID cards, you need a solutions provider that understands government identification. You need a provider with expertise in every phase of data capture, entitlement and production. And you need a provider with a complete portfolio of software, systems, supplies and services.

That solutions provider is Datacard Group. We have more than 35 years of experience with secure ID programs, and we have deployed solutions in more than 75 countries. In other words, Datacard Group knows what it takes to issue secure documents.

We provide many governments with innovative ICAO compliant passport and national identity card issuing systems, secure biometric data enrolment and other custom solutions, such as e-passport kiosks to enable citizens to read their own electronic identity documents. We understand what it takes to meet security requirements, and keep people and property safe.

Governments around the world trust Datacard Group to provide highly secure identification solutions through innovative technologies, products and services. Talk to us to today to find out how we can help you protect your program, your documents and your investment.

DatacardGroup

SECURE ID AND CARD PERSONALIZATION SOLUTIONS

PHONE (US): +1 952 933 1223
PHONE (UK): +44 (0) 1489 555 632
E-MAIL: INFO@DATACARD.COM
WEB: WWW.DATACARD.COM

Facing the Future

THE ADVENT OF THE ePASSPORT HERALDS A GLOBAL REVOLUTION IN TRAVEL IDENTIFICATION, PERMITTING AIRLINES AND BORDER OFFICIALS AT AIRPORTS TO MORE PRECISELY MATCH DOCUMENTS TO PEOPLE, AUTHENTICATE DATA AND GENERALLY TO PROCESS TRAVELLERS AT AIRPORT CHECKPOINTS AND GATES MORE ACCURATELY AND EFFICIENTLY. THE ePASSPORT ALSO OFFERS SUBSTANTIAL BENEFITS TO THE RIGHTFUL HOLDER BY PROVIDING A MORE SOPHISTICATED MEANS TO CONFIRM THAT THE DOCUMENT IS AUTHENTIC WITHOUT JEOPARDIZING PRIVACY. THE *ICAO MRTD REPORT* REVIEWS ICAO'S ROLE IN DEVELOPING AND IMPLEMENTING THIS IMPORTANT NEW INITIATIVE.

The need to verify identities to protect the travelling public, as well as to provide countries with higher degrees of certainty regarding individuals entering their borders, has accelerated the adoption of biometric technology in recent years.

In September 2006, ICAO published the two-volume, sixth edition, of Doc 9303, Part 1_*Machine Readable Passports* (MRPs). Developed by ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), the first volume is comprised of the specifications for the non-biometric MRP, while the second volume contains the specifications for the biometrically-enhanced MRP, or 'ePassport.'

The ICAO ePassport standard specifies that facial recognition technology will be the primary biometric standard worldwide for travel documents, and that the compressed image of the face will be stored, along with the data from the machine readable zone of the passport, in a contactless integrated circuit (IC) chip embedded into the passport itself.

According to a private study conducted in spring 2006, nearly 70 per cent of consumers worldwide support using biometric technologies administered by a trusted organization (e.g., a bank, government, airline or border control authority) as a way to verify an individual's identity. The study also found that 66 per cent of consumers worldwide favoured biometrics as the ideal method to combat fraud and identity theft as compared to other methods such as smart cards and tokens.

This use of facial recognition technology to enhance ePassport security and privacy is therefore reassuring to the travelling public in general while providing airline, airport and border control officials with the enhanced identification confirmation tools they were looking for in the aftermath of 9/11. As of March 2007, 34 ICAO Contracting States had begun issuing ePassports to their citizens.

ePassport data will have to be programmed according to a Logical Data Structure as specified by ICAO. To assure the reader of the chip that the data therein, including the facial image, is valid, the ePassport data will be digitally signed and a specially-tailored public key infrastructure (PKI) project has been specified in order to protect the signed data from counterfeiting or unauthorized alteration. This system ensures that any overwriting chip data cannot go undetected.

The public keys (i.e., strings of characters used to encrypt or decrypt information) will be distributed through a central public

key directory (PKD) that has been set up by ICAO. The Member States of the TAG-MRTD had recommended that ICAO be the designated organization to oversee the PKD because of its long track record as the developer of MRTD standards, its international stature as a United Nations agency and its substantial interest in document security. The oversight of a central, politically-neutral site overseen by ICAO was seen as essential to a cooperative, interoperable regime for passport security that would be accessible by all Member States.

Equally important is that a central PKD would be publicly accessible to any entity required to verify ePassports, such as airlines, who are on the front lines where the examination of travel documents is concerned. As a deterrent to the fraudulent alteration or counterfeiting of passports, or the use of stolen passports by impostors to gain access to aircraft, PKI represents a potentially very effective anti-terrorism and aviation security measure.

The ICAO Council confirmed the development of a PKD, on a cost-recovery basis, under the aegis of ICAO. The development, implementation and operation of this project involve three major stakeholders: the PKD operator, ICAO and the participants (i.e., an ePassport-issuing State or entity that follows the arrangements for participation in the PKD).

In 2006, the overall design and development of the PKD was approved, various levels of testing were completed and approved, and review and acceptance of the planned PKD facility was finalized. In February 2007, a Memorandum of Understanding (MoU) which set out the arrangements for participation in the PKD, and for its establishment and operation, was approved by the Council. In March 2007, with the receipt of the fifth Notice of Participation in the PKD, the MoU became effective. The PKD Board, the governing body responsible for the oversight and supervision of the PKD, was formally convened in March 2007, and the secure PKD Office was opened at ICAO Headquarters.

Implementation

ICAO has set up a special project to assist those States which have not yet begun issuing machine readable passports with the objective of universal implementation ahead of the mandatory April 2010 deadline as prescribed in Annex 9. ICAO provides assistance in the form of project planning, education and training, arrangements for financing, procurement assistance, as well as start-up project management and/or system evaluation services upon requests from Member States.

As part of this project, two self-financed, worldwide MRTD/Biometrics Symposia were held at ICAO Headquarters in 2005 and 2006. A third Symposium, with an aviation security emphasis, is planned for October 2007, also at ICAO Headquarters.

In June 2006, a biometrics and machine readable passport implementation workshop for the Asia-Pacific Region was held in the Hong Kong Special Administrative Region (SAR) of China, and a Latin American regional symposium on AVSEC-FAL (including MRTDs) was held in the Dominican Republic. Also, in July 2007, a regional conference for European and African Mediterranean States was held in Vienna on document security and ICAO MRTD standards. This conference was held in conjunction with the Organization for Security and Co-operation in Europe (OSCE).

Regional symposia for the Latin American and the African/Middle East regions are planned for 2008–2009 In 2005, individual UIMRTD assistance projects were implemented in Bhutan, Brazil and Colombia, and in 2006 assistance was provided to 12 States. For the 2008-2010 triennium, ten individual UIMRTD missions to States are planned for each year.

Finally, the 36th Assembly, shortly after the time of this writing, will have voted on several amendments to Appendix D of Assembly Resolution 43/1, Facilitation, regarding international cooperation in protecting the security and integrity of passports. These amendments include the recognition that Member States of the United Nations have resolved, under the Global Counter-Terrorism Strategy, adopted on 8 September 2006, to step up efforts and cooperation at every level, as appropriate, to improve the security on manufacturing and issuing identity and travel documents and to prevent and detect their alteration of fraudulent use; an urging by the Assembly to Member States to issue machine readable passports in accordance with the specifications of Doc 9303, Part 1, and; a request that the Council to continue the work on enhancing passport fraud, implementing the related SARPs of Annex 9 and developing guidance material to assist Contracting States in maintaining the integrity and security of their passports and other travel documents. ■

ICAO NEW TECHNOLOGIES WORKING GROUP REQUEST FOR INFORMATION 2007/8

BACKGROUND

The International Civil Aviation Organization (ICAO) Technical Advisory Group on Machine-Readable Travel Documents (TAG MRTD) is responsible for the development of specifications for travel documents with the goal of global interoperability. In addition, the TAG MRTD seeks to advise ICAO on technology issues related to the issuance and use of machine-readable travel documents.

The TAG MRTD, through its New Technologies Working Group (NTWG), issues an RFI every three years in order to keep abreast of new and improving technologies. Relevant information gathered during the RFI process is summarised and shared among the 190 ICAO Contracting States. ICAO also considers this information when international standards are developed.

AREAS OF INTEREST

Information regarding technologies that may be used in machine-readable passports, visas and card-based travel documents is sought for consideration. The technologies sought are to assist in the folowing areas:

- assessment of applicant eligibility;
- document security and production;
- linking documents to holders/bearers;
- providing reliable authentification of genuine documents;
- facilitate secure and reliable transit of travellers through airports, seaports and other international border control points.

Interested parties are invited to provide technical, application environment and pricing information for technologies in the following cathegories:

Category	Requirement
Multi-application data chip environment	Effective methodology for creating a secure multi-application environment within the data chip, where the e-passport application co-exists securely with other applications (e.g., e-government applications). Secure writing and retrieving without compromising the security of the original data is paramount.
Self-service facilitation	Technologies and processes suitable for automated self-identification at international borders and/or entitlement facilities that will enable either unattended border crossing or program enrolment.
Data mining technologies	Pattern recognition for applicant and staff behaviours to assist in the identification of external and internal fraud.
Travel document security concepts	Document security features, innovative data page materials, substrates, binding materials and adhesives, advanced anti-copying devices (e.g., holographic/crystagraphic features or security inks), and security technologies that allow for globally interoperable, machine assisted document authentication and verification.
E-government and e-commerce	Electronic online systems that may be applied to secure Internet based passport and visa application processes. Secure communications for multilateral data-sharing.
Biometric database management	Integrated ID management tool that enables concurrent, multi-factor biometric searching and matching for profiling and alert management.
Biometric verification on the move	Biometric matching in a non-intrusive way with a high tolerance for distance and angles.
Portable enrolment and verification stations	Portable multi-modal enrolment enabling the capture and verification of multiple biometrics (particularly fingerprints).
Transliteration software	Language software technologies to assist in transliterating non-Latin characters (e.g., Cyrillic or Arabic) into Latin characters.

CONSIDERATIONS

Interested parties must present their technologies in the context of ICAO Document 9303, which prescribes international format and on-board data storage standards for machine-readable passports, visas, and other official machine-readable travel documents. Interested parties must also be able to substantiate any claims related to performance of the technology proposed. Proposals will be reviewed against a variety of qualitative and quantitative factors, depending on the category. Generally, this will include such aspects as cost, innovation, and compatibility with current and future document issuance and border control processes. Dependant technologies, reliability, accuracy and speed are also factors that may be considered by the selection panel. Interested parties should also recognise that in the application of these technologies, the NTWG panel will give particular consideration to the ICAO goals of facilitation, security, and global interoperability.

SUBMISSIONS

Written responses to this RFI must be provided by 26th October 2007 to:

David Philp
RFI Coordinator
ICAO New Technologies Working Group
c/o New Zealand Passport Office Department of Internal Affairs
PO Box 10-526 Wellington
New Zealand

Interested parties are advised that ICAO is under no obligation to designate any standard or take any further action with any party as a result of this Request for Information. Summary sheets supplied in response to this RFI will be made available to Contracting States. Accompanying information and descriptive literature may also be made available to Contracting States. With the exception of the summary sheets, any other information that is considered non-disclosable to all ICAO Contracting States should be identified as such. Non-disclosable information will be retained exclusively for the use of the government members of the ICAO New Technology Working Group.

Requests for copies of ICAO standards documents (ICAO Document 9303, Parts 1 to 3) should be directed to:

ICAO DOCUMENT SALES UNIT
999 University Street, Montréal, Quebec, Canada, H3C 5H7
Tel: +1 (514) 954-8022
Fax: +1 (514) 954-6769
E-mail: sales_unit@icao.int
Online access to publications: www.icao.int/eshop/
Online ordering: http://icaodsu.openface.ca/mainpage.ch2

This Request for Information is placed by the New Zealand Passport Office, Department of Internal Affairs in furtherance of its participation in the TAG/MRTD also being a contracting State of ICAO, a United Nations specialised agency. The New ZealandGovernment and its employees accept no responsibility for the actions or undertakings of ICAO, ICAO participants, or ICAO staff.

Do You Know Who's Traveling?

Protecting and securing identities is critical to border, transportation and national security. Identity management is our business.

Automated ePassport Authentication

iA-thenticate® Smartchip

A full page document authentication scanner with RFID contactless chip reader for ePassports and government issued identification cards. It includes Basic Access Control (BAC) and 1 pass read with automatic authentication.

L-1 IDENTITY SOLUTIONS

At L-1 Identity Solutions (NYSE: ID), we offer a complete set of products, solutions and services to solve the toughest challenges in managing human identities. We provide the most advanced multi-biometric solutions for finger, face and iris, as well as document authentication devices and secure credential production.

Learn more about our products and services at www.L1id.com

296 Concord Road, 3rd Floor
Billerica, MA 01821 USA
Telephone +1 978-932-2200
Facsimile +1 978-932-2225

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.

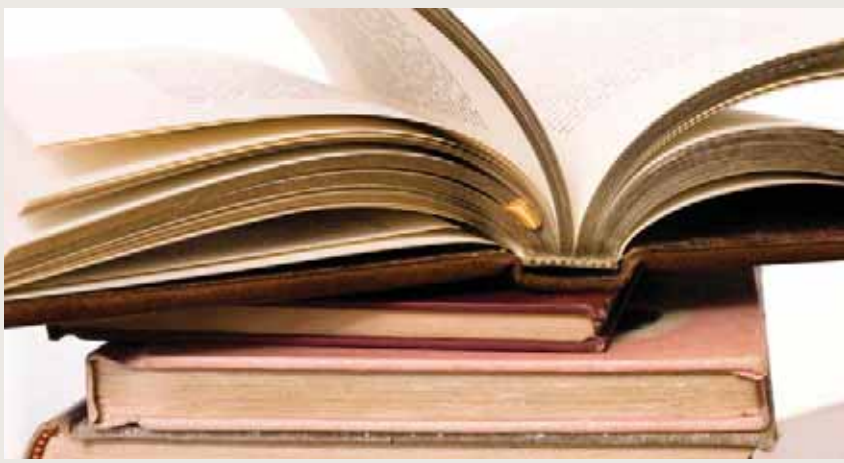
Chemical sensitizers Security reagents to guard against attempts at tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.

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, Vo lume 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 reoriginated 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 his3 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 traveller (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.

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

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

Multiple biometric The use of more than one biometric.

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

One-to-many Synonym for "Identification".

One-to-one Synonym for "Verification".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 centres of the eyes is parallel to the top edge of the portrait rectangle if this has not been achieved when the original portrait was taken or captured *(see Section 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.

DeLaRue

a trusted **partner**

secure **government identification** solutions from De La Rue

De La Rue Identity Systems is the world's leading supplier of secure government identification solutions. We work alongside global organisations such as ICAO and Interpol to help define and uphold international standards. Knowing that De La Rue has implemented over 50 successful identity programmes across every continent allows governments to have absolute confidence in what we do.

Our expertise ensures De La Rue's identity documents and systems, including biometrics, work seamlessly together to create a secure, integrated solution. Only this approach assures full protection against counterfeit and fraud. De La Rue's solutions offer governments the technology to provide complete security and integrity for 21st century identity management.

DE LA RUE
IDENTITY SYSTEMS

passport **ePassport** visa **national ID card** driving licence **voter registration**

Tel: +44 (0)1256 605000 Email: Identity.Systems@uk.delarue.com **www.delarue.com**

The world turns to 3M for identification solutions

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

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

3M