ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Vol. 7, No. 2 – Summer 2012

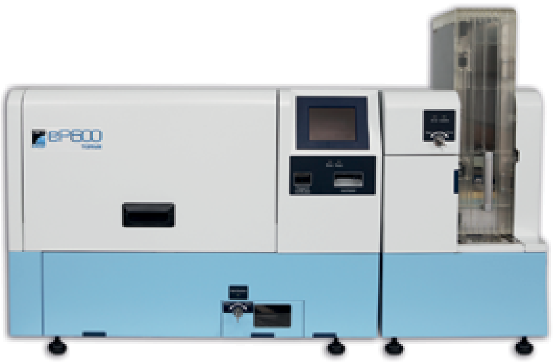
MRTD REPORT

GLOBAL

STANDARDIZATION

The global implementation of MRTDs can be achieved through extensive consultation, agreement and standardization among Member States.

In this issue:


eP600

ICAO MRTD REPORT
VOLUME 7, NUMBER 2, 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

Content Development
KDH Communications
Senior 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

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

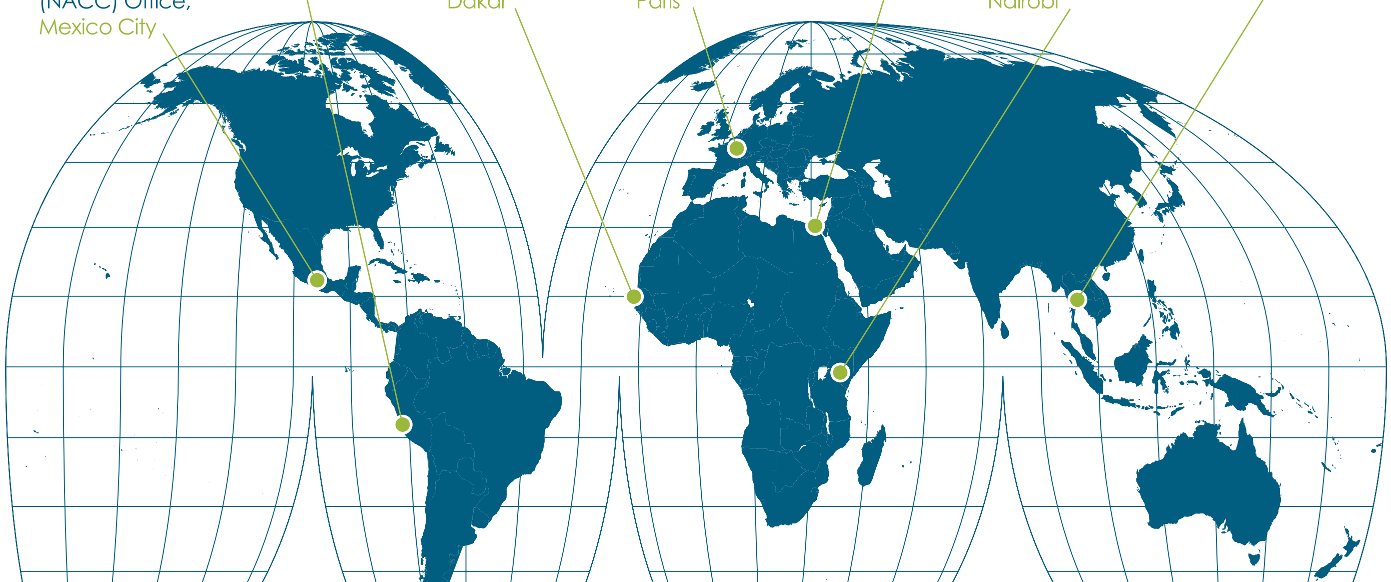
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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

MRTD SPECIFICATIONS: ONGOING DEVELOPMENT AND ADVOCACY EFFORTS

The silicon chip is changing the world. Globalization, increasing pace, ease of travel continue reshaping border controls and travel documents. With increasing speed, the latest technologies and solutions need to be incorporated into Document 9303. Compliance with ICAO MRTD Standards and specifications is essential to maximizing security and facilitation benefits for States and their citizens.

ICAO has been updating and streamlining the structure of Doc 9303 and enhancing its contents with the inclusion of up-to-date Technical Reports and the current Supplement. Ongoing activities include updating the Supplement, incorporating Technical Reports and re-structuring Doc 9303. The new edition of Doc 9303 is expected to be ready for translation and publication in the second half of 2013.

The Technical Reports and Supplement present current state-of-the art developments in MRTD specifications. They have been designed by leading experts of the Technical Advisory Group (TAG/MRTD) and its working groups. This edition of the magazine provides an overview of the latest Technical Reports. They all are available on the website of the ICAO MRTD Programme.

Having updated and relevant MRTD specifications is vital—but not enough. Advocacy and capacity-building efforts continue, enhancing government officials' knowledge of how to interpret and apply ICAO guidance materials in practice. The ongoing Canada funded project in the Americas marches on. Recent project activities in Panama, Mexico and the Dominican Republic are presented to readers in this issue.

The ICAO Regional Seminar on MRTDs took place in Rio de Janeiro. It was the second seminar in the Americas region. The first one took place in Montevideo, Uruguay, a couple of years ago. The focus of the Rio Regional Seminar was electronic passports. It examined current and emerging ICAO MRTD specifications, identity management best practices and related border security issues—with particular reference to the Americas region. The programme addressed in detail the advantages and challenges of using biometric data in travel documents, points of importance with regard to implementing electronic passports, technical specifications, procurement issues, reading ePassports at borders and the role of the ICAO Public Key Directory (PKD) in achieving robust global security. Insights generated by Seminar discussions are shared in this issue.

These capacity-building events provided an excellent opportunity to share lessons learned, challenges that were met and solutions found in implementing MRTD and border control projects. This knowledge cannot be found in books or scholarly magazines and is the major strength of MRTD regional events. Learning from each other, in an open and critical manner, remains a key component to the success of our joint global efforts. ■

WHERE WOULD THE INDUSTRY BE WITHOUT CONVENTIONS AND STANDARDS?

MICHAEL HEGENBARTH
Senior Director of Standardization and Consulting at Bundesdruckerei GmbH, is one of the original developers of communication security techniques based in chip cards used in digital signature applications. Chairman and delegate since 1986 to various international card standardization groups in ISO/IEC, CEN and ETSI, he has chaired the ISO/IEC working group SC17/WG8 for contactless interfaces since 1990 where he initiated the ISO/IEC 14443 project in 1991. In 1997, he invented the idea of combining mobile phones with contactless interface known under the term NFC since 2002. He has also been chairman of Germany's standardization committee for cards and personal identification since 1993.

What must be done to ensure travellers around the globe can prove their identities safely and reliably? Which organizations ensure that an identification (ID) document is authentic and belongs to the holder? What concepts have already been developed for the utilization of electronic identities and what developments are still in progress?

The subject of standardization plays a central role when designing the technical features of modern ID documents that safeguard identities. In this article, the first of a series of articles on this subject, Michael Hegenbarth, Senior Director of Standardization and Consulting at Bundesdruckerei GmbH, throws a little more light on various aspects of the on-going work taking place in international standardization and in the field of high-security research. Using electronic ID documents as an example, he explains how new standards are developed and the organizations involved in formulating and implementing them.

The technical design of ID documents must conform to precise rules and standards developed and jointly adopted by national and international organizations, such as the International Standardization Organizati on (ISO) and the International Electrotechnical Commission (IEC). ISO Working Groups have, for example, developed worldwide standards for machine readable travel documents and contactless eID chip cards that transfer data via high-frequency magnetic fields.

These standardization bodies publish their recommendations for implementation of new standards once all stakeholders have considered their national security interests and consensus has been reached. For a more detailed explanation, see the sidebar, HOW INTERNATIONAL STANDARDS EVOLVE.

MUTUAL AGREEMENT IS ACHIEVED BY BALANCING INTERESTS

However, multinational agreements reflecting the accepted standards are needed. ID documents, which are used for identification purposes not only in their country of origin, but also in other countries, are a classic example of the importance of these agreements. It is impossible to check the authenticity of these documents and correlate the personal data with a particular individual unless adherence to clearly defined technology and security standards is guaranteed.

In addition, electronic ID documents are being increasingly improved not only to detect optical but also biometric features. At the same time, the design of ID documents is governed by country-specific legislation. This means compatibility criteria must be planned at a multinational 'meta-level' before being integrated into the ensuing decision-making and production processes. This is no trivial task since the organization of national and international standardization activities is correspondingly diversified, as indicated in the sidebar, ORGANIZATIONS RESPONSIBLE FOR DEVELOPMENT OF NEW ID DOCUMENT STANDARDS.

AN EXAMPLE: THE INTRODUCTION OF ELECTRONIC PASSPORTS

One of the most extensive and significant interoperability projects of the past decade was the introduction of electronic passports. In 2001, a total of 189 countries gave ICAO the mandate to compile and recommend new Standards for machine readable travel documents, which necessitated the re-organization of production processes and national and international security structures. In Europe, the ICAO recommendations—in particular the storage of biometric data—were set out in European Union Regulation 2252/2004. In this new regulation, EU Member States went considerably further than just implementing ICAO's minimum requirements. Access to digitized passport photos has to be protected by Basic Access Control (BAC) and stored digitized fingerprints by Extended Access Control (EAC) mechanisms, which are specified in technical guidelines issued by the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*).

At the same time, EU Member States and the signatory States of the Schengen Agreement, which created Europe's borderless Schengen Area, continually strive to improve interoperability standards for European travel documents (including Article 6 Technical Sub Group – EAC Specification).

For instance, a study was conducted of 'Simple Procedures Online for Cross-Border Services' or SPOCS to analyze the required components for EAC public key infrastructure management and the results were set out in European Standard CSN 36 9791.

HOW INTERNATIONAL STANDARDS EVOLVE

At the International Standardization Organization (ISO), a globally active institution that issues recommendations for many national standardization projects, every project has to pass through at least five consecutive process steps.

Preliminary Work Item (PWI)
At the preliminary stage, a new standardization project is defined and its distinction from any similar products and/or technologies is established.

New Work Item Proposal (NP) / Working Draft (WD)
To ensure acceptance and future usability of a new standard, an existing group is consulted or a new group is founded, which includes representatives of all stakeholders (scientists, manufacturers, users, politically responsible institutions). This group outlines the standardization project and submits it to ISO.

Committee Draft (CD)
The new standard's first version, the Committee Draft (CD), is compiled and then distributed to international experts for comments and discussion.

Draft International Standard (DIS)
All comments are reviewed and, where applicable, integrated into new draft versions until the draft standard reaches a status (DIS) acceptable to all involved.

International Standard (IS)
The outcome of the entire procedure is a new standard documented in the manner specified by the respective organization and then published.

Review
The contents of a standard are reviewed at regular intervals and the standard may then be revised or even replaced by a new one after a 'withdrawal'.

Leadership and Vision in Global Civil Aviation

www.icao.int

The International Civil Aviation Organization

COMPATIBLE SYSTEMS ENABLE COOPERATION

Similar consultation and agreement structures apply as well to national identification documents such as the new German ID card, the equivalent of a passport within the Schengen Area, which is comprised of 31 European countries. Important input came from international ISO/IEC standards and especially from the Lisbon Strategy passed by all European heads of state and governments in March 2000. As part of this strategy, measures to promote a common scientific and economic area were implemented in Pan-European projects such as STORK (Secure Identity Across Borders Linked) and followed up by international standardization organizations.

To enable use of electronic identities across borders, various national ID systems and data protection and privacy laws, which differ from one country to the next, must be considered as well as factors such as whether to manage data administration centrally or decentrally. In its European Digital Agenda, the European Commission suggested some initial approaches to resolving these issues. However, in order for the EU to be opened up digitally with high-speed networks and interoperable applications, different models such as the middleware approach ('Bürgerkarte' or citizen ID card) favoured by Austria and Germany or concepts

ORGANIZATIONS RESPONSIBLE FOR DEVELOPMENT OF NEW ID DOCUMENT STANDARDS

International Civil Aviation Organization (ICAO), Montreal
Responsible for worldwide development of Machine Readable Travel Documents (MRTDs) since 1989.

International Organization for Standardization (ISO), Geneva
The international association of all standardization bodies worldwide.

International Electrotechnical Commission (IEC), Geneva
The international standardization organization dealing with electrical engineering and electronics. Information technology standards are developed by Joint Technical Committee 1 (ISO/IEC JTC1) set up by ISO and IEC. The subordinate standardization committee SC 17 deals with the standardization of cards and means of personal identification. Several Working Groups (WGs) are in this subcommittee. WG 3 develops standards relating to means of identification for and at the request of ICAO. Standards for contactless data transmission, such as for use in chip cards and ID documents, are developed in WG 8.

Comité Européen de Normalisation (CEN), Brussels
European Committee for Standardisation. The CEN's technical committee CEN/TC 224 develops standards for personal identification, electronic signature and cards and their related systems and operations.

Article 6 Technical Sub Group, Brussels
EU Commission technical working group ensures interoperability of European travel documents.

like the Pan-European Proxy Services (PEPS) have to be harmonized and their respective advantages and disadvantages investigated.

STANDARDS FOR A NETWORKED WORLD

The examples outlined in the sidebar, eID CARDS STANDARDS WITHIN EUROPE, clearly illustrate how complicated the work, consultation and agreement processes can be leading up to publication of a new standard. In addition, a distinction has to be made on whether only national security interests are affected or international ones as well. In the case of products and applications valid for use across national borders, the development of new ISO/IEC standards is largely driven by recommendations issued by the Joint Technical Committee (JTC1). Where no corresponding ISO/IEC standards are available, the recommendations of the European Committee for Standardisation (CEN), which has worked in close cooperation with the ISO since 1991, apply within the EU. The decision to use ISO/IEC or CEN standards or develop country-specific provisions is usually left up to the respective country's standardization organizations.

INTERDISCIPLINARY COOPERATION

Along with political decision-makers, many experts from the fields of commerce and science are actively promoting continued development of existing technology and security standards within these complex organizational structures. Experts especially in the international high-security sector are being encouraged to contribute to optimization of existing

> It is impossible to check the authenticity of documents and personal data… unless adherence to clearly defined technology and security standards is guaranteed.

eID CARDS STANDARDS WITHIN EUROPE

Country	Interface used	Biometric security features	eID function	eGovernment applications	eSignature function	Introduced in
Albania	Contact	X	X	X	X	2009
Austria	Contact	—	X	X	X	2009
Belgium	Contact	—	X	X	X	2004
Estonia	Contact	—	X	X	X	2002
Finland	Contact	—	X	X	X	1999
Georgia	Contactless	—	X	X	X	2011
Germany	Contactless	X	X	X	X	2010
Italy	Contact	X	X	X	X	2005
Liechtenstein	Contact	—	X	X	X	2009
Lithuania	Contact & contactless	X	X	X	X	2009
Monaco	Contact & contactless	X	X	—	—	2009
Netherlands	Contactless	X	—	—	—	2006
Portugal	Contact	X	X	X	X	2007
Serbia	Contact	X	X	X	X	2008
Spain	Contact	X	X	X	X	2006
Sweden	Contact & contactless	X	X	X	X	2005

standards by producing innovative technological approaches and concepts. Their input is welcomed in order to obtain as wide a spectrum of ideas and suggestions as possible. At the end of the long road that every standardization recommendation has to reach before approval, only those approaches which are acceptable to all involved and which gain broad consensus will become established and succeed.

LOOKING AHEAD

In upcoming issues of the MRTD Report, you'll journey through the world of international standardization. Further articles in this series will describe projects undertaken by international standardization experts such as the German ID card system as it stands roughly one year after introduction. Another article will take a look at state-of-the-art test methods for optimizing quality testing of OCR (optical character recognition) typefaces, an important feature of modern travel documents. The shape of things to come will be outlined in additional articles dealing with new display technologies and their application in future ID card designs and the planned harmonization of contactless chip card standards (ISO/IEC 14443) and mobile telephones in regard to the near field communication standard (ISO/IEC 18092). ■

IDENTITY VERIFICATION: THE IMPORTANCE OF ‘CONTEXT’ AND ‘CONTINUITY’ OF IDENTITY

ROSS GREENWOOD *is a consultant who advises agencies and vendors involved in passport issuance and civil registration, border control, biometrics and identity management. Until 2010, a senior executive in the Australian Passport Office, he was responsible for designing passports, applying biometrics in passport issuance and preventing, deterring and investigating passport fraud. He served as Australia's delegate to the ICAO TAG/MRTD and inaugural chairperson and member of ICAO's Public Key Directory Board. At the Australian Department of Immigration from 1977 to 2007, he held positions in border control and identity management roles and completed postings at Australian diplomatic missions in Turkey, Mauritius, Kenya, Syria and Hong Kong.*

Myths abound in today's challenging security environment. Identity verification is a critical initial step in the delivery of high-value services and in granting physical access to facilities and virtual access to sensitive and high-value information. A secure enrolment, the addition of physical or electronic security features to tokens and credentials and/or the introduction of automated biometric comparisons can assure identity verification are seductive propositions.

Sadly, there are no silver bullets in the complex system—subject to error and fraud—that is identity. Ross Greenwood, Principal of Identity Matters Consulting, and former TAG/MRTD member for Australia, highlights the importance of assessing ‘context’ and ‘continuity’ in identity verification and the critical role verification against highly transacted datasets plays in achieving this additional layer of assurance.

Identity matters. High-value goods and services are attractive targets for fraud. At the same time, managing the physical or virtual access of individuals is a foundation of security in both the public and private sectors.

IDENTITY SECURITY FUNDAMENTALS

Verifying the identity of individual people to a level of assurance appropriate to the credential being issued or the ‘access to’ or ‘value of’ the goods, services or entitlements being sought is a step common to many transactions. This is the case whether the transaction occurs online or in the real world and whether the citizen is transacting with governments or the private sector.

The fundamentals of assuring individual identity have remained constant and apply universally—both online[1], in the real world and in the public and private sectors. Identity is not constrained by national borders. The introduction into airline service of the Boeing 747 in the late 1970s made travel affordable to the masses. Now the Internet is transforming service delivery and retailing to give identity verification a new international dimension.

People seeking high-value access, goods, services or entitlements are invited to ‘claim’ an identity. It is up to the service provider to verify the claim by checks of:

- What they ‘have’, i.e., credentials and tokens with biographical and/or biometric matching the identity being claimed;
- What they ‘know’, i.e., verifiable information currently and/or previously associated with the identity being claimed; and
- Who they ‘are’, i.e., biometric identifiers.

The initial verification of a claim to an identity is often described as an ‘enrolment’. Client convenience, cost and privacy imperatives demand that after an identity is 'proved' through an enrolment process subsequent identity verification transactions must be as streamlined as practicable. This separation of the 'enrolment' and 'verification' tasks can be a useful simplification, for example, for business process and Information and Communications Technologies (ICT) systems design.

In fact the enrolment/verification construct is fundamentally flawed. The fundamental insight is that identity is a complex system, subject to error[2] and fraud in which claims to identity are made and tested and tokens issued and revoked—all for the purpose of allowing identities to transact economically and socially.

IDENTITY ATTRIBUTES, THE 'ASSOCIATION' CHALLENGE

Our biological identities are immutable and we are, in most important respects, unique as individuals.

However, our 'claim' to an identity is comprised of a set of identity and identity-related attributes that, when accepted, become associated with our identity rather than irrevocably being linked to our immutable selves. These identity attributes are most commonly biographic (name, date and place of birth, gender) but increasingly include biometric markers (face, fingerprints, iris, voice et al).

Whether biographic or biometric[3], these identity attributes are representative of but mutable from our biological identities and, as a result, they don't prove identity.

UNCERTAIN IDENTITY

The mutability of biographic identity markers' details is easy to accept:

- The name Mohamed is comprised of the Arabic equivalents of its four consonants but can be written more than 80 different ways in Latin script, once the vowels are added in transcription[4].
- Names can have shortened and lengthened forms, preferred spellings that differ from registration documents, a second given name may be used in preference to a first given name, etc.
- Dates of birth are subject to change (e.g., late registrations, transcription from different calendars).
- The same place of birth can be described in multiple different ways.
- Male and female are only the most common gender markers.

Biometric identity markers are also subject to variance and uncertainty:

- Every biometric enrolment has multiple qualitative dimensions regarding the circumstances of enrolment and the quality of the images or voiceprint captured[5].
- No biometric markers can be enrolled from birth[6]. All are absent in some people. All are subject to change due to accidents. Most degrade with age[7].

For convenience, a set of identity attributes, once accepted in an enrolment process are collated into credentials or tokens. Where the enrolment process is (relatively) strong[8] and the token is (relatively) secure[9] (e.g., as in national identity cards, passports and driver's licences), the set of identity attributes included in the token may be relied on for identity verification purposes. However, identity credentials are nothing more than a record of a prior enrolment of a set of identity attributes. *Identity credentials don't prove identity[10] (and reference to their underlying databases doesn't prove identity either[11]).*

Genuine identities have continuity so credentials and tokens issued in the past, successive enrolments and prior biometric information and transaction histories all have value in identity verification. But even if common identity attributes are able to be associated with successive claims to an identity over an extended period, this *continuity of identity is not proof of identity*.

If proof of identity means a 100% assurance that a set of identity attributes can be reliably associated with a biological entity then in fact *identity cannot be 'proved' at all.*

The discussion in the foregoing is intended to illustrate that verification of identity is inherently probabilistic[12]. While identity cannot be proved, we can reach a very high-level of assurance that a claim to a set of identity attributes may be accepted if that set of identity attributes matches or shares sufficient common elements with current and historical transactions and current and past credentials and enrolments.

Identity verification is the ability to associate identity and identity-related attributes claimed in previous enrolments and transactions with those being claimed in a current interaction. This process is complex and subject to variance, error and fraud.

Managing the association of identity and identity-related attributes is the key to identity verification.

THE IDENTITY PARADOX

When a customer seeks an identity-dependent service or entitlement and/or seeks identity-dependent access to a real or virtual environment, a determinative decision must be made—either yes or no. This is a commercial imperative from a service delivery efficiency and customer experience perspective that nevertheless carries identity verifications risks that cannot be fully mitigated. At the process level, this risk is hidden because the vast majority of identity-dependent transactions are concluded routinely with the claim to identity being accepted.

At the same time, the probabilistic nature of identity verification runs counter to our social instincts. As a species, humans have an exceptional ability to recognize people familiar

to them (and a poor much less well understood ability to distinguish people unknown to them)[13]. As social animals, we are hard-wired to add people to the set of 'known' people familiar to us. When was the last time you questioned the asserted identity of a stranger introduced to you?

Once an identity-dependent service or entitlement is delivered the *false* presumption is that the claim to identity has been conclusively determined. The identity paradox is that the probabilistic nature of identity verification remains hidden to the people delivering and managing identity-dependent services, even when the occasional error and fraud—its most obvious manifestation—is detected.

Identity verification means that a person's claim to a set of identity attributes can be accepted on this occasion to a sufficient level of confidence. Identity verification does not mean that the identity of a person has been conclusively determined. Understanding the identity paradox is the key to accepting that there can be no silver bullets in identity verification.

AN IDENTITY VERIFICATION MODEL

Identity verification can be described as the collection of identity and identity-related attributes for comparison with previously collected identity and identity-related attributes to check that the context and continuity of the claimed identity gives sufficient assurance for the current claim to an identity to be accepted. This model for identity verification is represented in tabular form in the sidebar, AN IDENTITY VERIFICATION MODEL.

Reflecting the complexity of the identity system, each step in identity verification has its challenges.

The collection of biographical identity attributes is time consuming. The collection of biometric identity attributes is in addition expensive and technically challenging. Not all biographic and biometric attributes are collected on every occasion to the same standards or in consistent formats. Streamlined reissuance processes mean that the more comprehensive initial enrolment is not repeated. As a result, in any identity system, the majority of historic identity enrolments have not been subject to the full range of internal controls and checks that may now be employed in first time issuance.

The collection of identity-related attributes is, in most cases, incidental to service delivery or enrolment. As a result, place and time information may be ambiguous, inconsistent or absent. Traditionally the strongest enrolments manage the transaction, place and time by requiring the person being enrolled to be present (e.g., the passport interview and live photo capture for driver's licences). Alternative models for online enrolment that have strong geospatial links and enable biometric capture are emerging. High-value identity credentials are high cost and, as a result, are only infrequently transacted—in Australia passports and driver's licences are typically issued for 10 years.

For many services, the collation of identity attributes to enable comparing the identity attribute data provided in support of the current identity claim with data supporting previous claims completes the identity verification. In these simple interfaces, the matching of biographic attributes in a current claim to those contained in a database or on a credential allows a service to be delivered. Discrepancies are treated as exceptions or excluded from receiving the identity-dependent access or service.

THE CASE FOR STREAMLINED RENEWAL PROCESSES

An identity verification process that relies on collection of identity attributes for simple comparison to a prior enrolment is suboptimal and can therefore be inappropriate for managing high-value identity-dependent access or transactions. Even the strongest enrolment processes are subject to error and fraud and even the most secure credentials can be compromised. For example, identity takeovers via 'tombstone fraud' or the exploitation of vulnerable identities will continue to result in genuine high-value identity credentials being obtained by fraudsters.

Of course, in general, it is true that comparison to a stronger enrolment (e.g., including an interview, biometric capture and database verification) will improve identity verification assurance. However because the high integrity identity enrolments undertaken by issuers of national identity cards, passports and driver's licences occur infrequently, they are generally poor indicators of the context and continuity of an identity.

The ICAO's Machine Readable Travel Document (MRTD) Technical Advisory Group (TAG) is developing guidelines for passport and civil registration authorities, which acknowledge the importance of social footprint checks[14]. In the United Kingdom, the passport issuance process for first time and high-risk applicants has since 2007 incorporated credit-related checks with a data aggregator to establish a social context[15]. Elsewhere, including in Australia, passport issuing agencies continue to establish a social context in more traditional ways—for example, by relying on address verification and checks of available public sector databases (e.g., the Electoral Roll). The issue of a national identity card, passport or driver's licence represents the best assessment of identity and entitlement than can be made at the time of issue. However, note that even if effective and comprehensive social footprint checks were used at identity card, passport and driver's licence issuance, reliance for identity verification on an identity document issued up to 10 years ago does little to confirm that the identity attributes associated with the claimed identity have been used consistently and continuously in the community in the intervening period.

AN IDENTITY VERIFICATION MODEL

STEP 1: COLLECT

Identity Attributes

- Biographic
  - Family name
  - Given name
  - Date of birth
  - Place of birth
  - Gender
  - Nationality
- Biometric
  - Face
  - Fingers
  - Iris
  - Voice

Identity-related Attributes

- Place
  - Address
  - Telephone no.
  - IP address
- Time
- Transactions

STEP 2: COLLATE

Associate attributes and compare to prior identity claims

STEP 3: ASSESS

1. Context of claim to identity?
   - Pattern analysis is transaction dependent
2. Continuity of claim to identity?
   - Frequency of token re-issue
   - Verification thresholds for transactions

In most developed countries, financial institutions have conducted identity verification as the initial step in checking the creditworthiness of their customers for many years. Over time, credit reporting agencies were created to provide this service to the financial industry. In the post 9/11 environment, the focus of identity verification extended from targeting organized crime to terrorism[16]. This extended focus led, inter alia, to analogous formal identity verification obligations being imposed on the telecommunications sector[17]. Associating transactions defined by place and time with a set of claimed identity and identity-related attributes can contribute to assessment of whether a credible context (i.e., social footprint) exists for the claim. Specialist data aggregators have emerged to meet this demand[18].

The key to scalable efficient, effective social footprint assessment is verification access to datasets that:

i. are transacted regularly and frequently;
ii. have explicit or implicit revalidation of identity or identity-related attributes (e.g., billing via a different communication channel to the one used to deliver the service);
iii. have extensive coverage;
iv. have a geospatial nexus to the service being delivered; and
v. incorporate time stamping features.

In addition to credit and other financial datasets[19], traditional utilities such as gas, water and electricity meet these tests well at the household level. Telecommunication utilities (voice and data) add a dynamic dimension to geospatial tagging and are more ubiquitous at the individual level[20]. Other datasets can complement results by extending scope of coverage. It is important to note that the identity verification value does not depend on disclosure of personal, sensitive or detailed transactional information since it is the pattern and existence of the transactions and their association with identity and identity-related attributes that confirm the social footprint.

The identity verification value of analyzing a pattern of current transactions can be further enhanced by historical searches and comparisons to establish continuity of identity. The assessment of continuity can be complemented by comparisons to historic (i.e., expired) tokens and credentials. The assurance provided by the continuity assessment then depends, inter alia, on the integrity and frequency of the reissuance processes of tokens and credentials and the integrity of the revalidation inherent in repeat transaction processes.

IMPLICATIONS FOR IDENTITY VERIFICATION PRACTICE

Systemic weaknesses remain in even the strongest national identity systems. For example, death records are unable to be matched to corresponding birth records to prevent identity takeover. This is because death and birth events can occur across civil registration jurisdictions as not all deaths are recorded and matching of birth and death records is not always straightforward—even in the relatively few jurisdictions with extant systems that attempt this task.

Collaboration and data exchange between the public sector agencies with civil registration responsibilities are essential for effective identity verification. However, while the public sector has the responsibility, capabilities and access to data to facilitate initial enrolments, in general, it has poor access to the transactional data that is critical to establishing context and continuity of identity. Typically data aggregators operating in the private sector have the capabilities and access to data that complements those in the public sector. Better private sector access to government identity datasets would improve identity verification in many countries. However, perhaps the greatest opportunities for improvement in identity verification

“Managing the association of identity and identity-related attributes is the key to identity verification.”

are for better use by both the private sector and public sector of the transactional datasets that are critical to assessing context and continuity of identity.

These opportunities are recognized by government. The Australian Attorney-General’s department acknowledged the importance to identity verification of public/private sector collaboration in the face of growth in online transactions in its 1 April 2010 response to the Australian National Audit Office’s Performance Audit of the National Identity Security Strategy:

> *“The expansion of the digital economy poses new challenges and opportunities for governments, particularly for citizen-centric, whole-of-government online service delivery. Australia’s federated system of identity credentials and the intersection of public and private sector management of identity also creates a greater need for partnerships with business and the community to achieve the overarching goal of the Strategy.”*[21]

CONCLUSION

There are no silver bullets in identity management. Improved enrolment practice is necessary but insufficient. Improved document security is necessary but insufficient. Improved application of biometric comparisons is necessary but insufficient. Improved verification to establish context and continuity of identity is necessary but insufficient. At the same time, the community needs to be assured that achieving better identity security will not come at the cost of efficient delivery of services, the customer experience and the right to privacy. Progress in all areas is required to assure identity security from the emerging threats of the Information Age.

Reprinted by permission of the publisher: Identity Verification: The Importance of ‘Context’ and ‘Continuity’ by Ross Greenwood, which originally appeared in the *Keesing Journal of Documents & Identity, Annual Report 2011-2012,* published by Keesing Reference Systems B.V. Copyright 2012. All rights reserved.

FOOTNOTES

[1] See: paragraph 2 of Foreword at page 3 of http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument

[2] See: http://www.nap.edu/openbook.php?record_id=12720&page=1 and http://www.economist.com/blogs/babbage/2011/01/secure_documents&fsrc=nwl

[3] See: http://www.economist.com/blogs/babbage/2010/10/biometrics and http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=12720 and http://www.prnewswire.com/news-releases/ibia-statement-regarding-the-release-of-the-national-research-council-report---biometric-recognition--challenges-and-opportunities-104577739.html and http://www.theregister.co.uk/2009/08/14/biometric_id_delusion/page2.html

[4] For other foreign name issues that impact on identity verification, see: http://www.centrelink.gov.au/internet/internet.nsf/publications/enp.htm

[5] See: e.g., http://www.nap.edu/openbook.php?record_id=12720&page=3 and http://www.dnaindia.com/scitech/report_study-reveals-likelihood-of-human-error-when-dealing-with-fingerprints_1542559

[6] Fingerprints and facial images are generally considered stable after puberty. Iris images may be stable somewhat earlier, but not from birth.

[7] Face and fingerprints are widely acknowledged to change over time in a variety of ways that impact matching performance. Iris has traditionally been regarded as more stable but see: http://nd.edu/~kwb/FenkerBowyerWACV_2011.pdf

[8] Illegal immigrants in the US obtain driver's licences from Washington State illegally by pretending to be Washington residents. See: http://www.foxnews.com/politics/2011/02/17/states-revise-rules-drivers-licenses-illegal-immigrants-national-id-approaches/ et al.

[9] High-quality 'novelty' (i.e., fraudulent) driver's licences are readily obtainable online. See: http://identity-solution.com/ and http://www.middletownjournal.com/news/middletown-news/high-quality-fake-ids-seized-1224886.html

[10] E.g., for genuine US passports issued in false names in 2010 GAO audit, see: http://www.federalnewsradio.com/index.php?nid=35&sid=2015164. For UK document fraud factory bust, see: http://www.ukba.homeoffice.gov.uk/sitecontent/newsarticles/2011/may/34Fake-ID-Factory-Lewisham

[11] The US experience with e-Verify, the system for checking the employment rights of foreigners, is instructive. See: http://www.migrationpolicy.org/news/2009_7_20.php and http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf

[12] See: http://www.nap.edu/openbook.php?record_id=12720&page=1

[13] See: http://web.mit.edu/bcs/sinha/papers/19results_sinha_etal.pdf and http://www.safeguardingaustraliasummit.org.au/uploader/resources/Dragana_Calic.pdf et al.

[14] See: http://www.icao.int/icao/en/atb/meetings/2011/tagmrtd-20/Docs/TagMrtd-20_WP005_en.pdf

[15] For announcement of UK passport issuance changes, see: http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/220.htm. Current UK passport application form refers to credit checks at the bottom of page 10, see: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_184487.pdf

[16] See: http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html

[17] Part 3 of Telecommunications (Service Provider, Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000, see: http://www.comlaw.gov.au/Details/F2005C00313

[18] In Australia and other countries, many of these data aggregators got their start as credit checking bureaus before diversifying and extending their datasets and offering, e.g., CRM, vetting and identity verification services. Data aggregators active in the US and UK include: http://www.acxiom.com/products_and_services/identity_solutions/Pages/IdentitySolutions.aspx http://www.acxiom.com/products_and_services/background_screening/Pages/BackgroundScreening.aspx http://www.lexisnexis.com/risk/identity-verification-authentication.aspx http://www.reedelsevier.com/OurBusiness/LexisNexisRiskSolutions/Pages/lexis-nexis-screening-solutions.aspx

[19] The UK's fraud protection service has recently called for expanded use of social footprint checks in identity verification. See: http://www.finextra.com/news/announcement.aspx?pressreleaseid=40379

[20] Mobile telephones are being transacted to revolutionize service delivery in myriad ways (particularly in the Third World) and becoming a stronger and more valuable identity-related attribute as a result. See: http://www.economist.com node/18008202?story_id=18008202&fsrc=nwl and for an identity verification specific application, see: http://identityx.com/

[21] Page 62 of ANAO Report No.29 2009–10, 'Attorney–General's Department, Arrangements for the National Identity Security Strategy', see: http://www.anao.gov.au/uploads/documents/2009-2010_Audit_Report_29.pdf ■

MRTD AND BORDER CONTROL NEWS

Netherlands
A pilot project of automated border controls was launched at Schiphol Airport that can identify forged passports and wanted persons. Electronic gates equipped with facial recognition check passengers' identities with digital passport photographs.

Germany
A new electronic residence permit is being issued to nationals from non-EU countries. Technically similar to the new identity card for German nationals, the card has a hidden chip containing biographic and biometric data (facial image and two fingerprints).

USA
TSA started testing new technologies to identify altered or fraudulent passenger documents and boarding passes at selected international airports. The Credential Authentication Technology–Boarding Pass Scanning System (CAT-BPSS) scans a boarding pass and photo ID and authenticates the pass by automatically verifying the name.

United Kingdom
The UK Border Force will have to meet the challenge of processing unprecedented numbers of visitors during the London 2012 Summer Olympics.

France
Toulouse-Blagnac Airport is testing SIM-based Near Field Communication (NFC) technology to allow passengers to pass through the airport's controls and gates using only their mobile phones.

United Nations
The United Nations is to launch a new biometric UN Laissez-Passer in 2012. UN participation in the ICAO Public Key Directory became official on 14 June 2012.

Algeria
Algeria started issuing new ePassports in early 2012. The progressive roll-out of biometric passports is expected to be completed by the end of the year.

Panama
The Government of Panama chose a consortium to supply ePassports. The first biometric passports are expected to be issued in early 2013.

Chile
The national records administration (Servicio de Registro Civile Identificación) will issue ID cards and ePassports under its new identification and travel document issuance system.

Argentina
Argentina started issuing new biometric passports in June 2012. Increased passport security will facilitate new visa-free agreements for Argentinean nationals.

Estonia

New passport enrolment equipment deployed by the Police and Border Guard Board makes passport application and enrolment available nationwide for Estonian citizens.

Latvia

Latvia is setting up a new infrastructure for issuing and verifying electronic ID documents. This new PKI system enables verification checks of passports and identity documents at border control posts and all Latvian embassies across the globe.

Europe Union

The new Schengen Visa Information System (VIS) was launched September 2011 in the consular posts in North Africa. VIS will be expanded to the Near East and Gulf regions and should be connected to all Schengen States' consular posts worldwide within two years.

Russia

Biometric ePassports with fingerprint data are now being issued by the Russian Federal Migration Service.

Czech Republic

Czech border police implemented an EasyGo eGate system at Prague Ruzyne Airport at the end of 2011, which verifies the authenticity of travel documents based on optical and electronic security features. A gate camera records a live image of the traveller, which is compared by the system to the passport photograph.

Moldova

To increase security of national passports, 35 biometric data capture stations and 200 fingerprint readers were installed. Moldova's new ePassports include digital facial photos, fingerprints and other document security features to prevent forgery and identity fraud.

Armenia

New biometric passports will be issued from June 2012.

China

New biometric passports issued May 2012 have a digital chip storing personal details, facial image and fingerprints. Over 38 million Chinese are passport holders with an expected 20% increase annually.

UAE

Dubai Airport opened a new eGate system based on biometric face recognition to speed travellers through border control. Rolled out in terminal three, the new system will be installed across all the airport's immigration controls.

Indonesia

Jakarta's Soekamo-Hatta International Airport launched Indonesia's first eGate system, which ePassport holders can use at two international departure gates and eight international arrival gates. Since January 2011, an estimated 12,000 Indonesians hold ePassports.

New Zealand

The new Immigration Global Management System (IGMS) will see further improvements to Immigration New Zealand's identity management systems, enabling real-time biometric checks internationally as well as introducing face biometrics and biometric alert lists.

From left to right: **Rodrigo Duarte Guimarães**, *Federal Police Commissioner, Chief of Passport Division, Federal Police, Brazil;* **Eduardo de Mattos Hosannah**, *General-Coordinator for Consular Planning and Integration, Ministry of External Relations, Brazil; and* **Mauricio Siciliano**, *MRTD Officer, ICAO.*

REGIONAL SEMINAR WITH GLOBAL OUTREACH

Addressing ePassport implementation in Rio

The ICAO Regional Seminar on MRTDs, Biometrics and Security Standards took place in Rio de Janeiro, Brazil, on 17 to 19 April 2012. It was organized with the support of the Government of Brazil, namely, the Brazilian Ministry of Foreign Affairs and Casa da Moeda, Brazil's national mint. The event attracted over 180 government and industry participants from 42 States: 22 from the Americas and 20 from Africa, Asia, Central Asia and the Middle East.

The seminar venue, the Itamaraty Palace, was symbolic of the Brazilian Government's commitment to ensuring the Seminar was a high-level success. The Itamaraty Palace is one of the finest historical buildings in Rio. Originally the seat of the Republican government (1889-1898), it later became the headquarters of the Brazilian Ministry of Foreign Affairs (1899-1970) until the national capital moved to Brasília. Diplomats' seven decade association with the palace remains so strong that

Itamaraty Palace

the name, Itamaraty, has become synonymous with the Brazilian Foreign Ministry. Built in the Neoclassical style, with an inner garden incorporating a row of imperial palms, the palace today is the regional office in the former capital of the Foreign Ministry. It houses the Historical and Diplomatic Museum, the Historical Archive and Map Collection and is used for high-level meetings and conferences sponsored by the Brazilian Government.

The focus of the Regional Seminar was electronic passports. This important Seminar addressed current and emerging ICAO MRTD specifications, identity management best practices and related border security issues—with particular reference to the Americas region. The programme addressed in detail the advantages and challenges of using biometric data in travel documents, points of importance with regard to implementing electronic passports, technical specifications, procurement issues, reading ePassports at borders and the role of the ICAO Public Key Directory (PKD) in achieving robust global security.

Itamaraty Palace

Complementing the Seminar were 12 industry partners who displayed a broad range of products and services related to MRTDs, biometric identification, travel document security applications and border inspection systems.

ICAO MRTD Regional Seminars—like the one in Brazil—have two main purposes. First, they provide an opportunity to brief participants from Member States about current MRTD specifications and new developments and clarify any specific questions and finer technical points. Secondly, they provide a forum for professional discussions about the current and emerging needs of States and other stakeholders. They also present an opportunity to discuss practical ways on how to join forces to strengthen MRTD implementation and border security capacity so that States and their societies can benefit from enhanced security and facilitation that the MRTD Programme offers.

MESSAGES AND THEMES

The Regional Seminar in Rio addressed those needs very well. In particular, the numbers and diversity of the participants highlighted the importance that government agencies and the private sector place on travel documents, border security and combating terrorism and trans-border crime. Some important messages and themes that emerged from Seminar discussions included:

- Franklin Hoyer, Director of the ICAO Regional Office in Lima, urged participants to reflect upon what has been achieved in the decade since 9/11 and what still could be done to ensure the greatest possible security worldwide. Security is a sector that allows no compromises. It is our responsibility, he said, to be proactive, innovative and explore every further option that adds to global security and cooperative international efforts in combating terrorism.

- Compliance with ICAO MRTD Standards and specifications is essential to maximizing security and facilitation benefits for States and their citizens. ICAO has been updating and streamlining the structure of Document 9303 and significantly enhancing its contents with the inclusion of up-to-date Technical Reports and information contained in the Supplement to Doc 9303.

- The Seminar highlighted significant additional security and facilitation benefits that ePassports offer to States provided they are properly implemented, rely on the ICAO PKD and are correctly read at borders. Discussions at the Seminar also highlighted a range of challenges that States often face in implementing or reading ePassports, identified key points to watch and stressed the importance of performing a detailed cost/benefit analysis before launching an ePassport.

On the left: Franklin Hoyer, ICAO Regional Director, Lima.
On the right: Ambassador Eduardo Gradilone, Under-Secretary for Brazilian Communities Abroad, Ministry of External Relations, Brazil.

- The session on the PKD stressed the importance of considering all the elements required to issue an ICAO-compliant ePassport, which includes implementation of the PKD. A passport with a chip that simply ignores or overlooks this element cannot be called an ePassport, according to ICAO official definitions.

- The Seminar addressed fundamental questions that have to be asked before implementing an ePassport. One requires a realistic assessment and understanding of what ePassports can and cannot do, what the cost and benefit implications are and what the indispensable foundations are of an effective ePassport system. These are key questions that policymakers and senior policy members must ask themselves before implementing an ePassport and the Seminar presentations and discussions provided a useful checklist and framework for decision-making.

- The security of the passport issuance process and Evidence of Identity require particular attention. This is an area where identity fraud efforts have been shifting globally and could be exploited for terrorist and trans-border crime purposes. ICAO will continue with the on-going work of codifying good practices in secure issuance and identity management for the benefit of all States.

- Smart Borders (eBorders) is an innovative area where new approaches are being explored to enhance both border security and facilitation. In particular, eBorder developments integrate the use of both travel documents and data to maximize security benefits. Success stories about eVisa show that Smart Borders can be a significant addition to the broader security framework. The ICAO Secretariat has been following eBorder developments worldwide and exploring options of providing guidance material to States about already existing best practices.

- It was acknowledged that MRTDs represent a vital—but limited—segment of overall border controls, especially in the rapidly digitizing world. In order to make border controls effective, both travel documents and data sharing have to be used in an integrated manner, especially when it comes to combating terrorism and serious transnational crime. Good examples are Advance Passenger Information (API) and Passenger Name Record (PNR), which are both closely linked to MRTDs.

- Some capacity gaps were identified during the Seminar's open and constructive discussions. The ICAO Secretariat and the TAG/MRTD Implementation and Capacity-Building Working Group will be following them up and exploring ways on how to address them through practical capacity-building projects. States were also encouraged to maintain dialogue with ICAO about their ongoing and newly emerging MRTD and border challenges, primarily through the ICAO Regional Office in Lima.

Participants at Rio Seminar held in Itamaraty Palace.

CONCLUSION

All participants noted the tremendous progress of our Brazilian hosts in implementing state-of the-art travel document and border control capacity and there is confidence the momentum will be maintained in this challenging but essential work. Participation of ICAO officers, numerous experts from the Technical Advisory Group on MRTDs (TAG/MRTD) and partner organizations provided state-of-the art expertise and facilitated informed discussions. The seminar sent a strong reminder that we no longer live in the 1950s.

Travel documents and identity management remain an important part of border controls and global security—but issuing ePassports is only half the job—they must be properly read at the borders. The use of electronic data and intelligence-driven border controls has become unstoppable and gaining further momentum. The expanding use of API/PNR is the best example. In managing border security, travel documents and electronic data sharing are two sides of the coin. Both have to be used in an integrated manner to offer optimal security and facilitation benefits to States.

This successful Regional Seminar was the result of excellent cooperation between many parties. The Government of Brazil, especially the Ministry of External Relations and Casa da Moeda, provided enormous assistance and support in organizing the event. Special thanks are due to Ambassador Valter Pecly Moreira, Head of Itamaraty Palace, whose substantial contribution, including making the venue available to the ICAO Seminar, was essential to its success. ■

SEMINAR PARTICIPANTS

A total of 42 States participated in the ICAO MRTD Regional Seminar held in Rio de Janeiro, Brazil, 17-19 April 2012.

- Argentina
- Austria
- Belgium
- Bolivia
- Brazil
- Burkina Faso
- Canada
- Central African Republic
- Colombia
- Costa Rica
- Chile
- China
- Dominican Republic
- Ecuador
- El Salvador
- France
- Germany
- Guatemala
- Guyana
- Honduras
- Indonesia
- Iran
- Lebanon
- Malaysia
- Mexico
- Namibia
- Netherlands
- Nicaragua
- Pakistan
- Panama
- Paraguay
- Peru
- Portugal
- Republic of Korea
- Russia
- Saudi Arabia
- South Africa
- Sri Lanka
- Suriname
- Trinidad & Tobago
- Uruguay
- USA

ONGOING MRTD CAPACITY-BUILDING EFFORTS IN THE AMERICAS: MEXICO, PANAMA AND THE DOMINICAN REPUBLIC

The need for Machine Readable Travel Documents (MRTD) capacity-building efforts has been increasing worldwide. The current MRTD specifications are elaborate and effective—in line with the practices of the most developed States—but given their complexity, numerous States have been struggling with implementing them because of the lack of technical expertise or funds or both. Such capacity gaps are weakening universal MRTD implementation and call for a closer technical dialogue with those States in need, intensified liaison with donor agencies and expanding capacity-building programmes.

The Americas and Caribbean have a long history of cross-border migration and, in many instances, weaknesses in border control and identity management. For the past decade, population mobility and effective border controls have become a matter of even greater concern for their governments due largely to the rise of irregular migration and trans-border crime. In addition, the linkages between national (and regional) security and border controls have prompted their governments to factor international organized crime and terrorism threats into their migration and identity management measures. As a result, the need for enhanced comprehensive border and identity capacity-building strategies has emerged as a priority for both individual governments and regional bodies.

At the Mexico Sub-Regional Workshop and Consultations, from left to right: Steven Griner, Coordinator, Universal Civil Identity Program in the Americas, Department for Effective Public Management, OAS; Kent Lewis, Chief of Section, Information Sharing and Technical Assistance, DHS/US-VISIT; José Sandoval, Director of Refugees in the Ministry of Foreign Affairs, Ecuador; Joel Rouchon, Police Captain, Security, Embassy of France in Mexico; and Carlos Vargas, Forensic Expert, Document Fraud and Security, CSDB INTERPOL.

ICAO has been working closely with regional agencies in the Americas, particularly those with a direct mandate in combating terrorism and trans-border crime. Advocacy of MRTD Standards and technical consultations that assist States with their implementation are a vital part of MRTD capacity-building efforts in the Americas. Some capacity gaps require long-term structural reforms and significant resources from the international community for delivery through technical cooperation projects. The ICAO MRTD Programme has been consolidating and expanding MRTD capacity building globally, including in the Americas, in order to deliver technical assistance to States in need.

A current example of such technical cooperation is the ICAO project, Capacity Building in Travel Document Security and Identity Management in the Americas, organized jointly with the Organization of American States' (OAS) Secretariat of the Inter-American Committee against Terrorism (CICTE). The three-year technical cooperation initiative, which started in late 2011, is funded by the Government of Canada. The objective of the project is to assist participating beneficiary States to achieve compliance with the standards contained in ICAO Annex 9, Document 9303, and the best international practices on travel document issuing. In particular, it also aims at consolidating the States' capabilities to prevent terrorism and trans-border crime through enhanced cross-border cooperation and capacity building in order to achieve effective travel document issuing and identity management systems through needs assessments, project development and future capacity-building activities.

FOCUS ON MEXICO

The first project event was a Sub-Regional Workshop and Consultations held in Mexico City on 12-14 December 2011. The workshop was hosted by the Government of Mexico and attended

Participants at the Mexico Sub-Regional Workshop and Consultations.

by 31 government officials from the national passport issuing, civil registry and migration agencies of the Dominican Republic and Mexico. The workshop focused on travel document security and identity management, using the ICAO Guide for Assessing Security Standards for Handling and Issuance of Travel Documents, to assess security in the handling and issuance of travel documents and identity and border controls.

Invited experts spoke on those topics and facilitated round-table discussions and working groups. Participants from Mexico and the Dominican Republic gave national presentations on travel document security and identity management in their countries, highlighting key challenges, capacity gaps, ongoing initiatives and best practices.

In particular, these sessions addressed:

- Issuance of secure MRTDs according to ICAO standards and specifications;
- Vulnerabilities and challenges in the issuance process and identity management;
- Improvement of the national civil registry and increasing security of birth certificates and other breeder documents;
- Enhancing the technical knowledge and security awareness of civil registry, migration and passport staff;
- Self-assessment of the passport issuance process using the ICAO Assessment Guide for assessing security in the handling and issuance of travel documents; and
- Importance of improving inter-agency cooperation between civil registries, passport, border control and related agencies and strengthening cross-border cooperation among participant States.

Before the workshop, participants completed a preliminary survey developed by the Implementation and Capacity-Building Working Group (ICBWG) of the Technical Advisory Group of MRTD. These findings assisted in generating informed discussions and identifying gaps and priority areas during the workshop.

FOCUS ON PANAMA

The second project activity was the Sub-Regional Workshop and Consultations on Capacity Building in Travel Document Security and Identity Management, which was held in Panama City on 27-29 February 2012. Hosted by the Ministry of Foreign Affairs of Panama, participating in this workshop were 41 government officials from the passport issuing, civil registry and migration agencies of Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama.

Participants from the Panama Sub-Regional Workshop and Consultations.

Carmen A. Fernández, National Director of Passports, Panama.

Round-table discussion in Panama.

Barry Kefauver, ISO Representative, at the Panama Sub-Regional Workshop and Consultations.

Joel Rouchon, Police Captain, Security, Embassy of France in Mexico, at the Panama Sub-Regional Workshop and Consultations.

The programme consisted of four sessions on topical and case study presentations led by technical experts, who also facilitated work group round-table discussions. In addition, the six Central American countries gave national presentations on their individual situations in the area of travel document security, identity management and border control. Each presentation identified and highlighted their key challenges, capacity gaps, ongoing initiatives and best system and process practices. Some of the themes and recommendations that emerged at the Panama workshop included:

- ICAO, OAS/CICTE and other international organizations should work together to coordinate and prioritize travel document security and identity management capacity-building efforts;
- Importance of developing further initiatives that help and assist participating beneficiary States to achieve compliance with the standards contained in ICAO Annex 9, Document 9303 and other best international practices on travel document issuing and control;
- States should be encouraged and their staff trained to communicate and use INTERPOL's Lost and Stolen Travel Document (SLTD) database in order to share real-time information on lost and stolen travel documents;
- Work towards developing a centralized database platform for information sharing between government agencies issuing identity documents to decrease identity fraud;
- Develop mechanisms that will improve interoperability, communication and collaboration between government agencies dealing with civil registry, document management, passport issuance and border control;
- Strengthen the training capabilities of State agencies to enhance the expertise of the staff who handle and verify travel and identity documents. In particular, provide further training on the use of the ICAO Assessment Guide for assessing security in the handling and issuance of travel documents; and
- Upgrade the security of breeder documents, a major priority area, including potential use of biometrics, national identity number and the broader Evidence of Identity framework.

FOCUS ON THE DOMINICAN REPUBLIC

The MRTD gap assessment and technical consultations in the Dominican Republic took place on 28-30 March 2012 in Santo Domingo. The assessment team consisted of Malcolm Cuthbertson, lead expert from the UK, and representatives from the OAS/CICTE and ICAO. The scope of the assessment included passport issuance and personalization, the integrity of the issuance process, Evidence of Identity, 'breeder documents' and related inter-agency cooperation matters.

The methodology included fact-finding from diverse sources and on-site interviews with Dominican Republic government officials as well as the study of background documents, legislation and other sources. The information collected was analyzed using the

ICAO Assessment Guide, with particular reference to compliance with Document 9303 and good international practices in passport issuance and identity management.

The assessment in the Dominican Republic had the following objectives:

- Assess the passport and issuance process of the Dominican Republic, taking into account compliance with ICAO Standards and specifications and good international practices;
- Examine its national identity management in relation to the issuance process of travel documents and 'breeder documents', chiefly birth certificates and the national ID card, *cédula de identidad*;
- Identify any current or potential challenges in relation to passport issuance and identity management and produce recommendations to relevant government agencies for consideration and action where appropriate.

While the primary focus of the meetings and technical discussions centred on the Directorate General of Passports and the Central Electoral Commission, other relevant government agencies were met in order to broaden the perspective. In total, about 30 government officials were encountered in their working environment, including the Directorate General of Passports,

At the Central Electoral Council, Dominican Republic, from left to right: Malcolm Cuthbertson, ISO Expert; Erik Slavenas, Programme Officer, ICAO MRTD Programme; Roberto Rosario Márquez, President, Central Electoral Council, Dominican Republic; Paola Fernández, Project Manager, OAS/CICTE; Kimberly Polacek, Assistant Project Manager, OAS/CICTE; Franklin Reynaldo Frías Abreu, Information Technology Director, Central Electoral Council, Dominican Republic; Gina Puello, Deputy Director, Directorate General of Passports; and Carlos Mesa, Advisor, Directorate General of Passports.

At the Civil Aviation and Airport Security Body Agency (CESAC), Dominican Republic, from left to right: Carlos Mesa, Advisor, Directorate General of Passports; Gina Puello, Deputy Director, Directorate General of Passports; Kimberly Polacek, Assistant Project Manager, OAS/CICTE; Colonel Franklin Garrís Peralta, Deputy Director, Civil Aviation and Airport Security Body Agency (CESAC); Paola Fernández, Project Manager, OAS/CICTE; Erik Slavenas, Programme Officer, ICAO MRTD Programme; and Malcolm Cuthbertson, ISO Expert.

At the Dominican Republic's Directorate General of Passports.

Central Electoral Commission, Directorate General of Migration, Civil Aviation and Airport Security Body Agency (CESAC) and Santo Domingo's Las Americas International Airport where the focus was on immigration and customs controls.

At the Directorate General of Passports, Dominican Republic, from left to right: Carlos Mesa, Advisor, Directorate General of Passports; Kimberly Polacek, Assistant Project Manager, OAS/CICTE; Paola Fernández, Project Manager, OAS/CICTE; Malcolm Cuthbertson, ISO Expert; interpreter; and Erik Slavenas, Programme Officer, ICAO MRTD Programme.

From the very beginning, it was stressed that the assessment was not an audit or a test. Instead, it was a technical consultations exercise that provided an opportunity to discuss challenges in passport issuance and identity management in an open and constructive manner and jointly identify solutions and recommendations. The atmosphere during the meetings and site visits was particularly open, welcoming and constructive. Meetings at the Directorate General of Passports, Central Electoral Commission and Directorate General of Migration started with their senior executives followed by detailed technical discussions with agency officials. The atmosphere of openness and transparency was a significant factor that added to the success and relevance of the assessment exercise and demonstrated strong interest, commitment and trust on behalf of the Government of the Dominican Republic.

Other project activities for the rest of 2012 include regional workshops in Trinidad and Tobago and Haiti as well as assessment missions to El Salvador, Guatemala and another Caribbean State.

A key asset in supporting ICAO MRTD capacity-building work has been the TAG/MRTD Implementation and Capacity-Building Working Group (ICBWG). Established in May 2008, the ICBWG has become an international framework to assist developing States in addressing their capacity gaps in travel document security, identity management and border security by providing technical expertise and developing capacity-building interventions. The ICBWG has been proactive in engaging States in need of assistance, the donor community and other partner international agencies in tackling identity management and border control challenges in a concerted and cooperative manner. ■

A PRACTICAL TOOL TO ENHANCE TRAVEL DOCUMENT SECURITY:

ICAO GUIDE FOR ASSESSING SECURITY OF HANDLING AND ISSUANCE OF TRAVEL DOCUMENTS

The security and ICAO-compliance of travel documents remains of the utmost importance worldwide. Increasingly discussed, as part of travel document security, is the integrity of the issuance process, a major focus as far as border security is concerned.

Since ICAO-compliant MRTDs have become so secure and difficult to forge, the trans-border criminal focus has shifted to manipulating Evidence of Identity or exploiting weaknesses in the travel document issuance process. Recognizing the newly emerging challenges and mandated by ICAO to take action, the ICAO MRTD Implementation and Capacity-Building Working Group (ICBWG) developed the *Guide for Assessing Security of Handling and Issuance of Travel Documents*, which can be used for both self-assessments and independent assessments by an external expert, depending on the needs of the travel document issuing agency. The Guide has been developed by an international group of independent ICAO-related experts with experience across all relevant aspects of the travel document continuum.

The scope of the Guide covers a number of core areas, including:

- Travel Document Issuing Authority: Organizational Structure, Internal Security and General Security Practices
- Application Processes
- Entitlement Processes
- Treatment of Materials and Blank Books
- Personalization and Delivery
- Document Security
- Facility Security
- Information Technology Security
- Personnel and Internal Integrity
- Lost and Stolen Travel Documents
- Overseas Issuance
- National and International Stakeholders

STRUCTURE OF THE GUIDE

It consists of three parts:

- Executive Summary outlines the rationale of the Guide.
- Part 1, Best Practices on Secure Issuance of Travel Documents, recommends security best practices for every step of the passport issuance process.
- Part 2, Assessor's Workbook, is a technical file that supports the practical assessment exercise and identifies the high-risk areas of particular concern. This is a comprehensive evaluation tool to assess issuance process vulnerabilities and follows the recommendations and chapter organization of Part 1.

LESSONS LEARNED

The Guide is a tool. It will never replace an experienced assessor familiar with the best international passport issuance practices. However, it can be used for self-assessment by national passport-issuing agencies as long as the person performing the self-assessment has reasonable experience with the issuance process and knowledge of the best global passport issuance practices and understands the limitations. Part 1 provides a compendium of good international practices. Ideally, the assessor should be well informed on these practices and solid practical experience in managing a national passport office.

However, as a tool, the Guide provides considerable value. It is a rigorous analytical framework that ensures no risk areas get through the cracks and are duly taken into account for overall risk assessment purposes.

THE FUTURE

The Guide has been used around the world for almost three years, including in the Americas, Central Asia and Europe, and valuable feedback has been provided on how further improvements can make it more relevant. ICAO has been exploring the opportunities of integrating this valuable knowledge and updating the Guide accordingly. In addition, options are being explored to move the Assessor's Workbook from Excel to a more user-friendly online software as well as designing training courses on the Guide for States to benefit from its use and application.

CONTACT US

Should you have any further questions or would like to share your practical experiences on using the Guide, please e-mail the MRTD ICBWG at icbwg@icao.int.

DOWNLOAD

The Guide is available free of charge and currently available in English, French and, coming soon, Spanish. Here is the link http://www.icao.int/Security/mrtd/Pages/Assessment-Guide.aspx to download a copy from the website. ■

KEEPING THE WORLD INFORMED

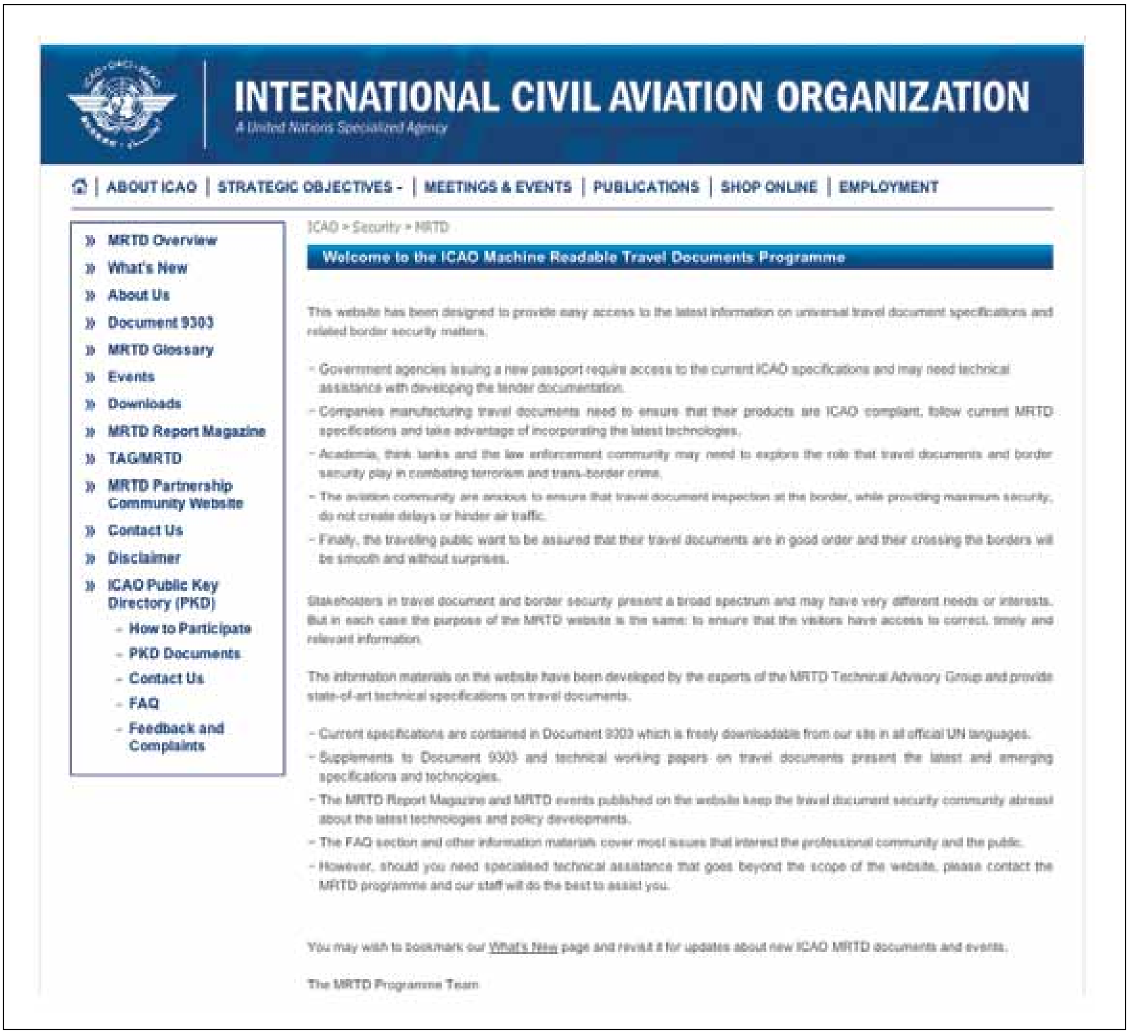
Welcome to the MRTD Programme Website

During the last year, the ICAO MRTD website underwent considerable changes in its structure and contents. In addition, it moved to a new software platform and was integrated into ICAO's overall website under the Security strategic objective.

Stakeholders in the travel document and border security community present a broad spectrum in the industry and governments. As a result, they can have very different needs or interests. But in each case the purpose of the MRTD website is the same: to ensure visitors have access to correct, timely and relevant information.

The information materials on the website, which were developed by experts within the MRTD Technical Advisory Group (TAG), provide state-of-the-art technical specifications on travel documents. The reference materials include:

- Current MRTD specifications contained in Document 9303 that can be downloaded without charge in all official United Nations (UN) languages.
- Supplements to Document 9303 and technical working papers on travel documents with the latest and emerging specifications and technologies.



Welcome to the ICAO Machine Readable Travel Documents Programme

This website has been designed to provide easy access to the latest information on universal travel document specifications and related border security matters.

- Government agencies issuing a new passport require access to the current ICAO specifications and may need technical assistance with developing the tender documentation.
- Companies manufacturing travel documents need to ensure that their products are ICAO compliant, follow current MRTD specifications and take advantage of incorporating the latest technologies.
- Academia, think tanks and the law enforcement community may need to explore the role that travel documents and border security play in combating terrorism and trans-border crime.
- The aviation community are anxious to ensure that travel document inspection at the border, while providing maximum security, do not create delays or hinder air traffic.
- Finally, the travelling public want to be assured that their travel documents are in good order and their crossing the borders will be smooth and without surprises.

Stakeholders in travel document and border security present a broad spectrum and may have very different needs or interests. But in each case the purpose of the MRTD website is the same: to ensure that the visitors have access to correct, timely and relevant information.

The information materials on the website have been developed by the experts of the MRTD Technical Advisory Group and provide state-of-art technical specifications on travel documents.

- Current specifications are contained in Document 9303 which is freely downloadable from our site in all official UN languages.
- Supplements to Document 9303 and technical working papers on travel documents present the latest and emerging specifications and technologies.
- The MRTD Report Magazine and MRTD events published on the website keep the travel document security community abreast about the latest technologies and policy developments.
- The FAQ section and other information materials cover most issues that interest the professional community and the public.
- However, should you need specialised technical assistance that goes beyond the scope of the website, please contact the MRTD programme and our staff will do the best to assist you.

You may wish to bookmark our What's New page and revisit it for updates about new ICAO MRTD documents and events.

The MRTD Programme Team

A screen shot of the *MRTD Report* section of the MRTD website.

- The ICAO *MRTD Report* magazine and MRTD events that keep the travel document security community abreast about the latest technologies and policy developments.
- The FAQ section (coming soon!) and other information materials that cover most issues of interest to the professional community and the public.

The main sections of the website are as follows:

MRTD Overview outlines the site's rationale and high-level guidance for navigating it.

What's New includes all the latest events and documents. Bookmark this page to keep updated about current MRTD developments

About Us provides a brief outline of the ICAO MRTD Programme yesterday and today.

Document 9303 provides free access to all parts and volumes of this Document in six official UN languages, including the current version of the Document's Supplement, which should be used for reference purposes in conjunction with the Document. The Supplement includes the latest specifications adopted by the TAG/MRTD, which will be incorporated into the next edition of Document 9303.

MRTD Glossary provides a list of MRTD technical terms. This glossary, which is not intended to be authoritative or definitive, will assist readers with terms that appear in articles published in the *MRTD Report*.

Events list upcoming MRTD events such as Symposia and Regional Seminars held around the world. At the bottom of this section, there's a link to past events where expert presentations and other documentation can be downloaded for reference.

Downloads provide easy access to key ICAO MRTD documents in PDF format, including a range of current MRTD Technical Reports.

MRTD Report provides access to digital copies of all issues of the magazine—from the first edition to the most recent. The *MRTD Report* is published by ICAO to serve a broad range of stakeholders in government agencies, aviation, document and border security industries, law enforcement, counter-terrorism and international organizations and the public interested in ICAO's work on Machine Readable Travel Document (MRTD) specifications and related technology. Published three times a year, the *MRTD Report* is available, without charge, in both hard copy and digital format.

TAG/MRTD provides current information on the ICAO Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), including reports and working papers from recent meetings and, prior to every meeting, logistical information for TAG members.

MRTD Partnership Community Website provides information about ICAO's commercial partners in the travel document and border management professional communities.

Contact Us for specialized technical assistance that extends beyond the scope of the website. Government agencies are welcome to contact the staff of the MRTD Programme who will do their utmost to assist you.

ICAO Public Key Directory (PKD) provides a broad range of information and reference documents concerning the functions, membership and administration of the ICAO PKD.

To keep yourself updated, visit the MRTD website at http://www.icao.int/Security/mrtd/Pages/default.aspx. ■

MRTD TECHNICAL REPORTS: EMERGING TECHNOLOGIES AND SPECIFICATIONS

Document 9303 is constantly evolving. New technologies keep emerging and need to be incorporated into Document 9303 with increasing speed. Compliance with ICAO MRTD Standards and specifications is essential to maximizing security and facilitation benefits for States and their citizens.

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 current Supplement. Ongoing activities include cleaning up the Supplement, incorporating Technical Reports and re-structuring Document 9303. The new edition of Doc 9303 is expected to be ready for translation and publication in the second half of 2013.

While the updated version of Document 9303 is being developed, the proper implementation of ICAO MRTD Standards and specification requires reading Document 9303 in conjunction with the Supplement and Technical Reports.

The Technical Reports and Supplement present the most current state-of-the art developments in MRTD specifications. They have been developed by leading experts of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), chiefly the New Technologies Working Group (NTWG). This issue of the *MRTD Report* provides a brief overview of the latest Technical Reports. They all are available on the website of the ICAO MRTD Programme. ■

TR: LDS AND PKI MAINTENANCE, VERSION 1.0, 5 MAY 2011

Updated and Current Specifications

The specifications for the electronic part of Machine Readable Travel Documents (MRTDs) were put in place in 2004. Specifications must be evaluated from time to time to stay up-to-date, especially with respect to cryptographic security features and Public Key Infrastructure (PKI). Therefore, an evaluation work plan was developed to address the various aspects that need to be updated. This Technical Report results from the evaluation and provides updated specifications.

STRUCTURE OF THE TECHNICAL REPORT

The 20-page report is comprised of five sections:

- Part 1, Introduction, outlines assumptions and terminology.
- Part 2, Logical Data Structure (LDS) includes present specification, revised specification, backwards compatibility, implementation strategy and documentation.
- Part 3, Certificate Profiles, also contains present specification, revised specification, backwards compatibility, implementation strategy and documentation.
- Part 4, Access Control, outlines present specification and revised specification.
- Part 5, Active Authentication, includes present specification, revised specification, backwards compatibility, implementation strategy and documentation.
- Part 6, Extended Length is comprised of present specification.

DOWNLOAD

Available free of charge from the website, here is the link to download this report http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx. ■

TR: MACHINE ASSISTED DOCUMENT SECURITY VERIFICATION, VERSION 1.0, 26 JULY 2011

Authenticating Security Features

This Technical Report provides advice on machine assisted authentication of security features incorporated in Machine Readable Travel Documents (MRTDs) made in accordance with the specifications set out in Document 9303, Part 1 (Machine Readable Passports), Part 2 (Machine Readable Visas) and Part 3 (Machine Readable Size 1 and Size 2 Official Travel Documents). The recommendations cover machine authentication of the security features in the document itself—based on materials, on security printing and on copy protection techniques—as well as advice on reader technologies that apply to machine authentication of documents.

The aim of the recommendations in this Technical Report is to improve the security of MRTDs worldwide by using machine assisted document authentication procedures. This report replaces Informative Appendix 2 to Section III, 'Machine-assisted document security verification', currently published in Doc 9303, Part 1, Volume 1, 6th edition, 2006.

STRUCTURE OF THE TECHNICAL REPORT

This 15-page report consists of six sections:

- Part 1, Scope, outlines the security features of the report's recommendations.
- Part 2, Introduction, provides the basis for the report.
- Part 3, Feature Types and Basic Principles, is comprised of machine assisted document verification features.
- Part 4, Document Readers and Systems for Machine Authentication, includes standard readers, advanced readers and PKI background systems.
- Part 5, Security Features and Their Application for Machine Authentication, contains substrate materials, security printing, protection against copying, personalization techniques, additional security measures for passport books and machine authentication.
- Part 6, Selection Criteria for Machine Verifiable Security Features, outlines the criteria for implementation.

DOWNLOAD

From the website, this report is available free of charge. To download a copy, here is the link http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx. ■

TR: MACHINE READING OPTIONS FOR TD1 SIZE MRTDS, VERSION 1.0, 7 APRIL 2011

Solutions for a Faster Machine-assisted Inspection Process

In the 1980s, ICAO published Part 3 of Document 9303, which set out the standards for 'Machine Readable Official Travel Documents'. Back then, few States changed their Identity (ID) Cards from the non-compliant ICAO model, or td2 format, into a td1 format.

In the late 1990s, more States started changing their ID Cards to an ICAO-compliant td1 format and included a contactless chip in the ID Card to be compatible with Doc 9303, Part 3, Volume 2. As a result, more border control authorities, airport authorities and airlines are using eReaders to read them.

However, with a td1 size card, the border control officer first has to read the Machine Readable Zone (MRZ) on the rear of the card to create a travel record, then remove it from the reader and turn it over to read the front side to collect the biographical profile of the bearer, including the photograph and document-related information.

This is a time consuming process. This Technical Report examines the challenges and comes up with alternatives.

STRUCTURE OF THE TECHNICAL REPORT

This 24-page report consists of six sections:

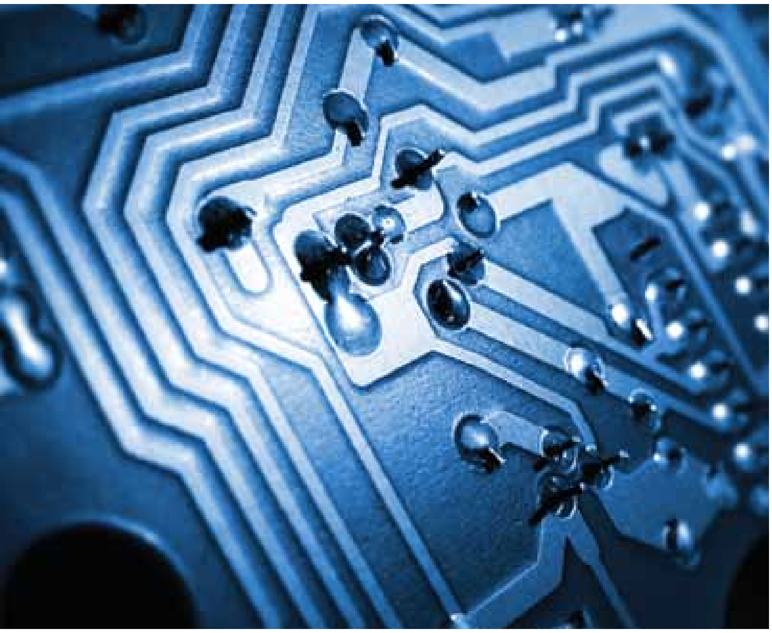
- Part 1, Introduction, outlines background, operational experiences, assumptions and terminology.
- Part 2, Overview, sets out the parameters of the requirements.
- Part 3, Identified Solutions, is comprised of options explained, prerequisites and pros and cons of options.
- Part 4, Application Comparison for One-Line MRZ, covers one-line MRZ with accent on a limited person query, benefits and consequences, one-line MRZ with accent on a complete document number query and benefits and consequences.
- Part 5, Non-Chip Versus Chip-Enabled td1 explains Outcome Tag 7 (9 December 2009 in Montreal) and New Technologies Working Group (NTWG) Meeting in Bangkok.
- Part 6, Specifications for Chip Based td1, sets out specification supplemental access control, Card Access Number (CAN) specifications and reference documentation.

DOWNLOAD

Here is the link http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx to download this report free of charge from the website. ■

TR: CSCA COUNTERSIGNING AND MASTER LIST, VERSION 1.0, 23 JUNE 2009

A Customized Approach to Implementing PKI



The principles of Public Key Infrastructure (PKI) schemes have evolved in their use to become highly complex in their application to modern scenarios. Their general primary use is in Internet transactions where keys are to be trusted across a broad range of users and organizational entities. This has resulted in elaborate systems of key certificates where public keys are issued in 'certificates', which are digitally signed by trusted issuing organizations called Certificate Authorities (CAs).

A complicating factor is the need for Certificate Revocation Lists (CRLs). These CRLs indicate where a key (certificate) has lost, for whatever reason, its validity. In fact, by revoking a certificate and publishing this revocation in a CRL, the certificate's issuer informs receiving parties that the contents can no longer be trusted.

The ICAO operating environment is different from the above mentioned commercial environments. The question of public key revocation applies in a different way—compared to individual users—since the unlikely event of a compromise of any State's private key, which was used during some period to sign many MRTDs, cannot deny documents were indeed legitimately issued and signed using that key. These (valid) documents will remain in use by their holders for travel purposes.

As a consequence, ICAO Doc 9303 has specified a customized approach. This approach is intended to enable the MRTD community to fast track implementation of this application for MRTDs with Integrated Circuit (IC) read-only access and take advantage of its benefits without attempting to address larger PKI policy issues and complex hierarchies. The ICAO PKI scheme specifies a two-layer certificate chain, enabling an inspection system to verify the authenticity and integrity of the data stored in the MRTD's contactless IC. The (highest level) root CA in this scheme is the Country Signing Certificate Authority (CSCA), which authorizes Document Signers (DS) to digitally sign the Document Security Object (SOD) on the contactless IC.

The approach described in this Technical Report aims to provide an electronic means of distributing and publishing issuing States' CSCA Public Keys. It covers a number of core areas, including:

- Issuing a CSCA Master List
- Master List Signer revocation
- Receiving a CSCA Master List
- CSCA Master List Specification

STRUCTURE OF THE TECHNICAL REPORT

This 15-page report is comprised of three sections:

- Part I, Introduction, outlines the background, operational experiences, modified approach, assumptions and terminology.
- Part 2, Overview, includes general outline, CSCA countersigning process, publication on the PKD and relying parties.
- Part 3, Technical Specifications, includes CSCA Master List specification and CSCA Master List signing certificate profile.

DOWNLOAD

This Technical Report is available free of charge from the website. Here is the link http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx to download a copy. ■

TR: SUPPLEMENTAL ACCESS CONTROL FOR MRTDS VERSION 1.01, 11 NOVEMBER 2010

Implementing A Cryptographically Secure System

This Technical Report specifies an access control mechanism that is supplementary to Basic Access Control (BAC). It is based on Password Authenticated Connection Establishment (PACE). PACE establishes secure messaging between an MRTD chip and an inspection system based on weak (short) passwords and enables the MRTD chip to verify the inspection system is authorized to access stored data.

Document 9303 had introduced BAC as an optional access control mechanism. Due to its simplicity, BAC turned out to be a very successful protocol and was implemented in almost every ePassport. As a result, BAC is now a recommended feature for privacy protection. However, as the security provided by BAC is limited by the protocol's design, PACE can now be implemented in addition to BAC for a cryptographically stronger access control mechanism system. But States cannot implement PACE without first implementing BAC.

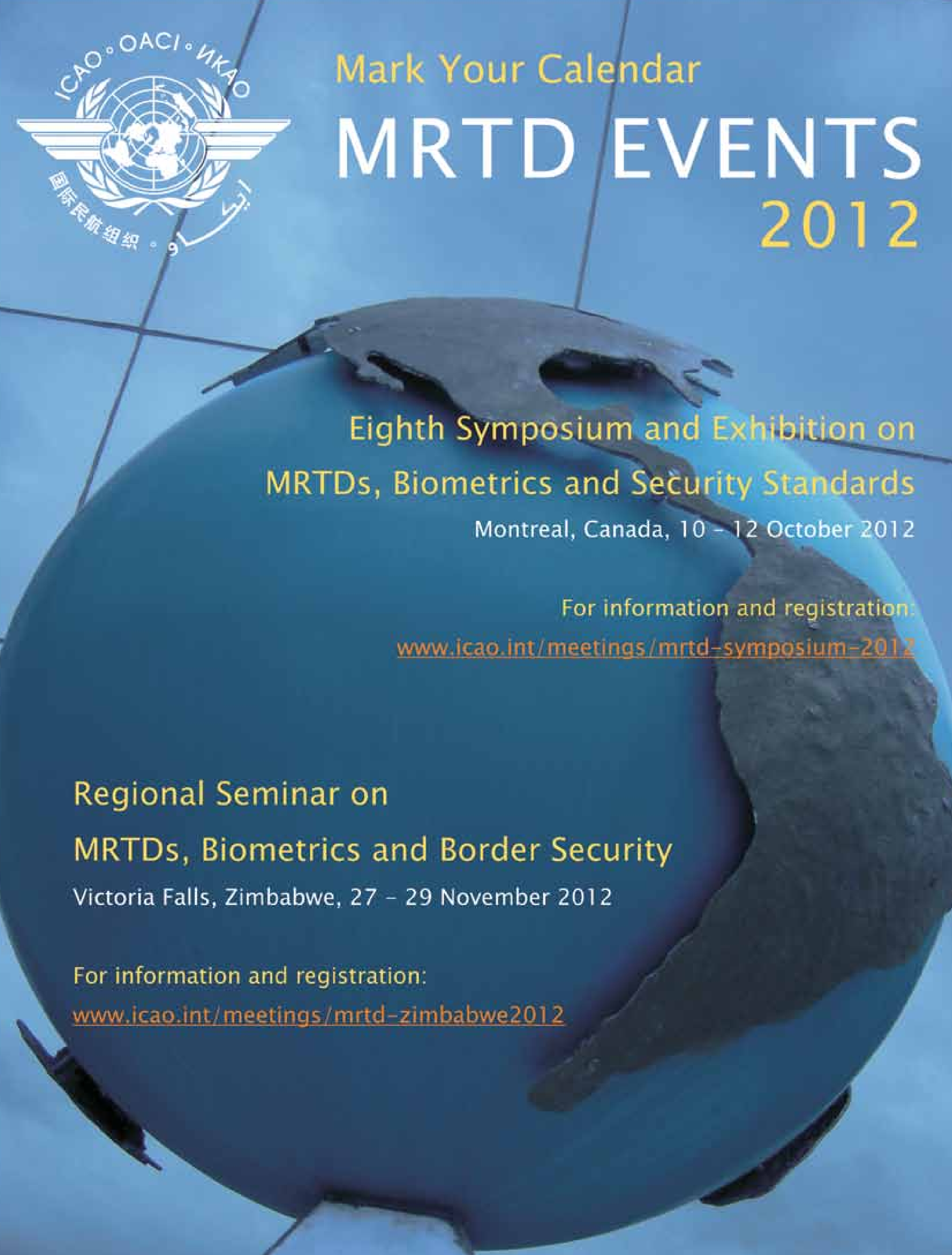
STRUCTURE OF THE TECHNICAL REPORT

This 31-page report consists of five sections:

- Part 1, Introduction, outlines the background, operational experiences, assumptions and terminology.
- Part 2, Overview, includes general outline and inspection procedure of PACE.
- Part 3, Technical Specifications, outlines logical data structure, application protocol data units, exchanged data and command chaining.
- Part 4, Cryptographic Specifications, includes key agreement algorithms, key derivation function, encrypting and mapping nonces, authentication token, public key data objects and secure messaging.
- Part 5, Point Encoding for the Integrated Mapping, high-level description of the point encoding method, implementation for affine coordinates and Jacobian coordinates.

DOWNLOAD

The report is available free of charge from the website. Here is the link http://www.icao.int/Security/mrtd/Pages/Technical-Reports.aspx to download a copy.



Mark Your Calendar

MRTD EVENTS 2012

Eighth Symposium and Exhibition on MRTDs, Biometrics and Security Standards

Montreal, Canada, 10 – 12 October 2012

For information and registration:
www.icao.int/meetings/mrtd-symposium-2012

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

POLICE
Mobile verification for all government documents