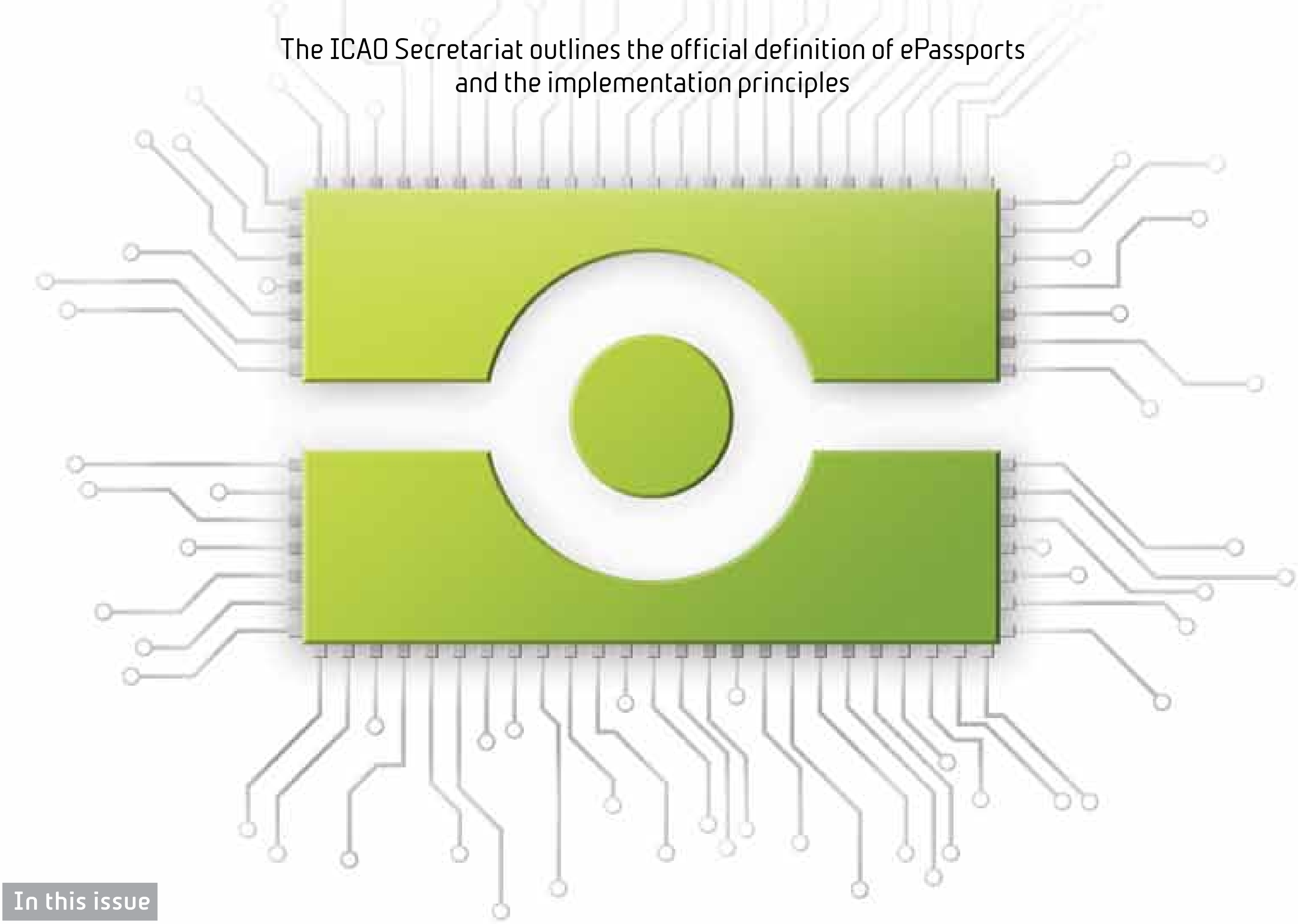
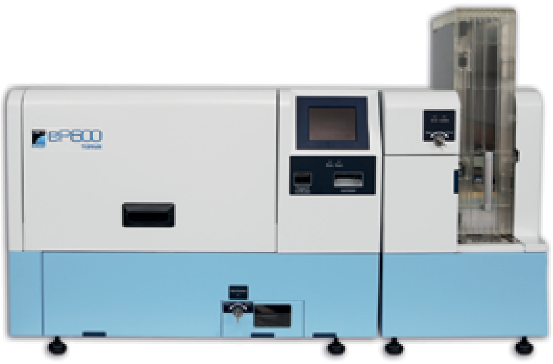
ICAO
INTERNATIONAL CIVIL AVIATION ORGANIZATION
Vol. 7, No. 3 – Fall 2012
MRTD REPORT

THE IMPLEMENTATION OF ePASSPORTS

The ICAO Secretariat outlines the official definition of ePassports and the implementation principles



In this issue


eP600

ICAO MRTD REPORT
VOLUME 7, NUMBER 3, 2012

Editorial
MRTD Programme—Aviation Security
and Facilitation Policy Section
Editor-in-Chief: Mauricio Siciliano
Tel: +1 (514) 954-8219 ext. 7068
E-mail : msiciliano@icao.int
Coordinator: Erik Slavenas
Tel: +1 (514) 954-8219 ext. 8242
E-mail : eslavenas@icao.int
Coordinator: Nathalie Teatin
Tel: +1 (514) 954-8219 ext. 6056
E-mail : nteatin@icao.int

Content Development
KDH Communications
Assistant Editor: Kathlyn Horibe
Tel: +1 (514) 697-8654
E-mail: khoribe@videotron.ca

Production and Design
Bang Marketing
Stéphanie Kennan
Tel: +1 (514) 849-2264
E-mail: info@bang-marketing.com
Web Site: www.bang-marketing.com

Advertising
Keith Miller, Advertising Representative
Tel: +1 (514) 954 8219, ext. 6293
Fax: +1 (514) 954 6769
E-mail: kmiller@icao.int

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, Editor-in-Chief, at: msiciliano@icao.int.

Opinions expressed in signed articles or in advertisements appearing in the ICAO *MRTD Report* represent the author's or advertiser's opinion and do not necessarily reflect the views of ICAO. The mention of specific companies or products in articles or advertisements does not imply that they are endorsed or recommended by ICAO in preference to others of a similar nature which are not mentioned or advertised.

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 ICAO Member States and the international aeronautical and security communities.

Printed by ICAO

Contents

MRTD
Partnership
Community

ICAO-COMPLIANT ePASSPORTS: IMPROVING BORDER SECURITY AND ENSURING SAFER AIR TRAVEL

This issue covers a broad range of topics. It illustrates the diversity and complexity of the evolving MRTD agenda and the relevance of MRTDs and identity management to many walks of life.

Our main focus is on ePassports and the importance of ensuring they are compliant with established Standards. Current specifications for issuing ICAO-compliant electronic passports provide a solid foundation for developing the most secure and robust travel documents ever issued. Over 104 States are currently distributing ePassports with about 400 million in circulation—nearly a third of all passports globally. And these numbers are increasing at a tremendous rate. However, an ePassport is only as secure as the biometric and biographic information in its chip and useful only if the data is validated quickly and securely.

According to TAG/MRTD experts, not all ePassports in circulation today are fully compliant with ICAO specifications. This prohibits issuing States from capitalizing on full security and facilitation benefits that ePassports are meant to deliver. In this issue, the ICAO Secretariat outlines the official definition of ePassports and the implementation principles, including mechanisms, such as the ICAO Public Key Directory (PKD), for effectively sharing and providing the information needed for verification and authentication of these ICAO-compliant travel documents.

The ePassport and PKD themes are explored by other authors. Sharon Boeyen looks into the vital role of Public Key Infrastructure (PKI) in ensuring global confidence in electronic passports. Crucially, the benefits of PKI must be realized by *both* eMRTD issuing States and eMRTD receiving States. They all must implement the necessary systems and policies to facilitate electronic processes at both ends. Issuing States must implement reliable, secure and compliant systems, including the National Public Key Infrastructure for issuing and managing CSCA, Document Signer and personalization systems as well as high-quality processes and procedures. Receiving States must establish initial trust with issuing States through processes that can be supported with PKI technology.

The role of the PKD is further discussed in an interview with Eckart Brauer, former ICAO PKD Chair, who reflects on PKD developments during the last years, the challenges encountered and solutions found. The PKD remains the most efficient, secure and economic means for distributing PKD-related information and a cornerstone of the security and facilitation benefits ICAO-compliant ePassports provide at borders.

ePassport implementation is a complex task and it always helps to learn from the first-hand experiences of States. Carlos Gómez provides a comprehensive account on implementing new ePassports in Spain, reflecting on its benefits to Spanish citizens, outlining lessons learned and providing helpful recommendations to the MRTD professional community.

In addition, the progressive development of MRTD specifications is addressed in this issue. ICAO has been updating and streamlining the structure of Document 9303 and enhancing its contents with the inclusion of up-to-date Technical Reports and the Supplement. Current activities include incorporating TRs and the Supplement into Doc 9303 and re-structuring Doc 9303 for the new edition of this vital document. Tom Kinneging provides an insider's perspective on the rationale and scope of its restructuring and the progress of this important work. The new edition of Doc 9303 is expected to be ready for publication in the second half of 2013 or the first quarter of 2014.

www.icao.int

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

Member	Nominated by	Member	Nominated by
Mr. R. Tysoe	Australia	Mr. J. Verschuren	Netherlands
TBC	Canada	Ms. A. Offenberger	New Zealand
Ms. M. Cabello	Chile	TBC	Nigeria
Mr. M. Vacek	Czech Republic	Mr. Y. Xuefeng	People's Republic of China
Ms. M. Pujau-Bosq	France	Mr. C. Ferreira Gonçalves	Portugal
Dr. E. Brauer	Germany	Mr. O. Demidov	Russian Federation
Mr. A. Manickam	India	Mr. S. Tilling	Sweden
Mr. J. Nugent	Ireland	Mr. R. Vanek	Switzerland
Mr. H. Shimizu	Japan	Mrs. K. Mitchinson	United Kingdom
		Mr. M. Holly	United States

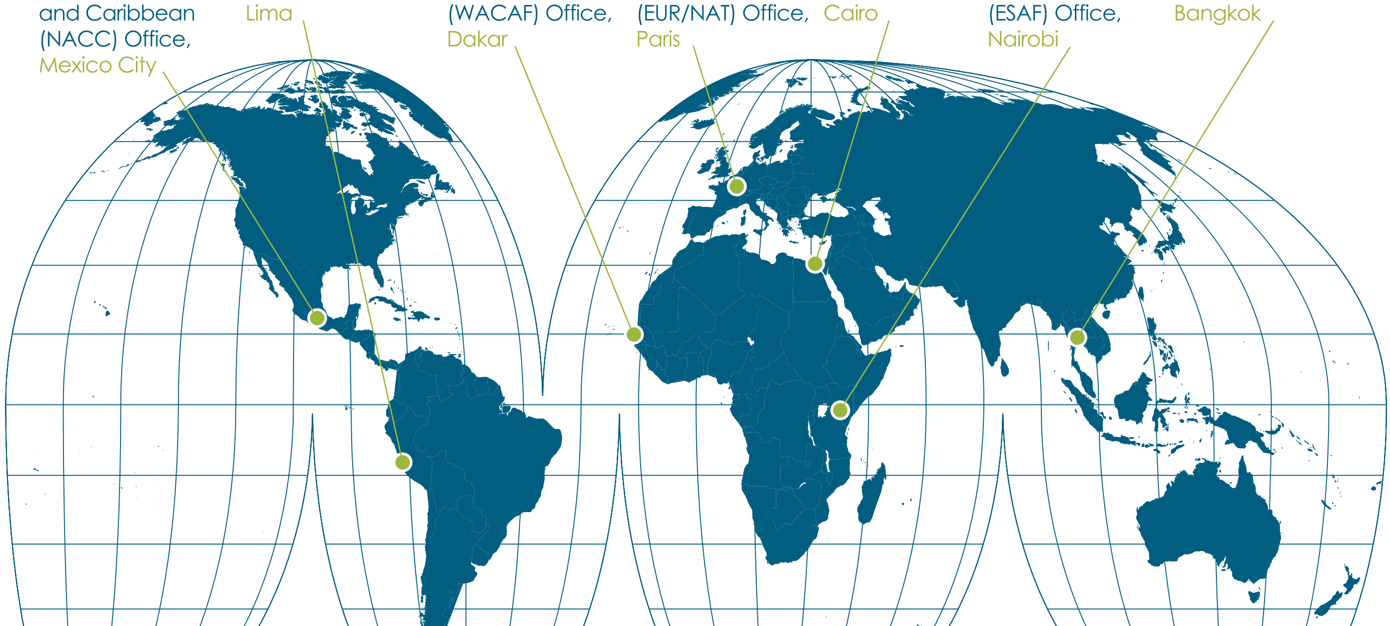
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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

Observer organizations

Airports Council International (ACI)
International Air Transport Association (IATA)
International Criminal Police Organization (INTERPOL)
International Labour Organization (ILO)
International Organization for Standardization (ISO)
Organization for Security and Cooperation in Europe (OSCE)
International Organization for Migration (IOM)
United Nations (UN)
Organization of American States (OAS) - Inter-American Committee on Terrorism (CICTE)

ICAO's Global Presence



North American Central American and Caribbean (NACC) Office, Mexico City

South American (SAM) Office, Lima

Western and Central African (WACAF) Office, Dakar

European and North Atlantic (EUR/NAT) Office, Paris

Middle East (MID) Office, Cairo

Eastern and Southern African (ESAF) Office, Nairobi

Asia and Pacific (APAC) Office, Bangkok

Secure MRTDs rely on robust identity management infrastructure where civil registries are the central actor. Mia Harbitz explores the role that civil registries play in providing security to the public. Going beyond national security requirements, she delves into the human aspect, the need to ensure civil rights and freedoms for citizens so they can maximize their economic and societal potential. The article also looks into the security-development nexus and ongoing efforts to assist the developing world with strengthening identity management capacity and promoting concrete civil registration practices.

MRTDs come in many different shapes and types. While everyone is familiar with ordinary, service and diplomatic passports, fewer people have heard of Convention Travel Documents (CTDs) for refugees and stateless persons. Nevertheless, CTDs are equally important and an obligation to signatory States, which should issue them according to ICAO specifications. Alexander Beck provides a comprehensive overview of the historical context, explores the special humanitarian needs of refugees and stateless persons and outlines key challenges in ensuring the ICAO compliance of CTDs. In particular, the article sheds light on the emerging Doc 9303-compliant technical specifications for CTDs that are being developed by UNHCR and the MRTD Implementation and Capacity Building Working Group (ICBWG).

This issue is distributed during the 8th MRTD Symposium that takes place in Montreal on 10-12 October 2012. This important annual event addresses ICAO MRTD Standards and specifi-cations, identity management best practices and related border security issues. In addition, this year's Symposium focuses on the humanitarian dimension, exploring global humanitarian assistance efforts where reliable identification and issuance of travel documents play an important role in post-disaster or post-conflict rehabilitation. A number of case studies are presented by relief organizations and international aid programmes, with reference to identity management and travel documents. This session also builds on the MRTD Programme's ongoing cooperation with UNHCR in addressing the needs of refugees and stateless persons. We look forward to seeing many of you at the Symposium, which provides an opportunity to explore current MRTD themes and the latest developments.

Finally, I would like to highlight the work done by Nathalie Teatin and Erik Slavenas in assisting me to put together the MRTD Report. Their suggestions, creativity and commitment to the MRTD Programme make an important difference. I would also like to thank Kathlyn Horibe, Assistant Editor, and Garleen Tomney, MRTD Programme Assistant. ■

ePASSPORT IMPLEMENTATION AND THE ICAO PKD

The current specifications for issuing ICAO-compliant electronic machine readable passports (ePassports) have provided a solid foundation for developing the most secure and robust travel documents ever issued by States. The main reason for designing and specifying the criteria for ePassports was to add robust new security features to current ICAO-compliant Machine Readable Passports (MRPs). However, an ePassport is only as secure as the biometric and biographic information contained in its chip and the information on it useful only if the data can be validated quickly and securely.

The ICAO Secretariat outlines its official definition of ePassports and the general principles for implementation, including the mechanisms for effectively sharing and providing the information required to verify and authenticate these travel documents, such as the ICAO Public Key Directory (PKD).

Based on a recent study conducted by the New Technologies Working Group (NTWG) of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), over 104 States are currently issuing ePassports with about 400 million ePassports in circulation—close to a third of all passports worldwide. And these numbers are increasing exponentially.

Many ICAO member States have invested time and money and created great expectations in subsequent implementation projects. Yet, according to some TAG/MRTD experts, not all ePassports are fully compliant with ICAO specifications. If this is the case, this prevents issuing States from capitalizing on their investments and improving border security and safer air travel globally. Non-compliant ePassports also thwart other States from reading, verifying and authenticating them, that is, taking full advantage of the information and functionality contained in ICAO-compliant ePassports.

ICAO ePASSPORTS DEFINITION

In Doc 9303, Part 1, Volume 1, Page II-3, ICAO defines ePassport as:

> 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.

The PKI technology prevents the information stored on the chip from being altered unnoticed.

Thus, any ePassport issued by a State or entity that does not comply with these specifications *shall not* be called an ePassport and *shall not* display the ePassport logo on the front cover.

ePASSPORTS ISSUANCE

The issuance of ePassports is not currently mandatory by ICAO. It is mandatory only for ICAO member States to issue MRPs, according to specifications contained in ICAO Doc 9303, Part 1, Volume 1 (Annex 9 to the Chicago Convention, Standard 3.10).

However, if States decide to issue ePassports, then the principles contained in Recommended Practice (RP) 3.9 and in Annex 9, must be applied. This RP establishes that States should incorporate biometric data in their MRPs, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine readable zone.

The RP goes on to detail what is known as the ePassports 'blueprint', which is specified in full in Doc 9303, Part 1, Volume 2, and the Supplement to Doc 9303, as follows:

> Contracting States incorporating biometric data in their Machine Readable Passports are to store the data in a contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure (LDS) as specified by ICAO.

The required data stored on the integrated circuit chip must be the same as that printed on the data page, that is, the data contained in the machine readable zone, plus the digitized photographic image. Fingerprint image(s) and/or iris image(s) are optional biometrics for member States that want to supplement the facial image with another biometric.

IMPLEMENTATION OF ePASSPORT PROJECTS

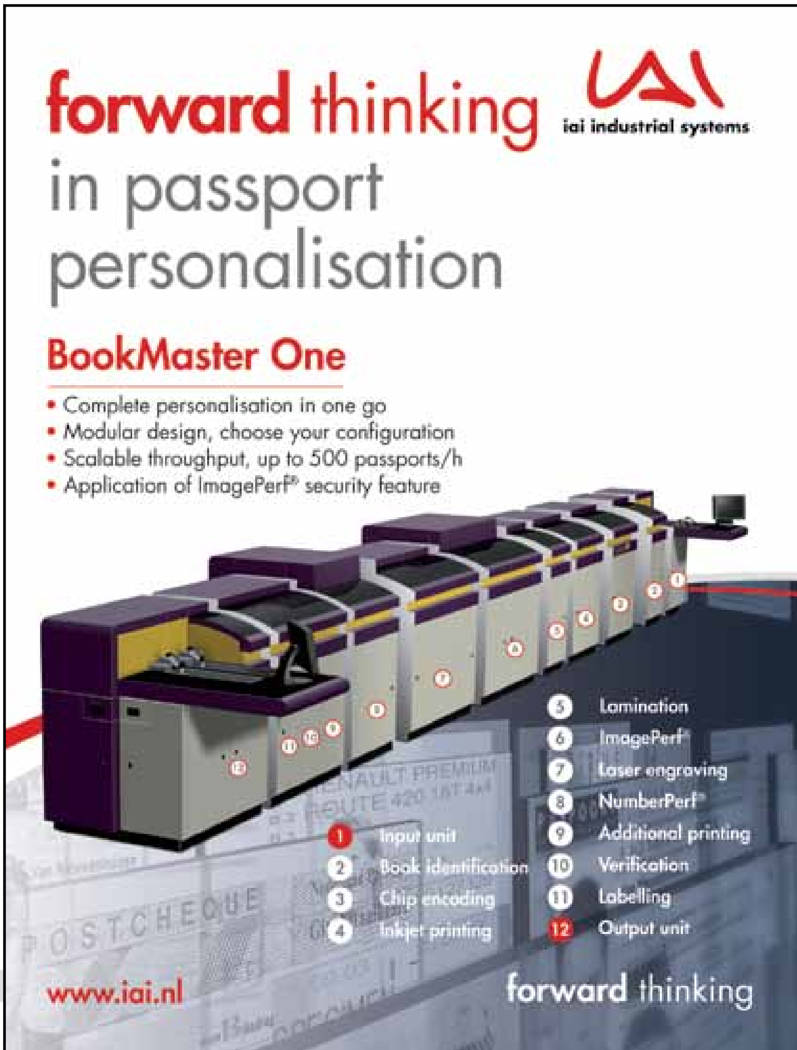
An ePassport, however, is only as secure as the biometric and biographic information contained in its chip. Information on the chip, in turn, is only useful if the data can be validated quickly and securely.

In addition to the ePassport holder's information, the chip also stores a country specific digital security feature, known as a 'digital signature', which is derived from the country's security certificates, the Document Signer Certificates and the Country Signing Certification Authorities (CSCA) Certificates. These digital signatures are unique to each country and can be verified using their public keys. When the ePassport is scanned, its digital signature informs border authorities the passport is authentic, was issued by the given country and has not been tampered with. The definition and specifications for each one of these elements are contained in Doc 9303, Part 1, Volume 2, and in the Supplement to Doc 9303.

However, when implementing ePassports, one of the biggest challenges States face is a timely, effective and secure way to distribute the certificates and Certificate Revocation Lists (CRLs). The volume of ePassports being issued by a growing number of States has challenged the practice of bilaterally exchanging this electronic information and has become increasingly error-prone, cumbersome and ineffective. Yet without full and timely access to these certificates, ePassports must be treated as non-electronic passports at the border, diminishing the pertinence and effectiveness of considerable public investments in ePassport systems and eroding trust in ePassports among border officials and citizens.

ICAO PUBLIC KEY DIRECTORY

In response, ICAO created a system to facilitate the sharing of public key information between countries: the ICAO PKD. The PKD is a repository that enables PKD Participants to input their security certificates and CRLs into the directory. It also offers public access to the validated security certificates of all PKD Participants that have completed their upload.



DEFINING THE ePASSPORT

First and foremost, an ePassport *must* incorporate all the basic specifications related to MRTDs contained in the sixth edition of ICAO Doc 9303 in the section, Machine Readable Travel Documents, Part 1, Volume 1. This volume contains all the specifications necessary for a State to develop and issue a Machine Readable Passport (MRP).

Secondly and more specifically, an ePassport must fully conform to Doc 9303, Part 1, Volume 2, and its Supplement, which includes the specifications a MRP *must* employ to conform to ICAO's globally interoperable requirements and qualify as a *true 'ePassport'*. These specifications include:

- High resolution digitized displayed portrait with the digital data of the image stored in the chip. The facial image is the only globally interoperable biometric.
- Data storage and communication via a contactless integrated chip (IC), conforming to ISO/IEC Standard 14443, Type A or B.
- Employment of the Doc 9303-mandated Logical Data Structure (LDS).
- Incorporation of a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology. It is recommended States join the ICAO Public Key Directory (PKD). The PKD is the main global distribution point for public key certificates from all e-Passport issuers.

These four characteristics comprise the basic definition of an ICAO-compliant ePassport. Where applicable and/or mandated, fingerprint and iris capture are also specified as secondary biometrics.

Doc 9303 and its Supplement are available free of charge from our web site: www.icao.int/Security/mrtd/Pages/default.aspx

Source: FAL Manual, ICAO Doc 9957

The PKD simplifies and modernizes the exchange of certificates and CRLs. It assures border control authorities the documents are genuine and unaltered and the biometric data is trustworthy.

This validation allows border control authorities to confirm the document held by the traveller

- Was issued by a bona fide authority.
- Has not subsequently been altered.
- Is not a copy or cloned document.

As a result, border controls' identity verification process of matching the document with the bearer takes place faster and is much more secure. In addition, if the document has been reported lost or cancelled, validation confirms whether the document is in the hands of the wrong person.

THE EFFICIENT AND SECURE PKD

The PKD provides an organized, uncomplicated and secure system for sharing this information. Without the PKD, a country must individually approach another country to securely exchange their security certificates. With PKD, certificate sharing, which involves hundreds of transactions and hours of labour, can be accomplished in just two exchanges—the upload and the download of validated information.

The PKD does not contain any passport holder's personal information nor does it provide access to ePassport secondary biometrics, like fingerprints.

Recommended Practice 3.9.1 of Annex 9 urges all member States issuing or intending to issue ePassports and/or implementing automated checks on ePassports at border controls to join the PKD.

NON ICAO-COMPLIANT ePASSPORTS

Unfortunately, as stated by several TAG/MRTD experts, it seems that some ePassports currently in circulation are not fully ICAO-compliant. The reasons for this may be numerous, such as a poorly printed machine readable zone, the wrong RFID chip, incorrect LDS programming, non-conformant PKI cryptographic technology.

Some of these issues can be solved if appropriately addressed. For example, some States have issued non ICAO-conformant PKI certificates for digitally signing ePassports. In some cases, they have been identified and documented as a known 'deviation' by the State. Yet other States require access to this information in a secure and prompt way. The answer to this is to use the ICAO PKD.

ePASSPORT DEVIATIONS

Not all PKD Participants implement the PKD contents specifications in exactly the same way, resulting, in some cases, in a non-conformance or 'deviation'. The electronic portion of the ePassport is then rendered invalid and handled as a MRP with the loss of certain privileges for the holder that can only have been obtained with an ICAO-complaint ePassport.

To overcome these issues and find a viable solution to handle 'acceptable deviations', the PKD Board, in cooperation with ICAO and ISO, implemented a set of PKD Upload Contents checks and error codes so that every border control authority or any other user is fully aware of the interoperability or security issues when downloading certificates or CRLs from the PKD.

The main reason to enforce these checks is to align all ePassport issuers with the Doc 9303 requirements. However, in order to validate all authorized travel documents—in some cases, already in circulation—entries not on the acceptable list are also published in the PKD. However, this 'provisional' solution does not give ePassport issuers a license to deviate from the Standards without consequences.

THE PKD BOARD SUPPORTS STATES' PARTICIPANTS

States are encouraged to join the PKD and benefit from the standard conformance reached and maintained for ePassports, and from the

PKD Board's expertise and vast experience in implementing ePassports projects, including overcoming non-compliance issues.

For more information on ePassports and PKI-related deviations, visit the MRTD Programme web site and review the PKD Documents available at www.icao.int/Security/mrtd/PKD%20Documents/Forms/AllItems.aspx. You can also contact Christiane DerMarkar, PKD Officer, (cdermarkar@icao.int), who will address your concerns to the appropriate person or institution.

CONCLUSION

Non-compliant ePassports may be treated as a Machine Readable Passport, preventing issuing States from capitalizing on their investments and improving border security and safer air travel globally. Non-compliant ePassports also thwart other States from reading, verifying and authenticating them, that is, taking full advantage of the information and functionality contained in ICAO-compliant ePassports. To capitalize on the important investments made to implement ePassports issuance projects and achieve the expectations created, ePassports issuing States must ensure that the booklets produced are fully ICAO-compliant.

Those States uncertain about such compliance should contact ICAO immediately, as several have already done so, to find ways of overcoming these problems.

In addition, States issuing or intending to issue ePassports and/or implementing automated checks on ePassports at border controls, should join the ICAO PKD. They would benefit from an organized, uncomplicated and secure system for sharing PKD-related information and from Board members' expertise on these matters.

ICAO ePASSPORT ASSISTANCE

If you are uncertain about other compliance issues, we urge you to seek out ICAO assistance. This assistance is available, if requested by the State, and can take different forms. In some cases, depending on the request, it can require the participation of the ICAO Technical Co-operation Bureau (TCB).

Some examples of assistance, among others, include:

- Interpretation of specifications.
- Organization of assessment missions on ePassport, ID management and civil registries processes and systems.
- Provision of quality assurance of ePassports booklets and systems.
- Development of tender documents and specifications.
- Procurement of equipment and systems on behalf of the State.
- Implementation of ePassport projects.

For more information on how to receive assistance from ICAO, please contact Mauricio Siciliano, MRTD Officer, at msiciliano@icao.int. ■

Leadership and Vision in Global Civil Aviation

www.icao.int

The International Civil Aviation Organization

SUNSET PROVISION FOR NON-MACHINE READABLE PASSPORTS

In order to accommodate those States issuing 10-year passports, Annex 9 also contains a sunset provision requiring all non-Machine Readable Passports to expire before 24 November 2015 (Standard 3.10.1). Because a large proportion of States are now issuing Machine Readable Passports (MRPs), it is likely holders of passports that are non-machine readable will find it increasingly difficult to travel internationally after 2015.

Furthermore, as non-MRPs are more susceptible to document fraud, these passports will come under closer scrutiny and their holders increasingly subject to secondary examinations—greatly delaying entry into a country.

An MRP holder is assured of quicker clearance at border control points because of passport readers and border control officers' increasing familiarity with MRPs. Also, more visa free travel is now available in some parts of the world for MRP holders. ■

Source: FAL Manual, ICAO Doc 9957

IMPLEMENTING ePASSPORT IN SPAIN: LESSONS LEARNED

CARLOS GÓMEZ

With more than eight years of experience in implementing programmes, such as the Spanish ePassport, electronic ID card, electronic Residence Permit, EU visa and driving license, Carlos Gómez is R&D and Innovation Manager of Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda (FNMT-RCM) (www.fnmt.es). He represents Spain at the European Commission Article 6 Committee and at the extinct BIG. With a wealth of experience in international identification projects, he is a consultant for foreign governments at FNMT-RCM and an independent expert for the ICAO Technical Co-operation Programme.

Back in 2006, when all the European Union (EU) member States were required to start issuing ePassports according to European regulations and ICAO Doc 9303 specifications, many people in Europe were asking this question: Why are we spending such a lot of money on an electronic document that nobody can read?

Carlos Gómez, R&D and Innovation Manager at Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda, outlines the advantages of electronic passports for Spanish citizens and the valuable lessons the Spanish implementation experience can teach States.

By 2009, the first electronic document verifiers had been deployed to border control facilities and the first Automated Border Control (ABC) systems, like those implemented at the international airports of Madrid and Barcelona, had been installed. With the installation of these systems, there were two advantages to an ePassport for Spanish citizens. First, the ABC systems became a simple, fast and convenient way to cross borders. Second, visas were not required by certain countries thanks to multilateral agreements among States like the Visa Waiver Program (USA), Schengen (Europe), Mercosur (South America), etc.

For States, the ePassport is one of the most secure identity or travel documents ever issued and this represents a number of important advantages. The production and issuance of ePassports can be accomplished in a very secure way thanks to the chip's cryptographic capabilities. In addition, verification at border controls is more reliable thanks to biometrics integrated as part of the chip's contents and authentication of digital signatures and certificates by issuing States.

THE ePASSPORT PROGRAMME

The first lesson we learned from our experience is that States should start by establishing an ePassport production and issuance programme. However, for this programme to succeed, States must first guarantee the security and authenticity of the breeder documents needed to issue an ePassport.

In Spain, the Civil Registry was created in 1870 and offers free services for registration of births, marriages, deaths or changes in names or surnames. Certification services are also available, of which the most important is the issuance of the 'verbatim birth certificate'. This certificate is the only breeder document valid for the issuance of a citizen's first Spanish ID card (Documento nacional de identidad or DNI), which is mandatory at the age of 14 for every Spanish citizen.

The DNI has been regulated by law since 1944 and is the only breeder document valid for issuance of a Spanish ePassport. Both the DNI and the ePassport are issued in Spain by the same authority: the Spanish Police, an organization under the authority of the Ministry of Interior.

The second lesson we learned is establish an ePassport issuance system based on secure breeder documents issued by trusted authorities.

DEFINITION OF ePASSPORT ACCORDING TO ICAO STANDARDS

When States are developing an ePassport programme, special attention must be paid to the definition of an ePassport booklet, particularly as far as the following physical characteristics are concerned:

- Format: The ePassport is comprised of a cover and a minimum of eight pages, including the data page.
- Data page: The recommended practice is to locate the data page on page 2 or on the second to last page of the ePassport.
- Dimensions: As specified in ISO/IEC 7810 for the ID3 size card, namely, 88 ± 0.75 mm x 125 ± 0.75 mm.

A very important aspect is the layout of the data page, which must be standardized, according to ICAO Doc 9303, to facilitate reading of data either by visual or mechanical means. States should also adhere as closely as possible to these recommendations when defining the ePassport's physical characteristics, general layout of the data page and security features.

With regard to security features, it is advisable to refer to the Supplement to Doc 9303. Appendix E contains an update on security Standards for ePassports. Some of the most interesting security features, found in the majority of ePassports being issued nowadays, are the following:

- Overprintings on the cover with invisible ultraviolet (UV) inks
- Intaglio printing in two or more colours, including latent images, on the inside covers
- Microtexts in intaglio and offset printing
- Optically variable inks
- Multitone watermarks
- Invisible fibres with UV response, particularly multicolour fibres with segments in different colours
- Guilloches in several colours with excellent register quality
- Images printed in offset using special security patterns
- Data personalization with invisible UV inks
- Booklet numbering by laser conical perforation
- Holographic film for data page protection

SECURITY FEATURES

Concerning security features, the lessons we learned are the following:

- Select security features according to Doc 9303 recommendations.
- Use proven technology already in use in similar documents.
- Avoid the use of a single supplier's proprietary technology.
- Source out more than one supplier.
- Carry out lab tests before approval of any material or security feature.

As for ePassport production, the set RFID chip and antenna must be integrated into the booklet's construction. There are several placement options, according to ICAO specifications. To some extent, the choice of the integration option depends on the technology selected for the data page construction. Nowadays, there is an increasing tendency towards the use of polycarbonate, although most of the passports still use a data page based on security paper, including the Spanish ePassport, which has the RFID chip and antenna integrated into the back cover.

Table 1: Polycarbonate Data Page

Advantages	Disadvantages
✓ Impossible delamination	✗ Data page and chip in a single component
✓ Lamination protects background printings and personalization data	✗ Weakness in data page substitution
✓ Data personalization takes place in inner layers	✗ Background printing differs from inner pages' background printing
✓ Holograms integrated in inner layers	✗ Portrait personalization in black and white
✓ High durability	✗ Very expensive personalization systems
✓ Possibility of engraving data in relief	✗ Difficult integration of security features in substrate
✓ Water resistant	✗ Need for extra security features
	✗ Re-engravable data page
	✗ Forgery threats by adhesion of personalized thin foils
	✗ Micro-cracks around chip location

When it came to selecting the technology for the data page construction, the advantages and disadvantages of security paper versus polycarbonate for the data page were taken into account. Tables 1 and 2 list some of the topics given serious consideration when selecting a specific technology for the data page technology.

The Spanish experience in this regard leads to the following recommendations:

- Carry out production and lab tests to determine the optimal location for chip and antenna.
- Conduct research to determine whether polycarbonate or security paper data pages are adequate for the ePassport.
- Use proven technology already in use in similar documents.
- Source out more than one supplier for the chip, inlays and eCover.

Table 2: Paper Data Page

Advantages	Disadvantages
✓ Data page and chip in different locations	✗ Data page protection required
✓ Harder data page substitution	✗ Expensive security films for data page protection
✓ Background printing identical to inner pages	✗ Good integration of inlay is a must
✓ Portrait printed in colour	✗ Insulating, stiffer covers
✓ Inkjet personalization inks penetrate into substrate	
✓ Low cost	
✓ Availability of several security features for integration in substrate	
✓ Availability of personalization systems based on UV inks	

When choosing a technology for the chip operating system and the LDS application, we recommend:

- Use proven technology already in use in similar documents.
- Search for an operating system that can operate on at least two different hardware platforms.
- Carry out electrical and functional lab tests for the chip, antenna and operating system before product approval.
- Demand a security certification of the products.
- Control the life cycle of the operating system.

The last item on the previous list, control the life cycle of the operating system, is particularly important, especially if, like the Spanish decentralized issuance system, blank passport booklets must be distributed to a number of issuing points.

INTEROPERABILITY OF ePASSPORT

When we talk about the interoperability of ePassports, we usually think almost exclusively about its electronic components. At the present time, dozens of countries have border controls equipped with electronic document verifiers. Not only are these verifiers capable of reading the RFID chip contents, they can also capture several data page images taken with at least three different light sources: visible, UV and infrared (IR). The portrait of the holder or a pattern—for a subsequent pattern matching

> "…establish an ePassport issuance system based on secure breeder documents issued by trusted authorities."

process—can be extracted from the visible image. The same can be done with the UV image, while an Optical Character Recognition (OCR) process can be derived from the IR image.

In order to ensure ePassport interoperability as a whole, the electronic component as well as the following recommendations should be considered:

- Apply the layout for data personalization as defined in Doc 9303.
- Keep the data page layout as simple as possible.
- Use the page adjacent to the data page for optional data.
- Make sure the format of OCR lines and chip contents are codified correctly.
- Verify the interoperability of the ePassport.

SPAIN'S ePASSPORT ISSUANCE SYSTEM

Spain has a decentralized issuance system for ePassports operating under the responsibility of the Spanish Police. With this decentralized system, citizens are able to obtain their ePassports in about 20 minutes, which is very fast and very convenient. However, we faced a lot of security challenges regarding distribution of blank passports and the physical and logical security of the ePassport issuing system itself.

When designing an ePassport issuance system, the Spanish experience should be borne in mind:

- Evaluate the feasibility of a centralized issuance system versus a decentralized system.
- Establish a scheme for protection of blank passports.
- Verify the security and trustworthiness of breeder documents at issuing time.
- Control the security of the entire issuing process.
- Set up security measures for personnel responsible for issuance.
- Assess the costs of the process.

PKI AND PKD

Spain established its Public Key Infrastructure (PKI) for ePassport issuance in 2006 when the first Basic Access Control (BAC) passports were issued. In 2009, on the occasion of the issuance of Extended Access Control (EAC) passports, a second PKI was set up for verification of EU ePassports.

So far, Certificate Revocation Lists (CRLs) and key distribution have been defined by bilateral agreements. However, since 11 July 2012, Spain has become the 32nd Participant in the ICAO Public Key Directory (PKD).

The lessons we learned from our PKI and PKD experiences are as follows:

- Establish a PKI of ePassport issuance based on proven and trusted technologies.
- Start with the issuance of BAC ePassports.
- Evaluate the necessity of implementing EAC and its associated costs.
- Distribute your keys.
- Join the ICAO PKD.

CONCLUSIONS

According to the recommendations and specifications of the EU and ICAO, Spain succeeded in developing an ePassport and a production and issuance system. Our final recommendations for devising and developing a successful ePassport production and issuance programme are:

- Conduct a study on the present situation of your country's passport issuance system and draw up a thorough transition plan for migrating to ePassports.
- Follow the recommendations of Doc 9303.
- Use proven technologies already in use in similar documents from other countries.
- Evaluate all the products and processes before approval.
- Search for specialized support.

We hope States that have not yet established an ePassport production and issuance programme will learn from our experience. They should also take advantage of programmes like the ICAO Technical Co-operation Bureau and the MRTD Programme (msiciliano@icao.int), which jointly provide technical assistance to States. They can also learn from the experiences of government agencies of other countries that have implemented these kinds of programmes. ■

THE ROLE OF PKI TECHNOLOGY IN eMRTDS

SHARON BOEYEN
is Principal, Advanced Security, at Entrust and a globally recognized expert in PKI and other security and directory technologies. At Entrust, she provides technical guidance to product and service developments and supports the business teams deploying PKI technologies for eMRTD application and other multi-application environments. An active participant in the ITU and ISO PKI Standard commonly referenced as X.509 since 1987, she has held several related leadership roles, including editor of the X.509 standard. She is a co-author of RFC 5280, the primary PKI specification in the IETF, and, since 2007, an active participant in the ISO SC17 WG3 on eMRTD Standards. As a member of the team restructuring Doc 9303, she is responsible for drafting the PKI component.

The Passive Authentication security scheme, defined in Document 9303, protects the authenticity and integrity of electronic data that is stored on a contactless integrated circuit chip. The technology supporting this security scheme is the Public Key Infrastructure (PKI), which plays a key role in the security of electronic Machine Readable Travel Documents (eMRTDs).

Sharon Boeyen, Principal of Advanced Security at Entrust, explains that the security benefits supported by PKI can only be achieved if the technology is properly implemented and deployed by eMRTD issuing States and eMRTD receiving States.

The PKI architecture specified for eMRTD application is a relatively simple one compared to architectures used in typical multi-application PKIs. For example, the eMRTD uses the 'direct' trust model rather than the more complex trust models typically used in widely distributed multi-application environments, such as hierarchical, distributed and bridge trust models. The result is simpler certificate structures that must be created by eMRTD issuing States and much simpler validation processes that should be executed by eMRTD receiving States.

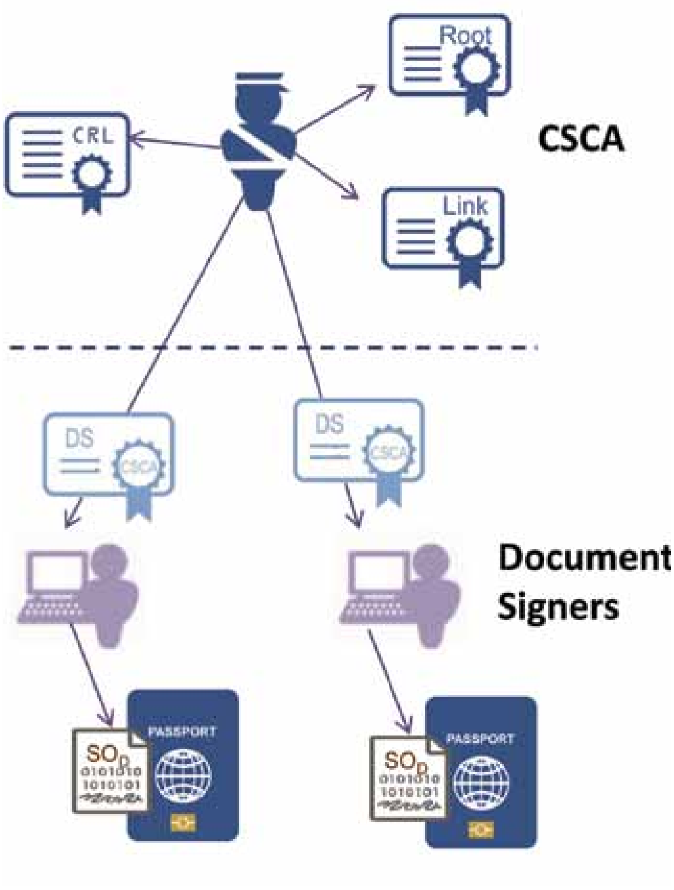
The responsibilities of eMRTD issuing States and eMRTD receiving States are outlined below.

ISSUING STATE RESPONSIBILITIES

eMRTD issuing States are responsible for operating PKI systems to issue certificates and the Certificate Revocation Lists (CRLs). These systems are known as Country Signing Certification Authorities (CSCAs). The systems that generate digital signatures on electronic data and create the Document Security Objects are Document Signers. Each issuing State has only one CSCA but may have several Document Signers. The issuing State is responsible for distribution of its certificates and CRLs to enable their use by eMRTD receiving States—this trust is fundamental to the validation or proof of data integrity and eMRTD authenticity. A typical eMRTD issuing State PKI architecture is illustrated in Figure 1.

In public key technology, keys are generated in pairs: the private key and the public key. The former must be kept private and securely protected. Known only to its owner, it is used by that owner to perform operations such as generating digital signatures. The corresponding public key can be widely distributed and, in the case of digital signatures, is used by others to verify the digital signatures the key owner generates with the private key. In order to bind a specific key to a specific key owner, public keys are distributed in the form of certificates. Certificates are signed by Certification Authorities and contain critical information including the public key itself, the 'subject' or owner of the key pair and additional information such as constraints on that key's use.

Figure 1: Issuing State PKI Architecture



Certificates are issued to Document Signers as well as to CSCAs. After certificates are issued, rare circumstances, such as the compromise of the corresponding private key, can cause them to be revoked. For this reason, the CSCA also issues a CRL, which identifies any certificates previously issued but since revoked and therefore no longer trusted.

CSCA CERTIFICATES

Issuing States issue two types of CSCA certificates: self-signed and self-issued certificates.

Self-signed certificates—commonly referred to as CSCA Root certificates—are typically issued when a new CSCA begins operation. However, optionally, new self-signed certificates may also be issued when CSCA keys are replaced with newer keys. The public key in a CSCA Root certificate verifies the signature on that certificate.

Self-issued certificates—commonly referred to as CSCA Link certificates—are issued when an existing CSCA replaces its keys with a new key pair. The public key contained in a CSCA Link certificate is the CSCA's new public key, while the CSCA's previous public key verifies the signature on a CSCA Link certificate.

The only difference between a CSCA Root certificate and a CSCA Link certificate is the public key being certified. Figure 2 illustrates some of the key elements of CSCA certificates.

In the CSCA Root certificate, the public key being certified is the one corresponding to the private key signing that certificate. In the CSCA Link certificate, the certified public key is a new replacement public key that corresponds to a new private key, which the CSCA uses after issuance of the Link certificate. All other content in the certificates are identical.

As CSCA certificates are all self-issued, the identity of the certificate issuer and the certificate subject, that is, the owner of the certified public key, is identical.

Figure 2: CSCA Certificates

Issuer	Canada CSCA
Subject	Canada CSCA
Key Usage	Certificate & CRL signing
Public Key	Canada CSCA Key 1
Certificate Signed By	Canada CSCA Private Key 1
Certificate Validity	Typically 10-15 years
Private Key Use Period	Typically 3-5 years
Etc.	
CSCA Root Certificate	

Issuer	Canada CSCA
Subject	Canada CSCA
Key Usage	Certificate & CRL signing
Public Key	Canada CSCA Key 2
Certificate Signed By	Canada CSCA Private Key 1
Certificate Validity	Typically 10-15 years
Private Key Use Period	Typically 3-5 years
Etc.	
CSCA Link Certificate	

The key usage element in CSCA certificates restricts use of the certified public key. These keys can ONLY be used to verify digital signatures on public key certificates and CRLS.

It is important to note that CSCA private keys typically have a three- to five-year usage period. The corresponding public key certificate must remain valid until all eMRTDs signed during that period have expired. Typical validity periods for CSCA certificates are 10-15 years. As a result, although a CSCA has only one valid private key at a time, there can be several valid public key certificates for that same CSCA at the same time.

DOCUMENT SIGNER CERTIFICATES

Figure 3 illustrates some of the key elements of Document Signer (DS) certificates. The issuer is the CSCA that issued the certificate and the identity of the Document Signer whose public key is contained in the certificate is the subject.

As with CSCA certificates, the key usage element restricts use of the certified public key. Document Signer public keys can ONLY be used to verify digital signatures. The document type

Figure 3: Document Signer Certificate

Issuer	Canada CSCA
Subject	Canada Document Signer 1
Key Usage	Digital Signature
Public Key	Canada Document Signer 1 Key 1
Certificate Signed By	Canada CSCA Key 1
Certificate Validity	Typically 10 years + 3 months
Private Key Use Period	Typically 3 months
Document Type	"P" (as per MRZ for passports)
Etc.	

further constrains use of the certified public key to a specific document type. In the Figure 3 example, that document type is passports.

Document Signer private keys typically have a one- to three-month usage period. However, the corresponding public key certificate must remain valid until all eMRTDs signed during that usage period have expired. Similar to CSCA certificates, typical validity periods for DS certificates are 10-15 years. As a result, although a Document Signer has only one valid private key at a time, there will typically be numerous valid public key certificates for that same Document Signer at the same time.

CERTIFICATE REVOCATION LISTS

Each CSCA issues a CRL on a regular basis—at least every 90 days. The CRL includes an identifier for each certificate issued by the CSCA and subsequently revoked. Revocations are rare but if one does occur it is important to publish this information quickly to alert certificate users, such as Inspection Systems at border control points. If a revocation occurs, a CRL can be issued immediately rather than waiting until the next regularly scheduled interval.

Revoked certificates, which are identified in the CRL by their certificate serial numbers, must remain on all subsequent CRLs issued by that CSCA until its own certificate validity period has expired.

A CSCA must continue to issue regular CRLs, even though no certificates have been revoked and the CRL therefore contains an empty list. CSCAs must issue a single CRL that covers all DS and CSCA certificates as partitioned CRLs are not supported in the eMRTD PKI.

CSCAs must digitally sign each CRL with the CSCA private key current at the time the CRL is created, even though that CRL may contain revocation notices for certificates signed with earlier CSCA private keys. CRLs cannot be signed with old private keys that have exceeded their stated usage period.

DISTRIBUTION MECHANISMS

To facilitate verification of signatures on eMRTD data by Inspection Systems in all States, CSCA certificates (Root and Link), DS certificates and CRLs must all be distributed globally. Figure 4 summarizes their primary and secondary distribution channels.

There are three primary distribution channels:

- Bilateral out-of-band exchange between States
- ICAO Public Key Directory (PKD)
- eMRTD integrated circuit chip

The primary distribution channel for CSCA certificates is bilateral out-of-band exchange with other States using mechanisms such as diplomatic courier, publication on the

CSCA website, etc. A secondary distribution channel for these certificates, the Master List, is now specified by ICAO in TR: CSCA Countersigning and Master List Issuance (Version 1.0, 23 June 2009).

The PKD is the primary distribution channel for a Master List, which contains a list of CSCA certificates the Master List issuer approves for its own local use after conducting an analysis. Master Lists are digitally signed by their issuers so that users of the lists can authenticate the issuer and verify the integrity of the signed data. Although Master Lists facilitate the task of obtaining CSCA certificates, users of these lists should perform their own analysis before allowing the downloaded certificates to be trusted within their own environments. Issuing States may also decide to publish Master Lists through other channels, such as the Master List issuer's CSCA website.

The primary distribution channel for DS certificates is the eMRTD chip. The PKD remains a secondary distribution scheme for these certificates and is particularly useful for earlier eMRTDs without certificates on chips.

For CRLs, the primary distribution scheme is bilateral exchange directly between States with the PKD its secondary distribution channel.

Figure 4: Distribution Schemes

	CSCA Certificates	Master Lists	Document Signer Certificates	CRL
Primary	Bilateral	PKD	eMRTD chip	Bilateral
Secondary	Master List	Bilateral	PKD	PKD

RECEIVING STATE RESPONSIBILITIES

eMRTD receiving States are responsible for establishing and managing trust relationships with eMRTD issuing States and managing Inspection Systems performing validation and signature verification operations of eMRTD data. Included in that is responsibility for locating and downloading all necessary certificates and CRLs and managing the set of trust anchors for the issuing States with which a trust relationship has been established.

Border control facilities must establish trust in the electronic data stored on the eMRTD chip so that visitors from foreign States as well as a State's citizens returning from abroad can be processed efficiently and effectively.

Establishment of trust has four phases:

- Initial trust establishment
- PKI validation
- Signature verification
- Physical comparison

INITIAL TRUST

Initial trust establishment is a manual process that should be conducted well in advance of border control using the electronic security features of eMRTDs from a given foreign State. Whether or not to establish electronic trust with another State for verifying and validating its eMRTDs is a policy decision, not a technical one. Before such a decision is reached, however, PKI and non-PKI aspects of the foreign State's operations need to be analyzed. PKI related aspects include, for example, assessing the security, reliability and Standards compliance of that State's CSCA and DS systems. Non-PKI aspects include analysis of any existing trust relationship with that foreign State as well as analysis of its policies and procedures for all aspects of the eMRTD issuance process, for example, its policy for verification of evidence of identity documentation.

Establishing trust in the electronic aspects of a foreign State's eMRTDs is of little value if the non-electronic aspects of those eMRTDs cannot be trusted.

PKI VALIDATION

Successful PKI validation ensures the Document Signer's public key, obtained from the DS certificate, is a valid public key that can be used to verify the Document Signer's signature created with the corresponding private key on the electronic data stored on the eMRTD chip.

With centrally managed advance planning, PKI validation can be an automated process at inspection time. The advance planning includes:

- Managing the trust relationships with foreign States.
- Identifying, locating and downloading the set of CSCA certificates, DS certificates and current CRL for each currently trusted State.
- Verifying and validating each downloaded object.
- Configuring and updating, on a regular basis, a set of Inspection Systems with the verified data so those systems can verify DS signatures on eMRTD electronic data.

> PKI plays a major role in eMRTD security as a technology that supports policy-based trust decisions.

In the automated process, the DS certificate is retrieved from the eMRTD chip—the CSCA public key to verify its signature has already been configured as a trust anchor on the Inspection System. The PKI path validation algorithm, specified in Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile, is performed to validate the DS certificate and check the certificate is currently valid, was issued by the correct CSCA and has not been revoked.

Although, in most cases, the DS certificate in question is available directly from the eMRTD chip, downloading DS certificates in advance avoids searching for them at inspection time should they not be present on the chip.

SIGNATURE VERIFICATION

Verification of the Document Signer's digital signature on the electronic eMRTD data is an automated process that involves two cryptographic operations. One operation uses the Document Signer's public key to verify the digital signature. The other creates a digital hash of the data and compares it with the digital hash stored in the Document Security Object at personalization time. Successful signature verification ensures the electronic eMRTD data stored on the chip was signed by a valid Document Signer and unaltered.

PHYSICAL COMPARISON

The final phase, physical comparison, is a manual process. Although Passive Authentication, through its use of PKI, verifies the authenticity and integrity of the electronic data, it does not detect copied/substituted chips. Therefore, the electronic data must be compared to the printed data page to ensure the electronic data corresponds to the printed data on the eMRTD containing the chip.

SUMMARY

PKI plays a major role in eMRTD security as a technology that supports policy-based trust decisions. In order for the benefits of PKI to be realized, both eMRTD issuing States and eMRTD receiving States must implement the necessary systems and policies to facilitate the electronic processes at both ends. Issuing States must implement reliable, secure and compliant systems, including CSCA, Document Signer and personalization systems as well as high quality processes and procedures for the complete issuance process. Receiving States must establish initial trust with issuing States through manual processes supported with PKI technology. Once initial trust is established, automated PKI validation and signature verification can extend that trust to individual eMRTDs. ■

MRTD AND BORDER CONTROL NEWS

Netherlands
New eGates deployed in March at Amsterdam Airport Schiphol rely on facial recognition technology that compares the captured image to the passenger's ePassport photo. More than 100,000 passengers were processed in the first two months of operation.

United States
Face recognition is being deployed in US airports to automate immigration processes, improve surveillance, security and seamless passenger travel and collect statistical information on passenger movements.

France
A joint effort between SITA, Orange, BlackBerry and Toulouse-Blagnac Airport is testing SIM-based Near Field Communication (NFC) so passengers can use mobile phones to pass through the airport's checkpoints, controls and gates.

El Salvador
A gap assessment mission was completed 5-8 June. The OAS/CICTE and ICAO joint project, Capacity Building in Travel Document Security and Identity Management in the Americas, was funded by the Government of Canada.

Republic of South Africa
The Department of Home Affairs announced a new plan for its smart card-based national identity system that will eventually replace the current civic and immigration systems.

European Union
To improve the safety of children while travelling abroad, new EU regulations require all children to travel with their own passports. Children of EU nationals can no longer add their names to their parents' passports.

Republic of Latvia
Latvia is setting up a new infrastructure for issuance and verification of electronic ID documents. The newly established system is based on secunet's eID PKI Suite.

Moldova
A two-day workshop organized by the Organization for Security and Co-operation in Europe (OSCE) promoted the benefits of participating in the ICAO PKD.

United Arab Emirates
New passport and biometrics technology installed at Dubai International Airport is catching increasing numbers of people trying to enter the country with fake ID documents, reports the *Gulf News*.

India
India's Ministry of External Affairs is issuing ePassports to its citizens.

East Africa
Civil aviation authorities from East African (EA) member States want implementation of a single EA passport and a single EAC visa to reduce barriers at entry points and ease movement of citizens.

THE RE-STRUCTURING OF ICAO DOC 9303

TOM KINNEGING
is Senior Expert, Standardization, within the Morpho E-Documents division. He has many years of experience in ICT and project management in the field of Identity Documents and related systems. In ISO, he is the convenor of ISO/IEC JTC1 SC17 Working Group 3 that is developing Standards for MRTDs. He also is the leader of two Task Forces: TF2 - ICAO Doc 9303 and ISO/IEC 7501 Editorial Drafting and TF5 - Data Structure and Security Framework for eMRTDs. As an active contributor to ICAO's TAG and NTWG, he was the editor of various technical papers, such as the Technical Report on PKI for Machine Readable Travel Documents, ICAO Doc 9303 and its Supplement.

With the silicon chip reshaping border controls and travel documents, Document 9303 needs to be incorporated with the latest technologies and solutions to comply with ICAO MRTD Standards and specifications.

The new edition of Doc 9303 is expected to be published in the second half of 2013. Tom Kinneging, Senior Expert of Standardization at Morpho B.V., and the convenor of ISO/IEC JTC1 SC17 WG3, the ISO Working Group supporting ICAO in the standardization of Machine Readable Travel Documents, provides the background on the origins of Doc 9303 and the rationale for its new structure.

Since 1980, ICAO has been mandated under the 1944 Convention on International Civil Aviation to maintain and promote Standards and Recommended Practices (SARPs) related to the issuance of Machine Readable Travel Documents (MRTDs), as outlined in the Convention's Annex 9 and ICAO Document 9303. The reference document for these Standards first started out as guidelines for issuing passports and visa cards but it has since developed into a three-part Standard for MRTDs.

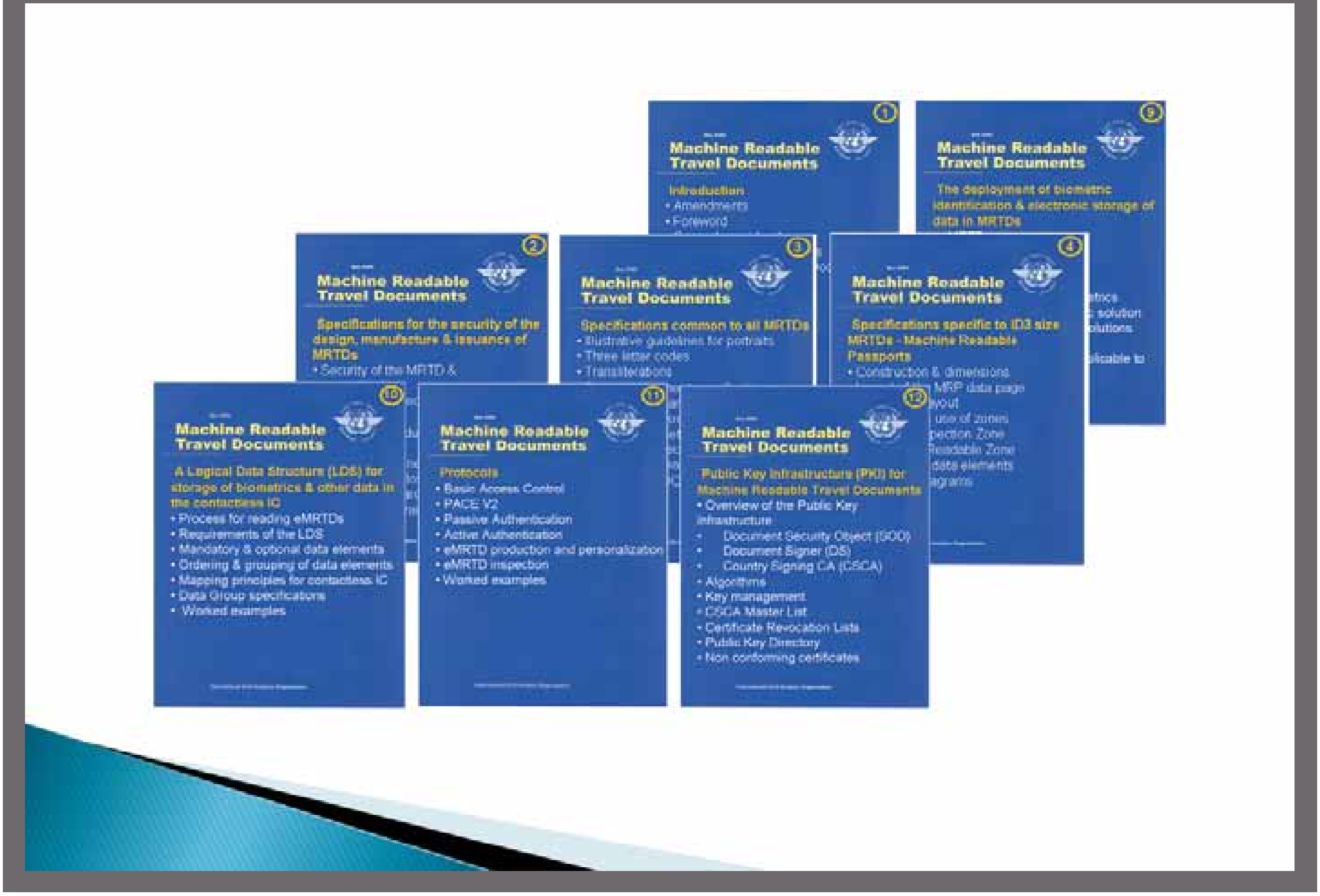
The physical specifications of travel documents differ significantly between passport books and cards, however, electronic specifications for chips, biometric use and cryptographic security are almost identical. Consequently, identical contents have been issued in separate Parts of Doc 9303. Not only has the chip-related information been duplicated, but also general information like three letter country codes, transliteration tables and OCRB typeface information have been published more than once in all three Parts.

In addition, as the three Parts of Doc 9303 have different issue dates, changes and updates may or may not have been incorporated at the time of their individual releases. Therefore, the information cannot be considered 'duplicate' but 'more or less duplicate'. As a result, maintaining the three Parts and ensuring the specifications are consistent is a complex time consuming undertaking.

New releases of Doc 9303 are usually drafted and published every five years. In the interim, new specifications are published in Technical Reports, which are effectively part of the Standard and envisaged to be incorporated into the next edition of Doc 9303. At the moment, six Technical Reports are 'waiting' to become part of a new edition of Doc 9303.

With the introduction of chip technology in travel documents, ICAO established a mechanism to address the vast range of issues border and airport authorities would encounter once this new technology was implemented. As a result, the Supplement to Doc 9303 was created to provide guidance, advice, updates and clarifications to MRTDs and a systematic continuing forum in which views are recorded and shared, issues raised and addressed and clarifications communicated. It contains any matters that must be urgently distributed and cannot wait for publication of a Technical Report or the next release of Doc 9303. Since 2004, 11 releases of the Supplement have been published.

ePASSPORT BOOK



1

Machine Readable Travel Documents

Introduction
- Amendments
- Foreword

9

Machine Readable Travel Documents

The deployment of biometric identification & electronic storage of data in MRTDs

2

Machine Readable Travel Documents

Specifications for the security of the design, manufacture & issuance of MRTDs
- Security of the MRTD &

3

Machine Readable Travel Documents

Specifications common to all MRTDs
- Illustrative guidelines for portraits
- Three letter codes
- Transliterations

4

Machine Readable Travel Documents

Specifications specific to ID3 size MRTDs - Machine Readable Passports
- Construction & dimensions

10

Machine Readable Travel Documents

A Logical Data Structure (LDS) for storage of biometrics & other data in the contactless IC
- Process for reading eMRTDs
- Requirements of the LDS
- Mandatory & optional data elements
- Ordering & grouping of data elements
- Mapping principles for contactless IC
- Data Group specifications
- Worked examples

11

Machine Readable Travel Documents

Protocols
- Basic Access Control
- PACE V2
- Passive Authentication
- Active Authentication
- eMRTD production and personalization
- eMRTD inspection
- Worked examples

12

Machine Readable Travel Documents

Public Key Infrastructure (PKI) for Machine Readable Travel Documents
- Overview of the Public Key infrastructure
- Document Security Object (SOD)
- Document Signer (DS)
- Country Signing CA (CSCA)
- Algorithms
- Key management
- CSCA Master List
- Certificate Revocation Lists
- Public Key Directory
- Non conforming certificates

For the user, navigating through Doc 9303 is complex. To be fully informed, the user must read relevant Part(s) of the Standard as well as the associated Technical Reports and the Supplement designed by the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) and its Working Groups.

THE ISSUANCE PROCESS

Until 2009, issuing Parts of Doc 9303 as separate documents made perfect sense to users of the Standard. As the documents were all paper-based, this was the only way to issue the information in a comprehensive way.

Since December 2009, ICAO issues Doc 9303 electronically in PDF format. This new approach allows the user to download the complete Standard or Parts of it, free of charge. The electronic format opens up a world of opportunities to improve both its maintainability as well as its readability through a new more efficient format.

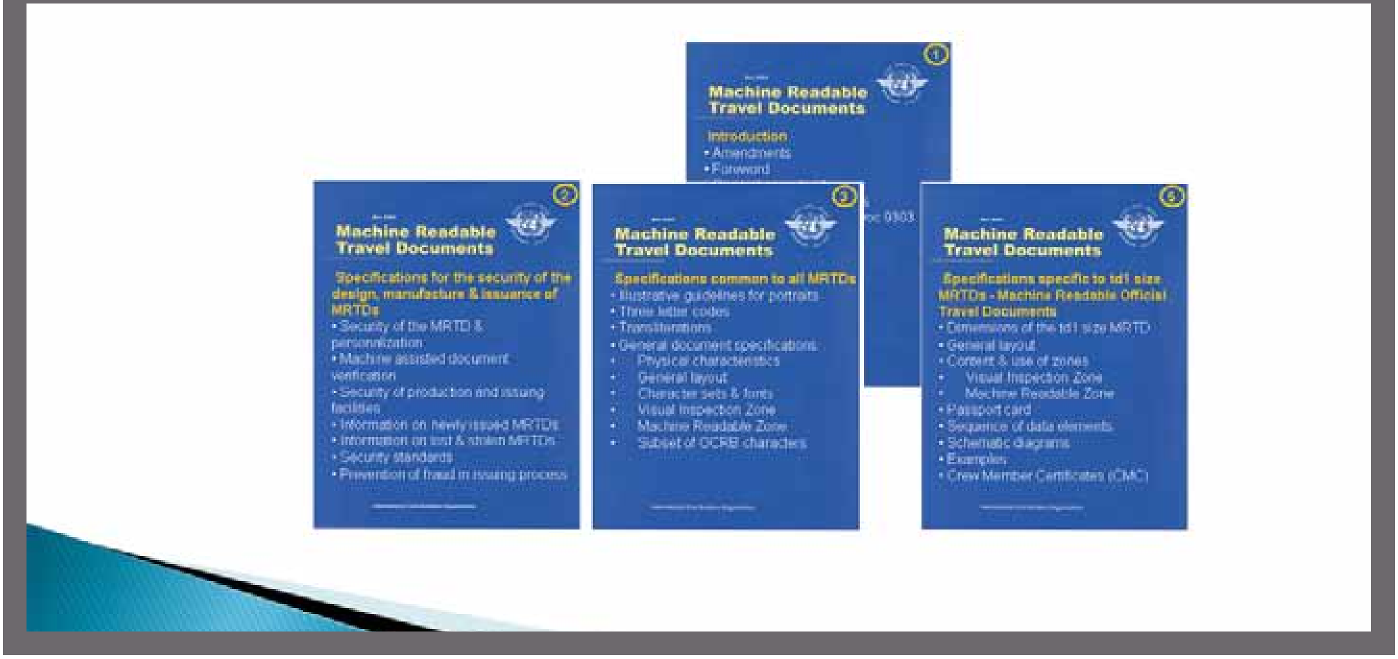
RE-STRUCTURING PROJECT

At its 20th meeting in September 2011, the TAG/MRTD endorsed the Working Paper to re-structure Doc 9303 and incorporate the six Technical Reports and the Supplement. An editorial group was formed and work on the project commenced.

In designing this new structure, improved readability and maintainability are the key goals of the editorial group and the following principles are being taken into account:

1. Physical and electronic specifications will appear in the Standard only once.
2. Doc 9303 will consist of a single set of specifications for td1, td2 and ID3 size documents comprised of various PDF files in which general—applicable to all MRTDs—as well as MRTD type specific specifications are grouped.
3. For each MRTD type, clear references will be made to help users access the relevant subset of specifications applicable for that type.

NON-CHIP td1 CARD



1

Machine Readable Travel Documents

Introduction
- Amendments
- Foreword

Doc 9303

2

Machine Readable Travel Documents

Specifications for the security of the design, manufacture & issuance of MRTDs
- Security of the MRTD & personalization
- Machine assisted document verification
- Security of production and issuing facilities
- Information on newly issued MRTDs
- Information on lost & stolen MRTDs
- Security standards
- Prevention of fraud in issuing process

3

Machine Readable Travel Documents

Specifications common to all MRTDs
- Illustrative guidelines for portraits
- Three letter codes
- Transliterations
- General document specifications
- Physical characteristics
- General layout
- Character sets & fonts
- Visual Inspection Zone
- Machine Readable Zone
- Subset of OCRB characters

5

Machine Readable Travel Documents

Specifications specific to td1 size MRTDs - Machine Readable Official Travel Documents
- Dimensions of the td1 size MRTD
- General layout
- Content & use of zones
- Visual Inspection Zone
- Machine Readable Zone
- Passport card
- Sequence of data elements
- Schematic diagrams
- Examples
- Crew Member Certificates (CMC)

In the first phase of the project, these principles led to a new design of Doc 9303, consisting of 12 Parts that organize Doc 9303 in a different way but do not change the specifications:

- *Part 1, Introduction*
- *Part 2, Specifications for the Security of the Design, Manufacture and Issuance of MRTDs*
- *Part 3, Specifications Common to All MRTDs*
- *Part 4, Specifications Specific to td3 size MRTDs, Machine Readable Passports*
- *Part 5, Specifications Specific to td1 size MRTDs, Machine Readable Official Travel Documents*
- *Part 6, Specifications Specific to td2 size MRTDs, Machine Readable Official Travel Documents*
- *Part 7, Specifications Specific to Machine Readable Visas*
- *Part 8, Specifications Specific to Emergency Travel Documents*
- *Part 9, Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*
- *Part 10, Logical Data Structure for Storage of Biometrics and Other Data in Contactless IC*
- *Part 11, Security Protocols*
- *Part 12, Public Key Infrastructure for Machine Readable Travel Documents*

This structure offers the user the ability to select only the Parts relevant for a specific MRTD form factor. For example, ePassport specifications will typically consist of Parts 1, 2, 3, 4, 9, 10, 11 and 12 (refer to the sidebar, ePASSPORT BOOK). Within that selection, developers would be interested in specific parts, that is, a PKI developer on an ePassport project would focus on Part 12 whereas a graphic designer would be interested in Parts 2, 3 and 4. On the other hand, a td1 card project without any chip technology would rely on Parts 1, 2, 3 and 5 (refer to the sidebar, NON-CHIP td1 CARD).

The second phase of the project consists of incorporating the more than 145 issues addressed in the Supplement. The mere fact these issues are contained in the Supplement indicates Doc 9303 is unclear or ambiguous on various subjects and therefore can be improved. Each issue will be evaluated in relation to the relevant descriptions in the Standard and, where useful, the text in Doc 9303 will be adapted. In accordance with the Supplement's intent, the nature of this activity will be to *clarify*, not change, the existing specifications. In the third phase, the Technical Reports will be incorporated into the Standard.

TIMELINE

The project is on schedule and the timetable is as follows:

- Design of the new structure: Quarter 4 2011
- Finalization of the re-structuring: Quarter 3 2012
- Incorporation of the Supplement: Quarter 4 2012
- Incorporation of the Technical Reports: Quarter 2 2013
- Editing, translation and publication: Quarter 4 2013 / Quarter 1 2014

The result will be a newly structured Doc 9303, 7th edition, published electronically by ICAO, which will outline the latest technologies and solutions for MRTDs in a streamlined more user-friendly format. ■

THE PKD: THE ISSUES AND THE CHALLENGES

ECKART BRAUER
is a senior civil servant in the Federal Ministry of the Interior of Germany who is responsible for biometrics strategy and document security in the domestic, EU and international context. Within that function, he is a Member of the Committee pursuant to EU Regulation 1683/95 that establishes a uniform format for visas, passports and residence permits (known as Article-6-Committee). He is also a Member of TAG/MRTD and the PKD Board, which he chaired from May 2008 to May 2012.

The ICAO Public Key Directory (PKD) was established to promote a globally interoperable ePassport validation scheme for electronic travel documents in support of ICAO's strategic objectives to improve aviation security and the efficiency of civil aviation. The PKD is maintained by ICAO on behalf of PKD Participants in order to facilitate the validation of data in electronic Machine Readable Travel Documents (eMRTDs).

Eckart Brauer, Senior Officer of the German Ministry of the Interior, who chaired the PKD Board from May 2008 to May 2012, provides insight on the issues and challenges he experienced during his four-year term.

ICAO *MRTD REPORT*: DR. BRAUER, HOW EASY OR DIFFICULT WAS IT FOR YOU TO HAND OVER THE RESPONSIBILITIES OF PKD BOARD CHAIR AFTER SUCH A LONG TIME?

Eckart Brauer: I handed over the position with mixed feelings. On the one hand, I was tempted to continue the successful work given the support of the PKD Board. On the other hand, there was no better time to renounce my candidacy as, with all the substantive PKD issues resolved, the new Chair could adjust to the position. In the end, the latter choice prevailed.

"...the legal obligation to introduce ePassports and participate in the PKD is of utmost importance."

IF YOU COMPARE THE SITUATION IN 2008 WITH THAT OF 2012, WHAT ARE THE MAIN DIFFERENCES?

My predecessor established the PKD Board from scratch within one year—a challenging enough task. Therefore, it was not surprising that I found a number of unresolved issues on my desk when I started in 2008. I will highlight just a few. In my opinion, it could not be taken for granted the PKD would become a success as it was still lacking an operational contract between ICAO and the PKD Operator. As a consequence, there was no clarity about the fees for participation in the PKD. In addition, the PKD contents did not yet cover the entire ePassport certificate chain as the Master Lists of CSCA Certificates were not yet implemented.

The next issue was that other forums for exchanging cryptographic material to validate ePassports nurtured the myth that bilateral exchanges would be sufficient. Also, the role of the PKD Board required improvement in terms of decision making regarding documentation and follow up. These issues and others caused a lot of doubts about the PKD. In a nutshell: there was little attraction to participate in it. But within four years, the PKD Board and I reversed the situation completely. We resolved the initial drawbacks and today there are no further criticisms of which I am aware.

WHAT HAS BEEN ACHIEVED DURING THOSE YEARS?

Some important milestones included reducing the one-time PKD Registration Fee from US $85,000 to US $56,000. In addition, with growing PKD participation, the shared burden principle for the ICAO part of the Annual Fee has led to decreasing fees. An operational contract as of 2009 and its extension as of 2012 guaranteed a smooth continuation of PKD services for all PKD Participants so they can easily prepare for automated PKD use. With the implementation of a procedure to handle non-standard conformant PKD contents, the PKD has evolved into the implemented operational reference for ICAO Document 9303 that ensures worldwide interoperability despite national circumstances that seem to resist it. With the Master Lists, today the PKD covers 50 ePassport issuing States.

Moreover, the PKD achieved political support from the G8, the Organization for Security and Co-operation in Europe and the European Union. And there is a very attractive PKD logo that is easily recognizable on the web and at international conference presentations. All this became possible because of the thorough and hardworking PKD Board. I once again thank all my colleagues around the world for their sustained support. We can be proud of what has been achieved.

WHAT ARE THE CHALLENGES FOR THE NEW PKD BOARD CHAIR?

Despite all these efforts, not everything is resolved and perfectly satisfactory. ICAO intends to place a tender for the PKD operational contract as of 2015 because the existing contract cannot be prolonged. The PKD Board must deliver substantive input for this tender procedure. For the next two years, this will be the main issue. In addition, the current number of 32 PKD Participants is impressive—when I started as Chair there were only nine. But there is still a serious gap in the number of ePassport issuing States, which is around 90 or 100. The present approach of promoting the PKD with workshops, presentations and written contributions to periodicals was sufficient to reach a critical mass of PKD Participants, including a number of global players. However, there is still no silver bullet to reach the many ePassport issuing States that are reluctant to participate in the PKD.

DO YOU THINK THAT ICAO CAN STILL ENHANCE ITS SUPPORT TO THE PKD BOARD?

Yes, I think so. The good news is ICAO announced that PKD expenses would be covered by the ICAO budget in 2012. There must be an ongoing commitment to further reduce the financial burden of the PKD Participants, which will also facilitate management of the PKD Board's budget. However, the legal obligation to introduce ePassports and participate in the PKD is of utmost importance. The next meeting of the ICAO Facilitation Panel in October this year deals with that question and I hope the outcome is the right one.

WHAT MESSAGE DO YOU HAVE FOR ALL THE UNDECIDED STATES THAT DO NOT PARTICIPATE IN THE PKD?

All those States that issue ePassports must be aware that an ePassport is treated as a passport without a chip, if there is no ability to validate the signature of the chip contents. This means the ePassport does not provide added value, which was the argument for its introduction. Therefore, the pertinent question is: why are people forced to pay a small fortune for an ePassport if nobody cares about the 'e' inside it? All States that issue ePassports can participate in the PKD, though I admit the regulation concerning national responsibility for the PKD and the installation of a national permanent budget for PKD expenses cannot be completed in one day.

I often hear that the fees for PKD participation are too high but I believe that is more of an excuse. The financial burden is small compared to a State making its own arrangements to exchange ePassport certificates worldwide. It is also a myth that for PKD participation national automated border controls are necessary.

The strongest argument for participation in the PKD is that ePassport standard conformance is reached and maintained as PKD Participants directly profit from the PKD Board's expertise. To put it another way: Secure worldwide travel with an ePassport is a successful facilitator in a global economy.

WHAT SOLUTIONS HAS THE PKD OFFERED AND IMPLEMENTED TO ACCOMMODATE POSSIBLE 'DEVIATIONS' IN THE IMPLEMENTATION OF ePASSPORT PROJECTS?

It is not always easy to fully understand ICAO Document 9303, the Technical Reports and the Supplement—given their extent and complexity. As a consequence, there are implementation 'deviations' that may be based on domestic, legal and technical restrictions as well as different opinions concerning the options or details missing from Document 9303. Insufficient experience or expertise can also play a role. On a global scale regarding ePassport based travel and verification, some ePassports and their respective signature verification certificates do not perform as expected or require specific treatment in order to allow automated hassle free use. The PKD Board, in cooperation with ICAO and ISO, implemented a set of PKD Upload Contents checks and error codes so that every border control authority or any other user is fully aware of the interoperability or security issues when downloading certificates or Certificate Revocation Lists (CRLs) from the PKD. You are invited to visit the PKD Board website for further information: www.icao.int/Security/mrtd/Pages/icaoPKD.aspx

ARE THERE ANY NEW INCENTIVES FOR STATES TO JOIN THE PKD?

Yes. The operational contract foresees reducing the PKD Operator's Annual Fee to around US $30,000 when there are 31 PKD Participants. Currently, the annual charge is US $43,000 for a full year of active PKD use, including automated uploads and downloads. However, the PKD Board and the PKD Operator are still resolving the details of this reduction. But as we now have 32 PKD Participants, the reduction will come sooner or later. I already mentioned the financial support we have received from the ICAO budget. I expect an Annual Fee reduction of about US $10,000 per PKD Participant per annum—should this support become permanent.

LOOKING INTO THE FUTURE, WHAT LONG-TERM DEVELOPMENTS DO YOU EXPECT OR RECOMMEND FOR THE PKD?

I am not a fortune teller, but in the short-term or medium-term, it will be mandatory to issue ePassports and participate in the PKD. Furthermore, the PKD Board is in close cooperation with ICAO and ISO to check how the so called Defect Lists can be implemented in the PKD. It is expected that this would significantly improve the flexibility of non-conformance handling. What I do not expect is that the PKD will manage access control certificates for ePassport secondary biometrics like fingerprints. This would be a desirable feature but a new PKD architecture and business model would be required, which is too complex given the uneven distribution of secondary biometrics use today. What I recommend is to keep the PKD Board an independent body. In my opinion, being subordinate to the ICAO Council or being integrated into ISO would not be helpful. The PKD Board always acted quickly and was pragmatic. This operational flexibility should be preserved.

DR. BRAUER, ARE YOU GOING TO CONTINUE REPRESENTING GERMANY ON THE PKD BOARD?

Yes, for the time being. Nevertheless, I cannot rule out changes in the future.

WOULD YOU CONSIDER APPLYING FOR THIS POSITION AGAIN IN THE FUTURE?

No, I do not think so. The PKD Board has plenty of qualified people who can fill the position of Chair. The crucial point is that not all of them receive the required support from their home State to attribute enough time to the work of the PKD Board. But so far the PKD Board has always found someone who is willing to take on the responsibility. ■

A LEGAL, UNIQUE AND SECURE IDENTITY FROM BIRTH

For some time, ICAO and ICAO member States have expressed concern about weaknesses in civil registries and the quality and veracity of the basic identity, or breeder, documents required to obtain a Machine Readable Travel Document (MRTD). While these are valid concerns, there are much wider governance implications as well as considerable social and economic consequences for millions of people around the world who are barred from obtaining legal identity documents.

Mia Harbitz, Senior Registries Specialist at Inter-American Development Bank, takes a closer look at the context in which civil registries function in order to find viable solutions to a multifaceted problem.

A civil registry has two main responsibilities: the primary one is to establish the identity of a person—ideally at birth—and the secondary one is to inform a country's national statistical system of vital events, such as births and deaths, to generate vital statistics. Vital statistics are indispensable for political decision-making processes and evidence-based policy making.

The lack of breeder documents exacts considerable costs to both the individual and society as a whole. The United Nations Development Programme (UNDP) calculates the Human Development Index (HDI) yearly based on statistical reporting conducted by countries. The HDI serves as a frame of reference for both social and economic development and is a composite indicator, that is, a comparative measure of life expectancy, literacy, education and standards of living. The more developed the country, the higher the HDI.

The same is true of birth registration. In more developed countries, there may be less concern about national breeder documents given the universality of birth registration and hence a more reliable process of establishing legal identity from birth. We understand legal identity as a composite of biographic, biometric and attributed identifiers. The combination makes the identity unique and the responsibility for safeguarding the data lies with the identity provider or the civil and identification registry.

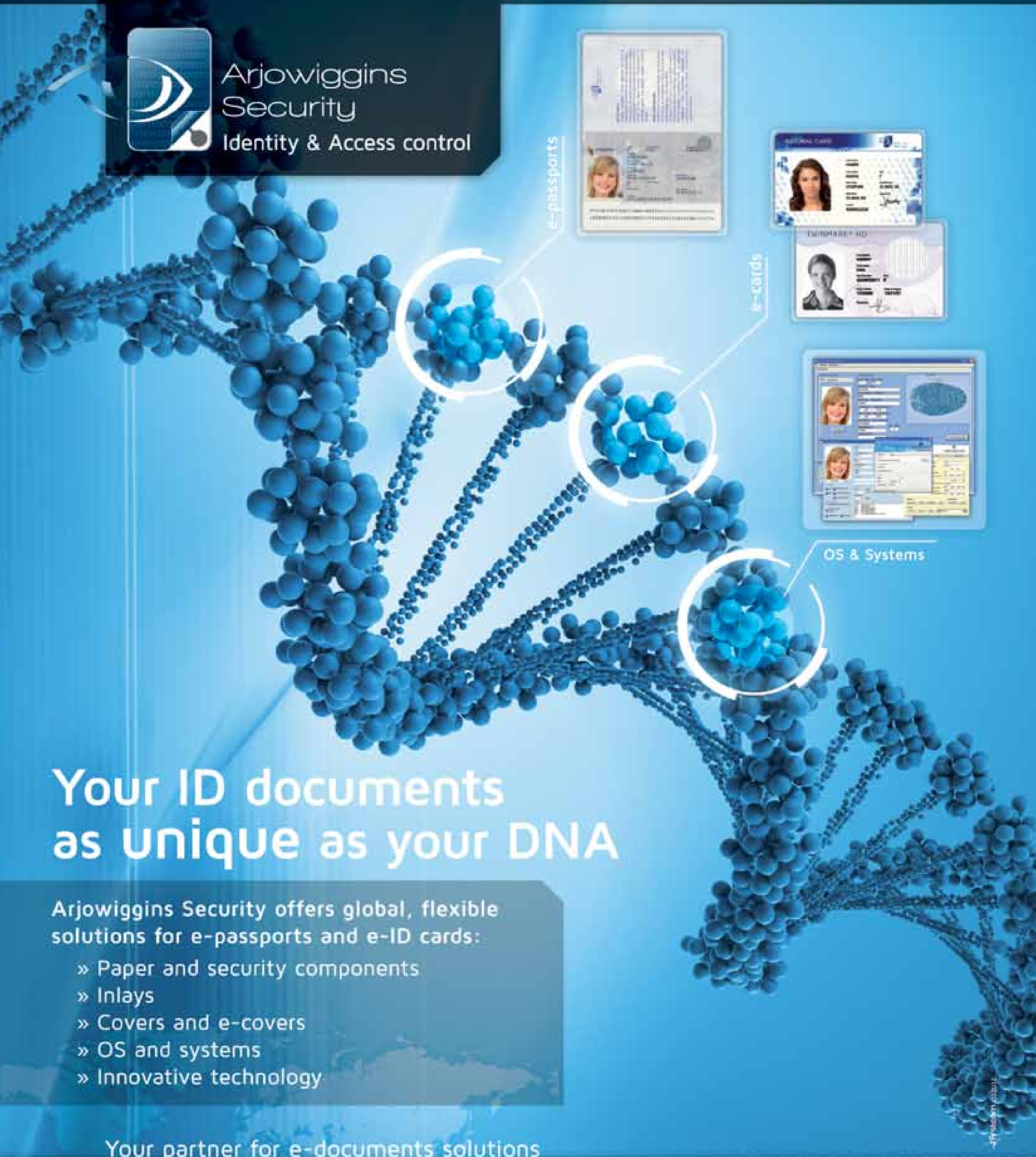
Having a name and a nationality are basic human rights. However, every year millions of children are born without their birth information being recorded. As a result, they run the risk of living their lives as 'ghost citizens' without access to benefits and constitutional rights. In turn, these citizens cannot obtain basic needs, such as health and educational services, passports, drivers' licenses. In addition, they cannot vote, open bank accounts or have access to formal employment and retirement benefits.

Countries are increasingly aware of this problem and are making efforts to improve the civil registry systems. Over the past decade, there have been many attempts to mitigate under-registration and late registration, that is, birth registration that occurs after the timeframe established in national legislation. Latin American and Caribbean countries have committed to reducing the under-registration rate to five per cent or less by 2015.

HINDERING FACTORS

Obstacles for a timely birth registration can be found in both the demand and the supply sides of the process. Common reasons for parents not registering a newborn include

MIA HARBITZ
With over 25 years' experience in development projects, Mia Harbitz is the senior expert in public registries in the Institutions for Development Sector of the Inter-American Development Bank (IDB). Since 2004, she coordinates the IDB's activities on civil registration and identity management. Her principal responsibilities have included studies assessing the practical implications of under-registration of citizens in Latin America and projects strengthening public registries' institutional and administrative capacity, while improving the quality of national vital statistics systems and promoting universal birth registration and civil identification. She has contributed to a number of publications and books and, prior to coming to Latin America in 1991, she worked in development programmes in East Africa and the Middle East.


e-passports
e-cards
OS & Systems

difficulties in accessing the registry office because of distance or seasonal weather conditions, poverty, cultural barriers, such as language and customs, discrimination against single mothers and the digital divide.

Civil registries often suffer from inadequate government resources, lack administrative capacity and maintain a limited institutional presence. There are also cumbersome legal processes if the registration does not adhere to certain parameters. Each country has established a maximum timeframe for birth registration—usually 30-45 days after the birth of a child. If the birth registration takes place after that date, a fee or a fine may be imposed and sometimes the registration process will require additional attestations by witnesses. These procedures are cumbersome and are often prohibitively expensive to persons with limited resources.

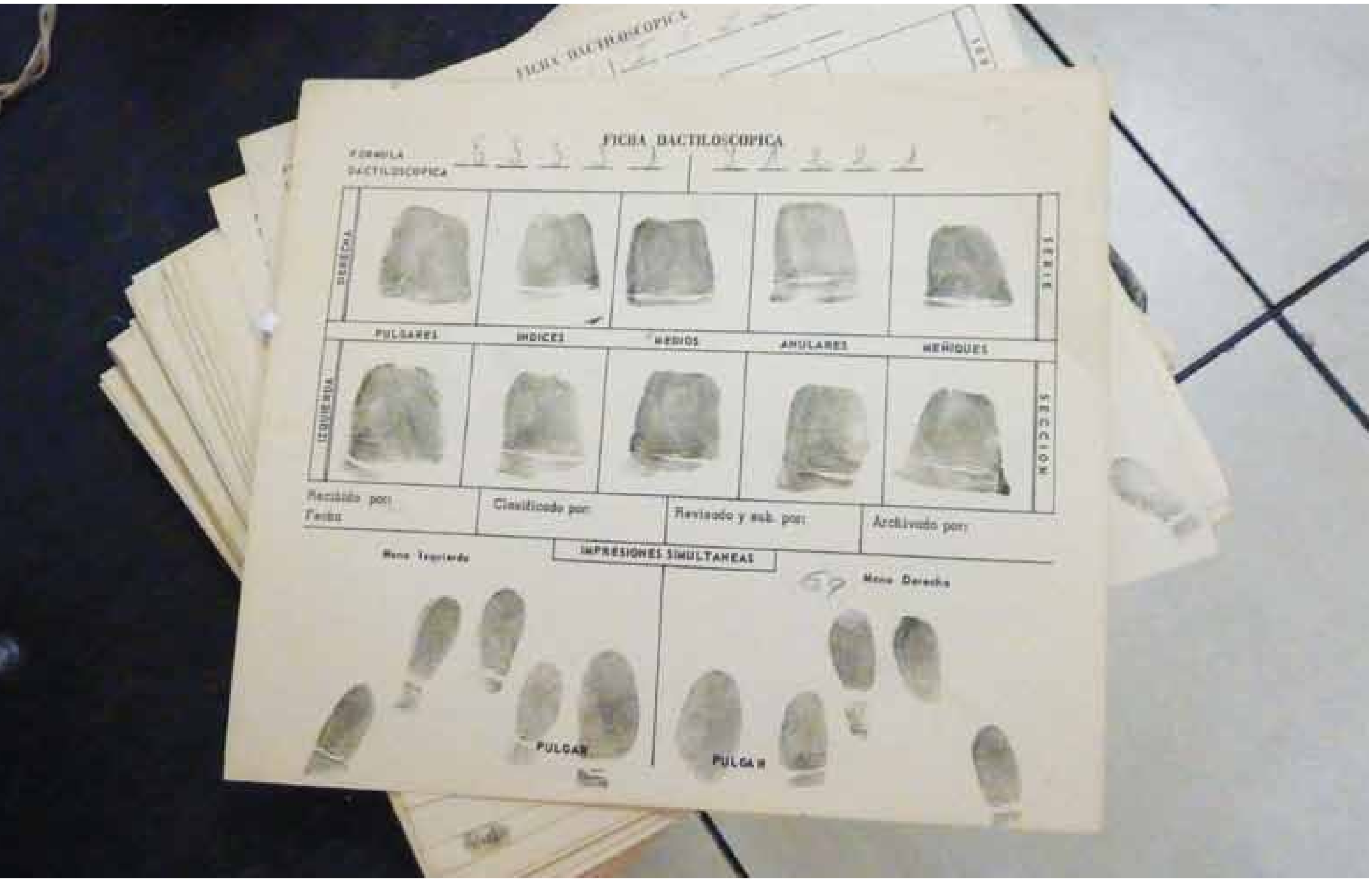
Children whose identities are established in a timely manner with their name, date of birth, place of birth and parents' names recorded are much more likely to receive the recommended childhood vaccines and get an education than those whose births have been unregistered.

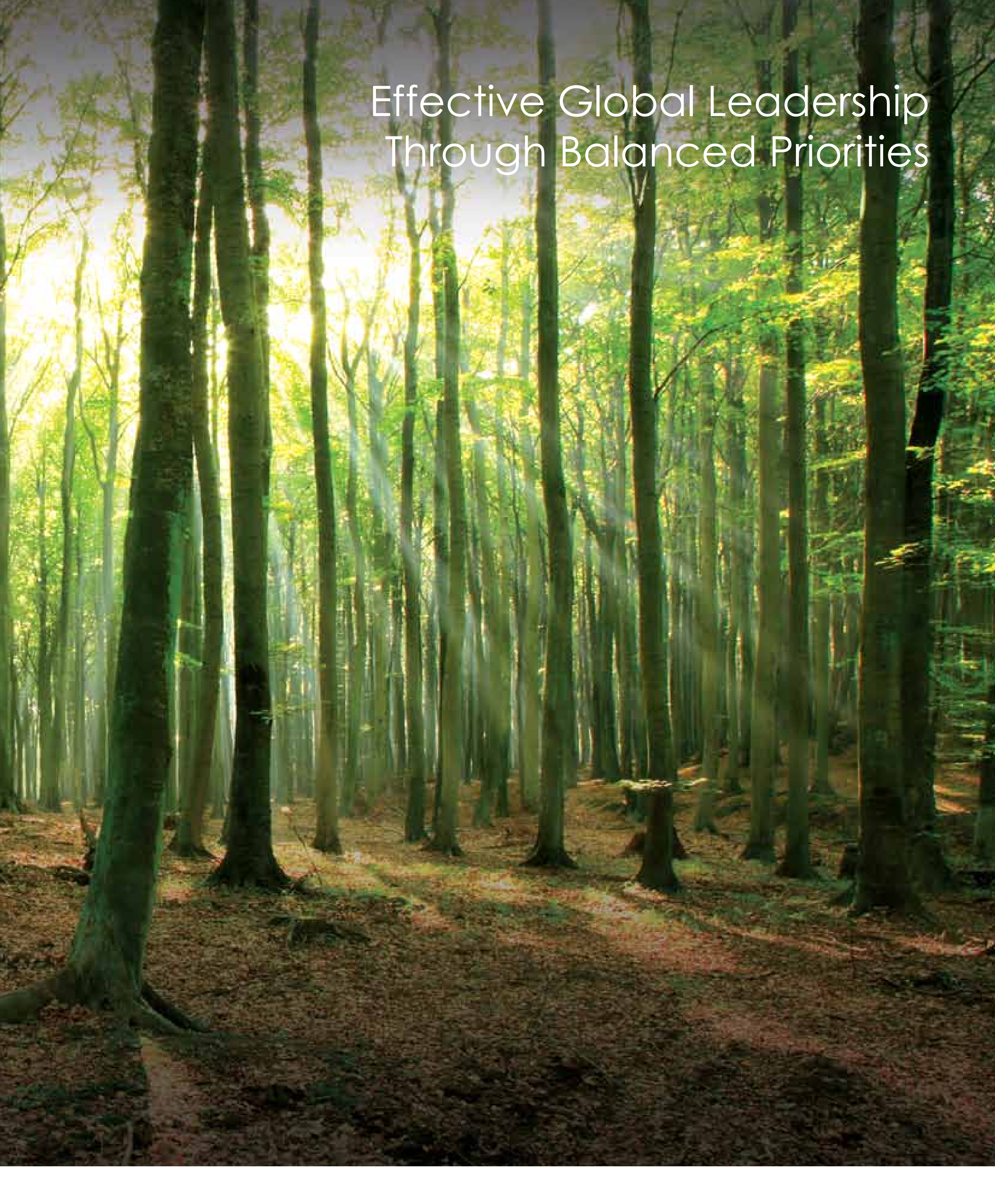
There are several reasons why universal birth registration and the establishment of a legal, unique and secure identity for birth are important to an international financial institution, such as the Inter-American Development Bank (IDB). The bank's mission is to support economic and social development and measure progress in member countries in which they invest. In order to do so, solid and reliable statistical systems are necessary. The bank also has to ensure the borrowed funds are used as established in the contracts and, in the case of social programmes, that the funding and the benefits reach the intended individuals or target groups. An eligible beneficiary, however, cannot receive his or her due assistance without a valid identity document.

To address the challenges of establishing secure identity management systems, the IDB has supported borrowing member countries for nearly a decade through studies, technical cooperation, such as donations and loans. The IDB is uniquely suited to promoting multi-sector strategies by emphasizing evidence-based lines of activities, measuring results, proactively sharing lessons learned with member countries and applying these lessons to new projects. A multi-disciplinary approach is required to combat under-registration of births and ensure a legal and unique identity for all citizens and residents.

THE ONGOING CHALLENGES

If birth registration is not universal, it will be challenging to establish a legal identity for all. To reach the goal of universal birth registration,





www.icao.int

The International Civil Aviation Organization

systems linking the civil registry to different key stakeholders, such as the Ministry of Health, the Ministry of Social Development (or Affairs) and statistical and passport agencies, among others, need to be in place.

The process to reach a fully integrated electronic registry system, however, must be staggered. For instance, working conditions in many registry offices in Latin America and the Caribbean, in both urban and rural areas, continue to be dismal. While the main office in the capital may be automated, many of the offices around the region still rely on the handwritten, two-book system—one of these books is sent to the central civil registry office for storage at the end of the year. Ideally the information is then entered into a central database, but often the records are stored in less than ideal conditions. Often, a citizen who wants to obtain a copy of his or her birth or marriage certificate must know where the registration originally took place as well as the year and date.

In countries where there is a push to automate the civil registry, it seems little forethought has gone into developing a common architecture to ensure interface with other relevant agencies. A grave concern is that the public sector often lacks the resources to retain qualified Information Technology personnel and the result appears to be vendor-driven modernization solutions. This leads to doubts in terms of sustainability of the system, sovereignty of the data and security of the information.

The unfortunate reality is, in many developing countries, civil registries are restricted by a lack of adequate resources and institutional and administrative constraints. The result is that birth registration records are incomplete, in imperfect condition, error-ridden or are characterized by a combination of all three factors.

THE ROLE OF THE CIVIL REGISTRY

More attention must be paid to the role of the civil registry as the primary source of vital statistics and its importance for governance. Countries with higher under-registration rates have less reliable demographic and statistical information about their citizens and residents and run the risk of under- or over-dimensioning public policies and programmes. Take, for example, the issue of how many childhood vaccines are needed for a particular vaccination campaign. Too many vaccines may signify a considerable extra cost to the government and too few may signify under coverage of a crucial vaccine. When birth and death registrations are not universal and/or late, the vital statistics are flawed in the best of cases and downright wrong in the worst of cases.

Furthermore, 10 of the indicators used to monitor the progress of the United Nations Millennium Declaration are linked to information originating in the civil registry. For example, one of the goals of the Millennium Declaration is universal education. If a country's Minister of Education does not know how many children were born in any given year, a number which originates in the civil registry, it is impossible to correctly plan for the number of required classrooms and teachers. Furthermore, many countries require a birth certificate as proof of identity to allow children into school in the first place. Without this document, they are often refused entry and effectively excluded from access to public education.

Children who are born in hospitals stand a better chance of being enrolled in the civil registry, while children born at home are at a greater risk of remaining undocumented because of the distance to civil registry offices and the direct and indirect costs associated with enrolment. In these cases, it is particularly important to establish the identity of the person, or persons, who want to register the child. Unfortunately, in many developing countries illegal adoptions and trafficking of children abound and those with malicious intentions exploit weaknesses in the civil registry systems.

If countries are going to be in a position to emit MRTDs based on verifiable and reliable breeder documents, civil registries need to be strengthened and upgraded to provide the services they are responsible, by law, to deliver to citizens and residents. It is necessary to link civil registration with civil identification processes, that is, the recording of biometric and attributes, and update or, in some cases, create legislation to protect personal data.

Many countries push for an electronic government, but in order for this to be effective and accessible for all, it is necessary to establish secure identities for clients. The digital divide continues to be a concern—given the relatively low Internet penetration rate in developing countries. A more creative—and secure—way would be using mobile phones in civil registration and identification processes to establish a legal and unique identity in order to produce safer breeder documents and, in turn, improve the veracity of the identity behind every MRTD. ■

Visit them at www.icao.int/mrtdc

Entrust® Securing Digital Identities & Information

SECURITY ON

entrust@entrust.com
www.entrust.com/epassport
888-690-2424 or 613-270-3400

The trust foundation for issuance and validation of MRTDs, citizen eIDs and ePassports

foster + freeman

Document Examination Solutions

www.fosterfreeman.com
usoffice@fosterfreeman.com
888 445 5048

Ingo Liersch
Head of Segment Marketing

Giesecke & Devrient

Goverment Solutions
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
P.O. Box 80 07 29
81607 Munich
Telephone +49 89 4119 - 2869
Fax +49 89 4119 - 96 18
Mobile +49 172 8594185
ingo.liersch@gi-de.com
www.gi-de.com

GET GROUP

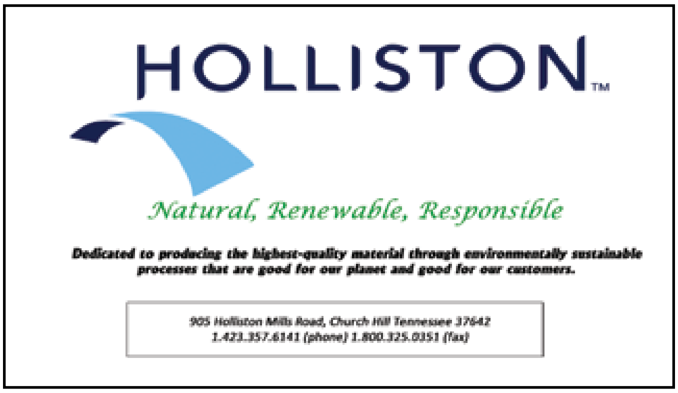
GET.Into the future

Global Enterprise Technologies Corp.
230 Third Ave., Waltham, MA 02451 USA
T: +1 781 890 6700
F: +1 781 890 6320
email: info@getgroup.com
www.getgroup.com

ID programs that
fit your country

HID

hidglobal.com/citizen-ID


HOLLISTON™

Natural, Renewable, Responsible

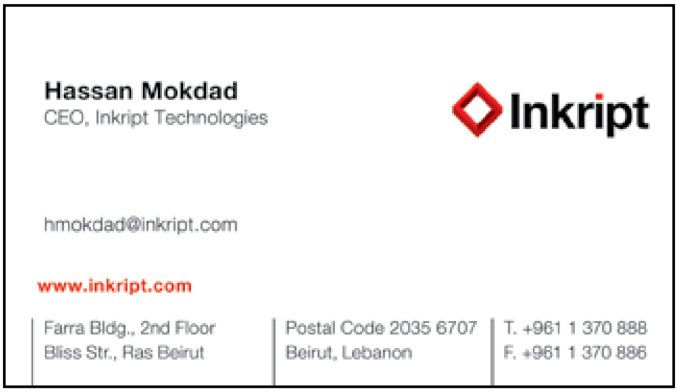
Dedicated to producing the highest-quality material through environmentally sustainable processes that are good for our planet and good for our customers.

905 Holliston Mills Road, Church Hill Tennessee 37642
1.423.357.6141 (phone) 1.800.325.0351 (fax)

Bart Crols
Sales Manager
M +31 (0)6 11 32 06 94
bart.crols@iai.nl

iai industrial systems

De Run 5406, 5504 DE Veldhoven, The Netherlands
P.O. Box 200, 5500 AE Veldhoven, The Netherlands
T +31 (0)40 254 24 45, F +31 (0)40 254 56 35
www.iai.nl


Hassan Mokdad
CEO, Inkript Technologies

Inkript

hmokdad@inkript.com

www.inkript.com

Farra Bldg., 2nd Floor
Bliss Str., Ras Beirut

Postal Code 2035 6707
Beirut, Lebanon

T. +961 1 370 888
F. +961 1 370 886

KEYNECTIS

Protecting Your Identity
Protecting Your Freedom

11-13, rue René Jacques
92131 Issy-les-Moulineaux Cedex – France

T. +33 (0)1 55 64 22 00
F. +33 (0)1 55 64 22 01

info@keynectis.com
www.keynectis.com

Luminescence International Ltd
The Fairway
Bush Fair
Harlow
CM18 6NG

Tel: 01279 456400
Fax: 01279 421142
www.luminescence.co.uk

LUMINESCENCE

Security Inks for Stitching Treads, Passports and ID Cards
The Original Security Inks Solutions

INNOVATIVE MACHINERY SOLUTIONS SINCE [illegible]

MELZER®

Bernd Brunken
Marketing & Sales Manager

MELZER maschinenbau GmbH
Ruhrstr. 51–55
58332 Schwelm/Germany
www.melzergmbh.com

Phone +49 (0)2336/9292-80
Fax +49 (0)2336/9292-85
E-Mail
bernd.brunken@melzergmbh.com

Mühlbauer
High Tech International

Your turnkey solution provider to realize Government ID projects
More than 30 years of experience and a constant development of highly efficient quality products

Mühlbauer INC. USA
226 Pickett's Line
Newport News, VA 23603-1366
Ms. Heike Davis, Sales Manager

Phone: 757 947 2823
Mobile: 757 876 6070
Fax: 757 947 2930
Mail: heike.davis@muhlbauer.com
info@muhlbauer.com

SECURITY ID DOCUMENTS IT MANAGEMENT CARDS SUPPORT DESIGN ENROLLMENT PERSONALISATION IT INFRASTRUCTURE BUILDING SURVEILLANCE INTERNATIONAL STANDARDS MAILING IDENTITY WORKFLOW ARTWORK EFFICIENCY PROCUREMENT

www.muhlbauer.com

Tel: +971 4 3669520
Fax: +971 4 3625355
Mobile: +971 50 6258030
mahmoud.musbah@omnix.ae

Office No. 229, Building No. 7
Media City, P.O.Box: 50999
Dubai, United Arab Emirates

Mahmoud Musbah
Vice President
Public Services Solutions

omnix
International LLC.

OPTAGLIO®
OPTICAL MICROSTRUCTURE TECHNOLOGIES

Optaglio s.r.o.
Technology Park Řež,
Hlavní 326, 250 68 Husinec-Řež,
Czech Republic

T +420 220 941 075
F +420 220 941 077
E obchod@optaglio.cz
W www.optaglio.cz

Trust your eyes

Thanks to the KINEGRAM®, the authenticity of government documents can be checked by the naked eye.

www.kinegram.com

KINEGRAM

OVD Kinegram is a member of the KURZ Group

ruhlamat
solutions for your needs.

Your professional engineering
and machine building partner.

- Smart card solutions
- (e-) Passport solutions
- Inlay / RFID solutions
- Module solutions

ruhlamat GmbH
Sonnenacker 2
99819 Marksuhl/Germany

☎ +49 36925 929 - 0
🗋 +49 36925 929 - 111
@ info@ruhlamat.de
🌐 www.ruhlamat.com

Visit them at www.icao.int/mrtdc

SAFELAYER

eGovernment Solutions: Citizen ID & ePassport & Government PKI

Safelayer Secure Communications S.A.
World Trade Center (Edif. Sud - 4ª Planta) Moll de Barcelona s/n 08039
Barcelona (Spain)
Telephone: +34 917 080 480 E-mail: sflyr@safelayer.com
www.safelayer.com

SICPA
ENABLING TRUST

THE COMPLETE SOLUTION
FOR SECURING VARIABLE DATA

www.sicpa.com

Pandelis Papadimitriou
Sales Director Value Document Inks
pandelis.papadimitriou@sicpa.com

Smart Cube

PASSPORT
NATIONAL ID
INTEGRATOR
FINANCE

Tel: +962 6 460 2000
Fax: +962 6 460 2010
info@smartcube.co

www.smartcube.co

SMARTRAC

Martin Kuschewski
ppa., Dipl.-Ing.
Head of Business Unit eID

SMARTRAC N.V.
Strawinskylaan 851
1077 XX Amsterdam, The Netherlands
Phone +49 351 88 960 45
Fax +49 351 88 960 11
e-id@smartrac-group.com
www.smartrac-group.com

Decades of innovation and experience
Identity documents, Swiss made

www.trueb.ch

TRÜB
SWITZERLAND

Trüb AG
Hintere Bahnhofstrasse 12
CH 5001 Aarau

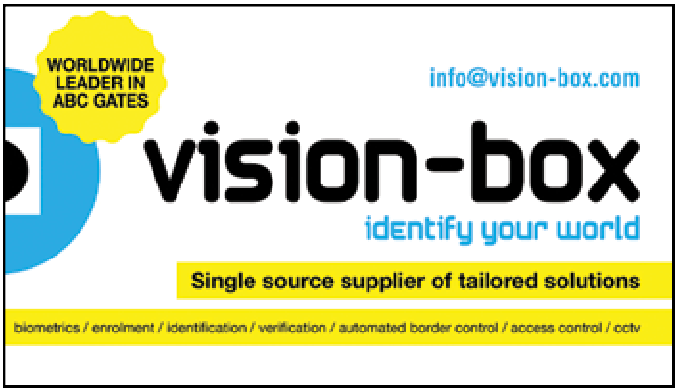
u-nica® global security solutions

Stephan D. Hofstetter
Managing Director
Government

U-NICA Security AG
Industriestrasse 4
CH-7208 Malans
Switzerland

Mobile: +41 79 641 11 24
Direct: +41 41 919 99 23
E-Mail: stephan.hofstetter@u-nica.com
Web: www.u-nica.com

Phone: +41 41 919 99 00
Fax: +41 41 919 99 49



WORLDWIDE LEADER IN ABC GATES

info@vision-box.com

vision-box
identify your world

Single source supplier of tailored solutions

biometrics / enrolment / identification / verification / automated border control / access control / cctv

WORLDREACH software

VISA & OVERSEAS PASSPORT ENROLMENT & ENTITLEMENT SPECIALISTS

Mark Stoochnoff
GLOBAL, Business Development & Sales
mark.stoochnoff@worldreach.com
cell: +1-613-867-9452

Hugo Guardado
LATIN AMERICA, Business Development & Sales
hugo.guardado@worldreach.com
cell: +1-613-867-9452

FROM THE NANSEN PASSPORT TO eMRCTDs

ALEXANDER BECK
is a Senior Legal Officer in the Protection Policy and Legal Advice Section of the Division of International Protection at the United Nations High Commissioner for Refugees. He represents UNHCR in the ICBWG of the TAG/MRTD.

Readers of the *MRTD Report* are all too familiar with the panoply of travel documents: ordinary passports, diplomatic and service passports, alien passports, identity cards and even emergency travel documents. They may be less familiar with travel documents for refugees and stateless persons known as Convention Travel Documents (CTDs).

Alexander Beck, Senior Legal Officer in the Division of International Protection at the United Nations High Commissioner for Refugees, provides an overview of the historical development of travel documents for refugees and stateless persons—from the Nansen Passport to electronic Machine Readable Convention Travel Documents (eMRCTDs).

Normally, persons with one or more nationalities can request a national passport from the designated issuing authorities whether they reside in their country of origin or abroad. In the latter case, embassies or consulates can usually issue passports. By definition, refugees have a well-founded fear of being persecuted as they are outside the country of their nationality and unable or unwilling to avail themselves of that country's protection (Article 1 of the 1951 Refugee Convention). In other words, because of a serious rupture between the citizen and his/her country of origin, refugees cannot be expected to approach the authorities of their country of origin to request a passport. Even more obvious is the case of stateless persons who are not considered nationals by any State under its laws (Article 1 of the 1954 Statelessness Convention) and hence are unable to obtain a national passport.

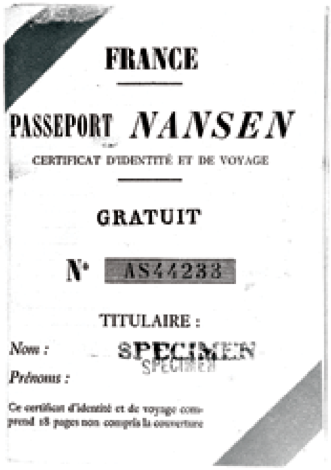
In short, refugees and stateless persons have no country to turn to in order to obtain a national passport. However, travel documents may be crucial for them to secure better protection, to reunite with family members, to access adequate medical treatment, education, employment or to benefit from resettlement. This is not a new phenomenon. Two converging historical developments, namely, the growing importance of passports since the early part of the 20th century and a number of—what we would call today—international or non-international armed conflicts producing large numbers of refugees and stateless persons called for an international response in the years after the First World War.

THE NANSEN PASSPORT, A HISTORY OF 90 YEARS

In 1921, Dr. Fridtjof Nansen, the Norwegian explorer and the League of Nations' first High Commissioner for Refugees, was tasked to find solutions for the massive outflow of Russian refugees following the Russian Revolution. For most of them, return and repatriation to Russia was prohibited following a 1921 Russian decree. This decree revoked Soviet citizenship for those who had resided abroad for more than five years and for those who had left Russia after November 1917 without permission. It was estimated that approximately 200,000 Russian refugees were in dire circumstances. With no valid passports, they had difficulty working in the country of first refuge and/or could not move to another country in search of protection.

In July 1922, the League of Nations convened an intergovernmental conference, which adopted the 'Arrangement with regard to the Issue of Certificates of Identity to Russian Refugees'. It was the birth of the Nansen Passport. Because of its immediate success, the Nansen Passport system was extended to Armenians in 1924 following the Greco-Turkish

war and again to Turkish, Assyrian, Assyro-Chaldean and assimilated refugees in 1928. Then, in 1933, Article 2 of the first Convention Relating to the Status of Refugees featured travel documents prominently: 'Each Contracting Party undertakes to issue Nansen certificates, valid for not less than one year, to refugees residing regularly in its territory (…)'. But not many countries signed this treaty.


FRANCE

PASSEPORT NANSEN

CERTIFICAT D'IDENTITÉ ET DE VOYAGE

GRATUIT

N° AS44233

TITULAIRE :

Nom : SPECIMEN

Prénoms :

Ce certificat d'identité et de voyage comprend 18 pages non compris la couverture

The Nansen Passport.

During the subsequent German refugee crisis, more specific agreements on refugees from Germany (1936) as well as the Saarland (1935), Austria (1938) and Czechoslovakia (1939) were negotiated, each providing for the issuance of identity certificates. The Nansen Passport system had become a standard feature of international efforts to protect refugees. After the Second World War, the 'Agreement Relating to the Issue of a Travel Document to Refugees who are the Concern of the Intergovernmental Committee on Refugees' of 1946 introduced the first travel document for refugees in book form. The provisions of this agreement largely determined what became the Schedule and Specimen to the 1951 Refugee Convention and the 1954 Statelessness Convention.

CHARACTERISTICS OF THE NANSEN PASSPORT

The original Nansen Passport consisted of a single sheet of paper. It was issued annually by the authorities of host countries and extended as required. It certified the status of the holder and granted rights (generally as 'other aliens') in the host country and freedom of international travel to other countries that accepted it. There was an important shortcoming however. The grant of the certificate did not in any way imply the refugee's right to return to the State in which he/she had obtained the certificate without the special authorization of that State. The problem was quickly recognized and the 1926 'Arrangement Relating to the Issue of Identity Certificates to Russian and Armenian Refugees' approved the principle of affixing return visas on identity certificates for refugees in order to facilitate their freedom of movement. This was an important amendment as many States were reluctant to admit refugees who they could not send back to their first host country if their stay became undesirable.

The 'Identity Certificate for Refugees Coming from Germany' was also issued on a single sheet of paper. The accompanying text stated:

> The present certificate is issued for the sole purpose of providing refugees from Germany with identity papers to take the place of a passport. It is without prejudice to and in no way affects the holder's nationality. On the expiration of its validity, the present certificate must be returned to the issuing authority. (….) Failing express provision to the contrary, the present certificate entitles its holder to return to the country by which it was issued during the period for which it is valid. It shall cease to be valid if the holder enters German territory.

As mentioned above, the Intergovernmental Conference on the Adoption of a Travel Document for Refugees held in London, 8-15 October 1946, marked an important shift in the history of travel documents for refugees. Besides the Agreement of 15 October 1946, the Conference, considering it highly desirable to achieve complete uniformity in the system of travel documents for refugees, recommended that all appropriate steps be taken to ensure the adoption of one single travel document for all refugees.

The Specimen travel document clarified that the document would be in booklet form (approximately 15 cm x 10 cm) and total 32 pages. On the top left side of the cover, there were two diagonal black stripes and the title, 'Travel Document (Agreement of 15th October 1946)'. A photograph of the holder and the stamp of the issuing authority were to be inserted. Children accompanying the holder could be mentioned and there was space for extensions and visas.

CTDS PURSUANT TO MODERN REFUGEE AND STATELESSNESS INSTRUMENTS

The 1951 Refugee Convention combines and consolidates the earlier Refugee Conventions and the 1946 Agreement on travel documents. While it did not introduce an entirely new travel document regime—the provisions of the 1946 Agreement were almost literally transposed into the Schedule to the Convention and its Specimen—it broadened the scope of application to all categories of refugees. Limited to events occurring before 1951, the 1951 Refugee Convention eventually became the modern refugee protection instrument with the adoption of the 1967 Protocol relating to the Status of Refugees.

More of a novelty was the adoption of the first universal instrument specifically dealing with the status of stateless persons, the 1954 Statelessness Convention, complemented in 1961 by a Convention on the Reduction of Statelessness. The travel document regime of the 1954 Convention is essentially the same as for refugees. Just as refugees, stateless persons have a right to a CTD with virtually identical features as the CTD for refugees.

Compared with the earlier instruments, the 1951 and 1954 Conventions had much more success among States. The Refugee Convention is close to being universally recognized. Some elements are also customary international law. The CTD regime, as developed in 1946 with its international legal basis in the 1951 and 1954 Conventions, has proven to be solid and long lasting. This does not mean there were, or are, no problems and difficulties.

THE ROLE OF UNHCR AND ITS EXECUTIVE COMMITTEE

In 1950, the United Nations General Assembly established the Office of the United Nations High Commissioner for Refugees to provide international protection to refugees and seek durable solutions for them. UNHCR is also responsible for supervising the implementation

German eMRCTDs.

of international instruments for the protection of refugees and stateless persons, including the provisions on travel documents.

Starting in the 1960s and 1970s and continuing until today, certain States do not make the necessary technical and administrative arrangements to enable the issuance of CTDs. Moreover, some States have not even set up formal procedures for determining refugee status, which causes entitlement problems. Based on its mandate, UNHCR started assisting States to remedy both issues. Firstly, it sometimes carries out status determination itself—based on agreements with host governments—and, secondly, it printed and provided governments with blank CTD booklets in different languages that governments could personalize and issue. Initially the intention was for UNHCR to assist those States, particularly in the developing world, which had recently become parties to the Convention and/or Protocol. However, this practice persists even today in more than 40 countries.

In the 1970s and 1980s, the Executive Committee of the High Commissioner's Programme considered the issue of CTDs and, on two occasions, urged all States parties to the 1951 Convention and/or the 1967 Protocol to take appropriate legislative or administrative measures to issue to all refugees, lawfully staying in their territory and who wish to travel, travel documents as provided for in the 1951 Convention (Article 28, Schedule and Annex). It also expressed appreciation for the various types of assistance the High Commissioner provides governments with respect to the issue of travel documents for refugees.

A positive consequence of UNHCR's assistance to States in providing the blank booklets was the model character this version of the CTD gained. At an early stage in the activities of UNHCR, it was thus concluded that the CTD would be as uniform as possible—not only as regards the text, which is prescribed in the Annex, but also with respect to colour, type of cover, format and printing.

For this purpose, UNHCR, in consultation with governments, produced a model document in booklet form with a blue cover and two black diagonal stripes that resembled the Specimen of the 1951 Convention (and the earlier 1946 Agreement). The High Commissioner's Advisory Committee on Refugees (predecessor to the present Executive Committee) recommended that governments issue their CTD in conformity with the model prepared by UNHCR. The majority of States, which issue the document, have adopted this model with the result that the blue CTD has become universally known and accepted even by non-Contracting Parties to the Conventions. No blank CTD booklets for stateless persons were produced.

THE NEW CHALLENGE OF MRCTDS

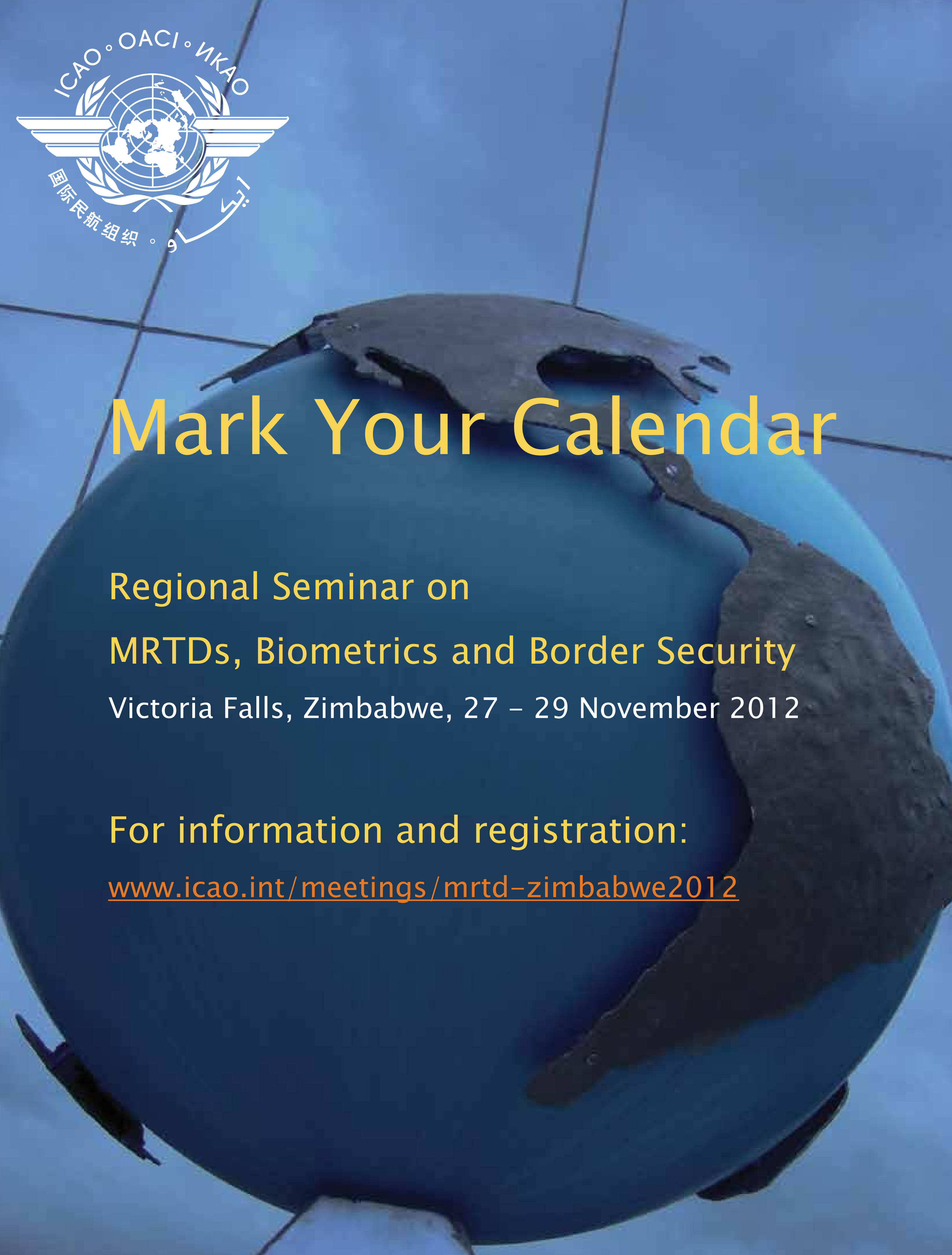
While the challenge of full implementation persists, the latest challenge to the CTD regime is the development of international Standards for Machine Readable Travel Documents (MRTDs) by ICAO. On the one hand, this development furthers the aim of a uniform CTD because of increased security Standards and mutual recognition and trust that ultimately helps the ability of refugees and stateless persons to travel. On the other hand, it highlights the implementation problem—for decades remedied by the provision of blank books by UNHCR to certain countries. However, this stop-gap practice will necessarily come to an end as the November 2015 deadline approaches.

A number of States have introduced MRCTDs for refugees and some of them have even moved or are in the process of moving to biometric CTDs (eMRCTDs), even though this is not required by ICAO. However, more than 80 of the 148 Contracting Parties to the 1951 Refugee Convention and/or the 1967 Protocol do not produce and issue their own CTD—let alone MRCTD. Therefore, insofar as countries of destination or transit no longer recognize non-machine readable CTDs after November 2015, refugees hosted by these countries risk being deprived of their right to travel. With regard to stateless persons, the situation is not much better with 40 Contracting States of the 1954 Convention not issuing CTDs.

To close this important implementation gap, all the stakeholders involved, that is, the Contracting Parties, UNHCR, ICAO, other relevant international and regional organizations and vendors from the private sector will need to assume their respective roles and responsibilities.

The Nansen Passport, namely the CTDs, is one of the most formidable inventions and achievements in the history of international protection of refugees and stateless persons. The move to MRCTDs or even eMRCTDs should strengthen, not weaken, its accessibility and value for the individuals who need them.

For the past few years, UNHCR has worked with ICAO, in particular, with its Implementation and Capacity Building Working Group (ICBWG) of the TAG/MRTD to find solutions to these implementation gaps. One concrete outcome of this cooperation is a forthcoming Guide on MRCTDs. ■



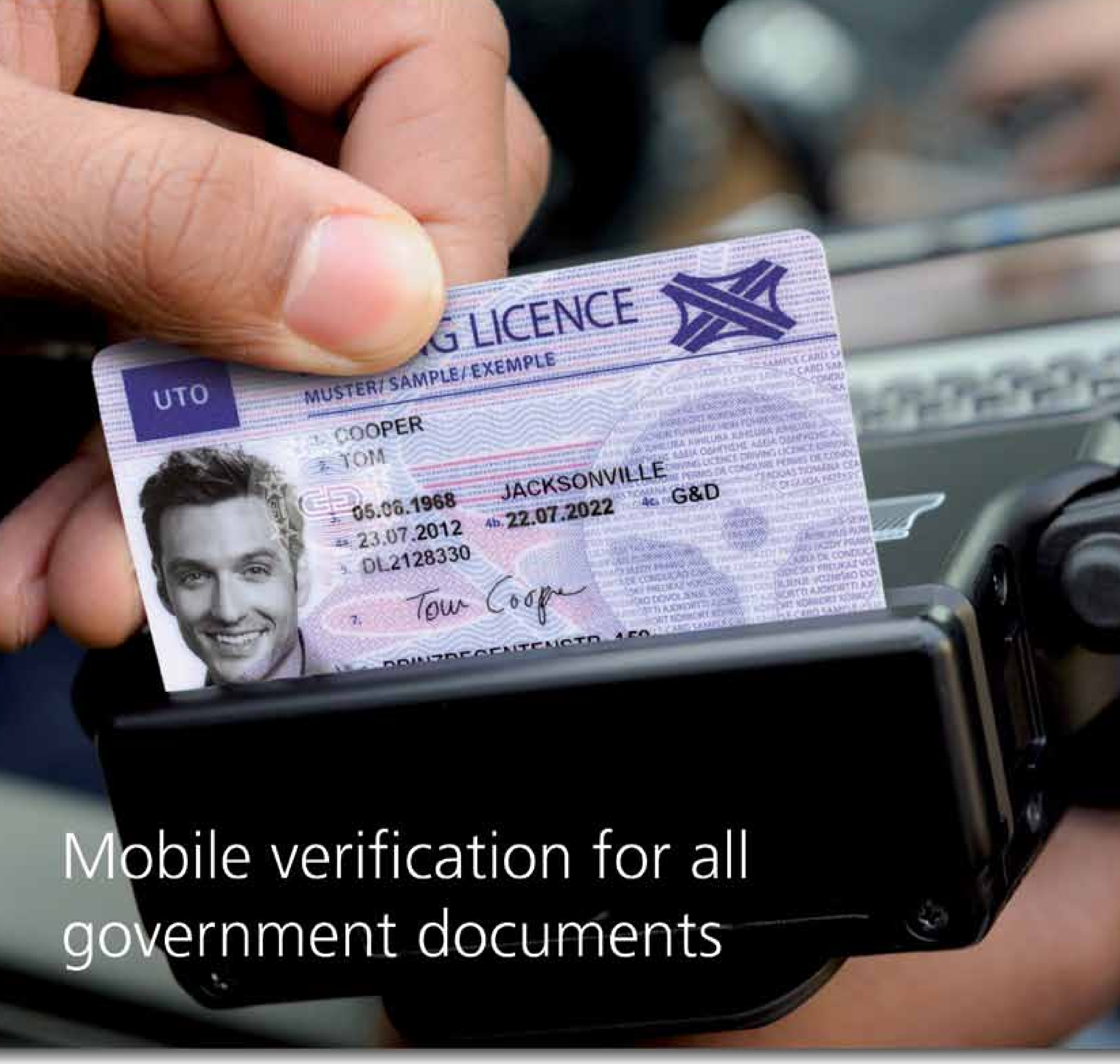
Mark Your Calendar

Regional Seminar on MRTDs, Biometrics and Border Security

Victoria Falls, Zimbabwe, 27 – 29 November 2012

For information and registration:

www.icao.int/meetings/mrtd-zimbabwe2012


G LICENCE
MUSTER/ SAMPLE/ EXEMPLE
UTO
1. COOPER
2. TOM
3. 05.06.1968 JACKSONVILLE
4a. 23.07.2012 4b. 22.07.2022 4c. G&D
5. DL2128330
7. Tom Cooper
Mobile verification for all
government documents