ICAO

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Vol. 8, No. 2 – Summer 2013

MRTD REPORT

THE ICAO PKD STATE OF PLAY:

Future Perspectives

In this issue

ICAO-AD-10-CAN-04-13-EN

When security is your priority, only the technology trusted by the world's premiere governments will do.

25 years and over **200 million passports** personalized.

info@getgroup.com

Copyright © 2013 GET Group. All rights reserved.

ICAO MRTD REPORT
VOLUME 8, NUMBER 2, 2013

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

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

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

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

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

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

The publishers extend their thanks to the companies, organizations and photographers who graciously supplied photographs for this issue.

Published by
International Civil Aviation Organization (ICAO)
999 University Street
Montréal, Québec
Canada H3C 5H7

The objective of the ICAO *MRTD Report* is to provide a comprehensive account of new developments, trends, innovations and applications in the field of MRTDs to the ICAO Member States and the international aeronautical and security communities.

Copyright © 2013
International Civil Aviation Organization

Printed by ICAO

Contents

www.icao.int

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

Member	Nominated by	Member	Nominated by
Mr. M. Lynch	Australia	Mrs. R. Ong-de Jong	Netherlands
Ms. L. Pezzack	Canada	Ms. A. Offenberger	New Zealand
Ms. M. Cabello	Chile	Vacant	Nigeria
Mr. M. Vacek	Czech Republic	Mr. Xuefeng Yang	People's Republic of China
Ms. P. Moutafian	France	Mr. C. Ferreira Gonçalves	Portugal
Dr. E. Brauer	Germany	Mr. O. Demidov	Russian Federation
Mr. B.K. Gupta	India	Mr. S. Tilling	Sweden
Mr. J. Nugent	Ireland	Mr. R. Vanek	Switzerland
Mr. H. Shimizu	Japan	Mr. H. Bloomfield	United Kingdom
		Mr. M. Holly	United States

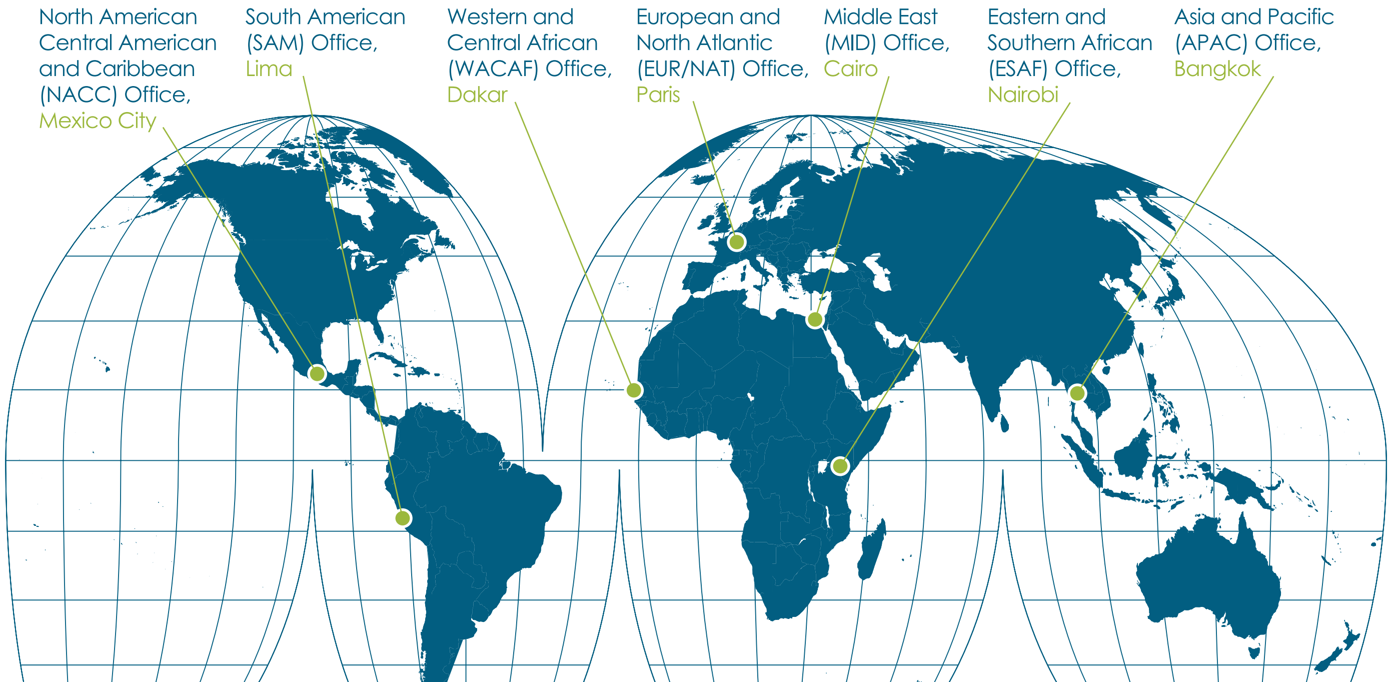
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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

WELCOME TO THE SUMMER ISSUE OF THE *MRTD REPORT*

2013 is a defining year for the MRTD programme and the global traveller identification community. The proposed ICAO Traveller Identification Programme (ICAO TRIP) Strategy, already endorsed by the ICAO Council, will be presented to the ICAO Assembly in the fall. Responding to the driving global forces and needs of Member States, the Strategy provides a framework for achieving the maximum benefits for travel documents in the future by bringing together elements of identification management and building on ICAO leadership in matters related to Machine Readable Travel Documents (MRTD).

At the centre of the ICAO TRIP Strategy is the key proposition for States, ICAO and all stakeholders to address: a holistic, coherent, coordinated approach is essential to the interdependent elements of traveller identification management. The ability to uniquely identify individuals requires a holistic and coordinated approach, which links the following five elements of traveller identification and border control management into a coherent framework: evidence of identification, document issuance and control, MRTDs, inspection systems and tools and interoperable applications. Such a broadened scope shapes a framework for multidimensional integrated efforts and synergies, under ICAO's leadership, to support ICAO's Strategic Objectives in the 2014-2016 triennium and beyond.

For ICAO and its Member States, the vision in traveller identification management is that all Member States can uniquely identify individuals. When the elements of identification management are optimally achieved, States will be in a position to identify individuals by their travel documents, which will comprise the highest possible degree of certainty, security and efficiency. Recognising the benefits of traveller identification management to aviation security and facilitation and the vision that all Member States can uniquely identify individuals, ICAO's mission would be to contribute to the capacity of Member States to uniquely identify individuals by providing appropriate authorities worldwide with the relevant supporting mechanisms to establish and confirm travellers' identities.

In addition to focusing on the aviation world, the TRIP concept serves the broad transportation sector by assuring border integrity and efficiency in maritime and land transport settings as well. These important benefits extend the contribution of ICAO's travel document related activities beyond border integrity at airports, with no additional cost to ICAO and Member States.

The contents of this *MRTD Report* reflect the diversity of issues and challenges in holistic traveller identification management. The PKD Chair reflects on the state of play—and future direction—of the ICAO Public Key Directory and its role in enhancing the security and facilitation benefits of ePassports. OSCE experts look into the challenges and advantages within a broader area of all electronic travel documents. Also presented are the results of an innovative collaboration between experimental psychologists and the Australian Passport Office to improve face verification accuracy at border controls. A Frontex team explores the dynamic world of border controls, with particular reference to the role of Automated Border Controls (ABCs) and biometric travel documents. Another article explores the fundamental relationship between identity fraud and trust in travel documents. Finally, an article on Russian travel documents presents a case study on how challenges and solutions were applied within a given context in issuing ePassports in one of the largest countries in the world.

And, of course, the MRTD Symposium in Montreal is approaching. Mark 22-24 October 2013 on your agenda. Like every year, the Symposium will explore ICAO's role and mandate in MRTDs, biometrics and identification management. Policy level presentations will include an overview of the global regulatory framework, an update on the results of the 2013 ICAO Assembly and new strategic directions for the proposed ICAO Traveller Identification Programme for the 2014 to 2016 triennium. The special feature of the Symposium is the focus on ABCs, its objectives, practices and challenges of developing related standards and specifications. It will explore a broad range of considerations shaping state-of-the-art ABC developments: newly emerging technologies, trust, reliability, non-intrusiveness, biometrics, use of the PKD, costs, privacy and human rights.

Other specialised topics include security and facilitation considerations in ABCs and the relevance of ABCs to the aviation industry and sustainable economic development. The Symposium will also address a range of practical challenges and solutions for ABCs and border management, including ABC operational and technical guidelines, biometric verification processes, quality control, proper reading of biometric travel documents at the border, trusted traveller programmes, the role of the ICAO PKD, challenges to border integrity and ways to combat them and much more.

Keep reading the *MRTD Report* to stay informed about the latest new developments. ■

THE ICAO PKD STATE OF PLAY

Future Perspectives

ABOUT ROMAN VANEK
He became Chairman of the ICAO PKD Board in May 2012. He is Chief of the Identity Documents & Special Tasks Division of the Switzerland Federal Office of Police. Aside from responsibilities in other areas, he is also responsible for the Swiss Passport and Identity Card. In this function, he is the Swiss representative at the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) of ICAO and the Article 6 Committee of the European Commission.

Roman Vanek, Chairman of the ICAO Public Key Directory, outlines the benefits of the PKD to enhance ePassport security, the cost reductions in the annual PKD participation fee and the need to shift the focus from the traditional representatives of countries participating in the PKD, the ePassport issuing authorities, to attracting border control authorities to also join the PKD.

The introduction of ePassports has been a tremendous success. Today more than 100 States and non-state entities issue ePassports. The additional security and the wish to make use of the new technology pushed countries towards the introduction of this new document type. According to a survey conducted by the New Technologies Working Group, over 500 million eMRTDs are in circulation today. It's safe to say that ePassports are here to stay—although it's already certain today that they will develop further.

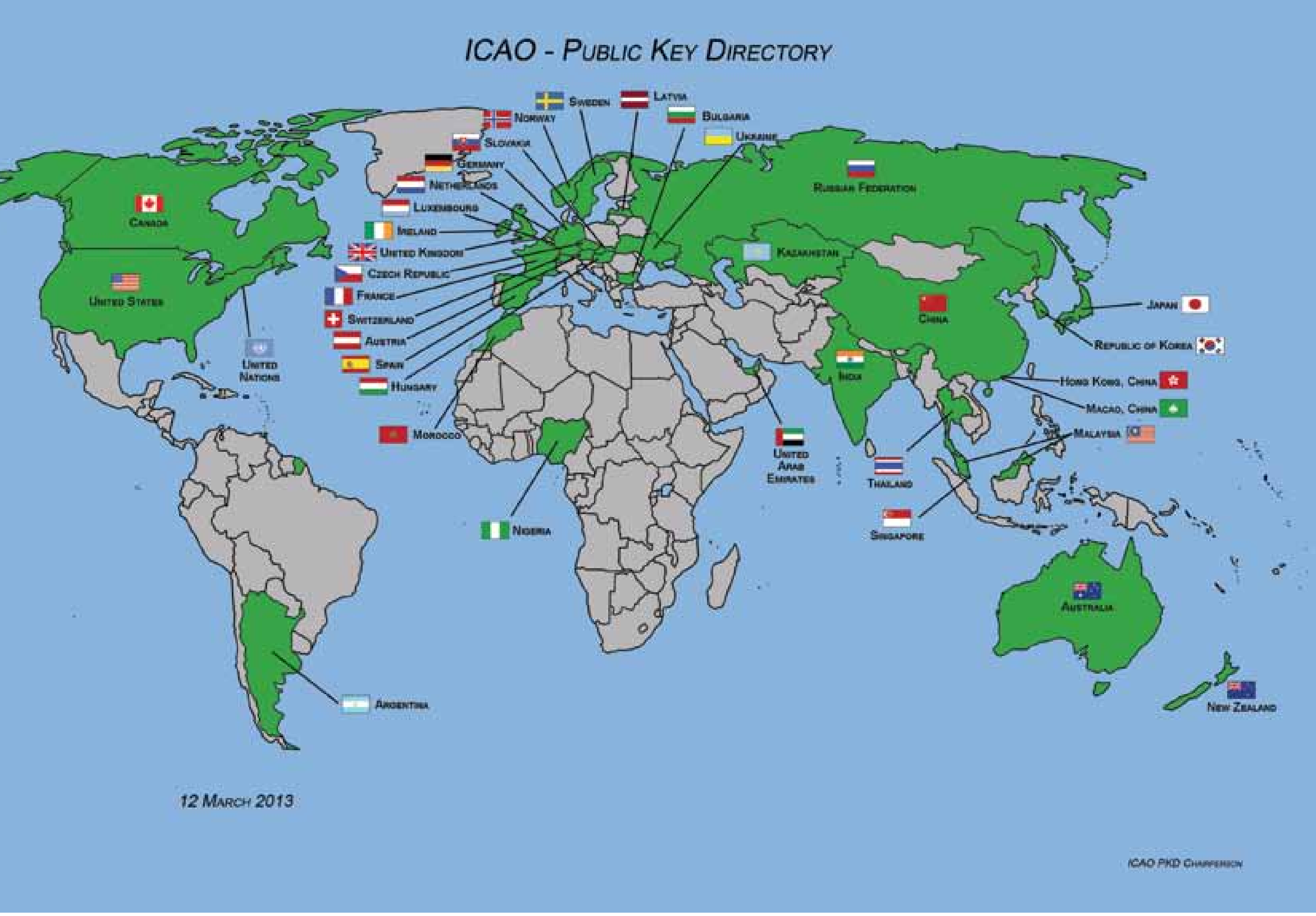
Therefore we now need to look on how the control of these documents is organised in an efficient and reliable way and how we make best use of the investment made into ePassports. If we do not use the technology properly we won't get a benefit from the investment made. And when I say 'we', I mean all the issuing authorities but also in particular the ones that paid for the new technology in passports. In most cases, this will be the tax payer and the buyers of an ePassport or, in other words, the citizens.

Air traffic and passenger numbers are expected to grow substantially in the coming years. Border control authorities, airport operators and airlines are looking at ways to cope with these growing numbers. At the same time, they have to compensate tight budgets by increasing the efficiency and productivity. Travellers and citizens on the other hand wish to cross borders as hassle free and as quickly as possible while expecting maximum security and facilitation. There are different ways to meet these requirements that sometimes seem to collide together. Today many countries are looking at different types of automated gates that might even include a self-service security scan. But no matter what kind of border control operation countries are looking for, if they wish to authenticate ePassports in a correct and efficient way, they must make use of the ICAO PKD.

In 2007, the PKD went into operations based on the initiative of a few countries (Australia, New Zealand, Canada, United States, United Kingdom, Singapore). Today the PKD consists of 37 participants from all over the globe (refer to the **ICAO PKD World Map**). This may seem a small number compared to the more than 100 issuing States and non-state entities that issue ePassports. However when these figures are put into relation with the overall number of issued ePassports, the picture looks very different. In fact, based on a survey conducted by ICAO's New Technologies Working Group (NTWG), 74% of the ePassports issued so far have been issued by a PKD participant. This means that border control authorities that use the PKD have access to the elements necessary to successfully authenticate the majority of the ePassports in circulation.

I therefore strongly encourage border control authorities to make use of the PKD and download the available certificates, master lists and revocation lists. One could argue that this is not necessary and that there are other ways to get hold of the certificates. Yes, there are other ways. However none of them is so convenient and reliable. The PKD offers an independent, organised, secure and cost effective online source for validated up-to-date information. The available Master Lists, containing validated Country Signing Certificates (CSCA) of other countries by other participants, give access to CSCAs even if a country has not established the initial CSCA exchange with all countries that issue ePassports. Looking at our operational experience in Switzerland, I have to say that getting hold of the CSCA of a country and the means to validate it independently through a thumbprint comparison proved to be one of the real live challenges when implementing ePassport based border controls. The Master List scheme gives the border control authorities a valid alternative to the bilateral not always feasible CSCA exchange.

Countries participating in the PKD are traditionally represented by their ePassport issuing authority. In the past, the issuers were the focus of the attention. It was the common goal to start issuing ePassports and improve travel document security. But now we need to shift the focus towards the control authorities. There might be good and valid reasons why a country decides not to issue ePassports. Before issuing ePassports, a country should first establish a reliable and robust system to guarantee the evidence of identity of an applicant. ICAO has recognised the importance of the secure identification of citizens and has started some important work in order to support issuers by implementing these necessary base lines in countries around the globe. The fact that a country doesn't issue ePassports yet should not hinder a country to join the PKD and be represented in the PKD by its border control agency. Such a country can use the PKD without any restrictions in its border control operation. In the meantime, the issuing of ePassports can be prepared and the experiences learned from cooperation with the other PKD



participants can be used in the ePassport implementation programme. As the current Chairman of the PKD, I would recommend such participation and I am looking forward to the inputs and needs of these bodies to our discussions in the PKD Board.

A total of 37 ePassport issuers have already decided to join the PKD and take advantage of its benefits. The PKD offers the participant a rapid and reliable distribution of certificates all over the globe. I compare this certificate distribution to the distribution of Specimens every time a new passport model is introduced. Only that in today's digital world the certificate distribution takes place more often and border control authorities therefore need to have immediate access to the certificates. Countries have spent millions of dollars or Swiss francs in the case of Switzerland to make ePassports available to its citizens. We did that in the interest of enhancing security but also because our citizens should be able to cross international borders as easily and securely as possible. I think that making certificates easily available around the globe and paving the way for facilitated and/or automated border controls is a good way to make use of this investment.

Compared to the cost of national ePassport projects and the cost of setting up and running national border control posts (with or without automation), the annual PKD participation fee remains very reasonable. The 2013 annual fee is US $47,950. This amount includes a reduction of about 19% compared to 2012 thanks to a generous participation from ICAO. ICAO has recognised the importance and the need of the PKD and in its conclusion the High Level Conference on Aviation Security that took place 12–14 September 2012 invited States to consider joining the PKD. Bearing in mind the different situations and challenges ICAO Member Countries are facing, I very much welcome and appreciate this support and hope to be able to count on the ongoing support for the PKD in the years to come.

Growing participation also leads to a reduction of the operator fee by 21%. As of 1 January 2014, the operator fee will be US $34,000 compared to the current fee of US $43,000. Issuing authorities should make their own calculations. They should also consider that the citizens and holders of an ePassport want to make use of their new document and are looking for fast, easy, reliable and hassle free border controls. In my opinion, the PKD is a valuable contribution to the pay back to citizens and taxpayers for the investment made in ePassports.

The PKD is not only the designated tool to distribute the certificates, including the revocations list, it is the instrument that guarantees the compliance of the distributed and therefore available certificates to Doc 9303. The built-in conformity checking engine checks every certificate forwarded to the PKD for publication. Should an inconsistency occur, the issuer will be contacted immediately allowing him to stop the production of a non-conformant certificate. Non-conformant certificates will be detected in properly set up border controls and cause problems for the holders of these ePassports. By assuring the conformity and origin of the certificate worldwide, verification of the travel document and trouble free travels are facilitated. Since the production of non-conformant ePassports can't always be avoided, ePassports with these certificates will be presented at borders for inspection. These certificates will therefore also be published and made available for border control use. Like the conformant certificates, the non-conformant certificates are also available for public download at: **https://pkddownloadth.icao.int/ICAO/pkdLDIFDownload.jsp.**

In my opinion, border control authorities should be interested in the PKD. They must protect the country's borders in a reliable, cost effective and fast way living up to citizens' and travellers' expectations for facilitation and security. Issuing authorities' interests in the PKD are to support the worldwide recognition of a nation's ePassport, allowing its citizens to cross borders as easily as possible. It doesn't matter which authority of a country joins the PKD. The most important fact is the new challenges that come with ePassport are well accounted for.

So far I have only mentioned government agencies. But PKD use is in principle also open to other parties that need to check travel documents, especially airline or ground handling agents mandated by airlines. There are already basic mechanisms in place to allow private companies that have a proven need to check documents to access the PKD. But there is still work ahead and the process and workflows must be defined in the next month. The PKD Board will work on this issue and hopefully I will soon be in a position to inform the interested parties. ■

Principled Secure Solutions Since 1897

More than 80 nations have engaged CBN as their partner for:

- Travel Documents
- National ID
- Driver Licences
- Civil Registry Documents
- Document Issuing Systems
- Border Management Systems

Through a consultative approach, we develop and deliver tailored solutions that address the unique challenges encountered by our customers.

www.cbnco.com
identification@cbnco.com

cbn
CANADIAN
BANK NOTE
COMPANY, LIMITED

IDENTITY FRAUD PUTS PRINCIPLE OF TRUST UNDER PRESSURE *What can be done about it?*

ABOUT FONS KNOPJES
He is managing partner of IDManagement Centre. He is a member of the United Nations' core group of experts on identity-related crime and of the International Association of Identification. He has both developed and taught various national and international training courses focusing on identity management and was responsible in an advisory capacity for the successful development and implementation of travel documents for various countries, including the renowned Dutch travel documents.

The Publisher Keesing Reference Systems B.V. grants herewith permission to republish the work, Identity Fraud Puts Principle of Trust under Pressure, by author Fons Knopjes published in the Keesing Journal of Documents & Identity, Annual Report Identity Management 2012-2013, Amsterdam, The Netherlands. Reprinted by permission of the publisher. All rights reserved.

Effective and lawful interaction between the government and its citizens is dependent on the government knowing its citizens' identities. This is conditional upon the careful establishment of certain identity data. It is the government's job to keep and manage good and reliable population records, a duty expressly set out in the United Nations' 1959 Declaration of the Rights of the Child. Reliable population records are a fundamental condition and an effective tool for verifying the identity of a person trying to commit identity fraud. Citizens must be able to trust that identity documents issued by a government contain the correct data and are issued to the person entitled to them. This so-called principle of trust forms the foundation for reliable dealings in the public and private sector, as Fons Knopjes, Managing Partner of IDManagement Centre, explains in this article.

THE (SOCIAL) IMPORTANCE OF HAVING A RELIABLE IDENTITY

In a small scale, closed and static society there is no need for personal data registration and data exchange. However, in a society such as the one we currently live in, which is characterised by its large scale anonymity and mobility, an orderly social and economic life is dependent on the processing of data. Citizens must be able to trust that identity documents issued by a government contain the correct data and are issued to the person entitled to them. This so-called principle of trust forms the foundation for reliable dealings in the public and private sector.

With the electronic highway increasingly being used for communication, citizens also have a growing need for a reliable digital identity. To address this need, some governments are already providing their citizens with a reliable digital identity and are issuing electronic identity cards. Every citizen is building a virtual identity and it has to be possible to locate this identity somewhere within a defined organisation. This is not just about public systems, it is about a complex whole of public and private systems that may or may not be connected to the Web or to one another via the Web. **Case: Consequences of Identity Fraud** describes the possible consequences when someone's identity document and identity are stolen.

THE ROLE OF THE GOVERNMENT

Traditionally the government has been the keeper of its citizens' identity. It provides each citizen with his or her identity by establishing and registering it, managing it and issuing them with a reliable identity document.

The United Nations (UN) has published guidelines and recommendations for setting up population records. In addition to principles for compulsory registration, universality and confidentiality of the data, it set out what legal and administrative frameworks exist to safeguard the reliability and integrity of the data. There are also various (UN) guidelines and recommendations setting out what information should be included in a register.

CASE: CONSEQUENCES OF IDENTITY FRAUD

Gordon, a 22-year-old student, applies to the local authorities for a new passport. He completes his application form and submits it along with a photograph and his application is accepted for processing. Gordon is told he can collect his passport from the local authorities in a week's time. At a central government site, Gordon's personal details are entered in a passport and the document is dispatched to the local authorities by secure transport. During this transport Gordon's passport is stolen. The police inform the local authorities that the passport has been stolen but neither the police nor the local authorities inform Gordon of the passport theft. The municipal authorities immediately apply for a new passport for Gordon and let him know that his document will be available several days later than expected but do not explain the reason for this.

About a year after Gordon has collected his passport from the local authorities, he receives a letter from a rental company asking him when he will be returning the cherry picker he hired (at a cost of €25,000). Gordon never hired a cherry picker and reports the matter to the police. At the police station, it turns out that the rental firm has reported the misappropriation of a cherry picker. Gordon tells the police that he has never hired a cherry picker and there must be a misunderstanding. On reporting the case, the rental firm provided the police with a copy of the renter's passport and this is a copy of Gordon's passport. The police launch an investigation into the case. After some time, Gordon is summoned by the police and told that more cases have been reported to the police and that he is under suspicion of embezzling various goods, including a cherry picker and that a criminal investigation is to be launched against him. Gordon is dismayed and tells the police that he wants to report an offence because someone is misusing his passport and identity. At this point, the police make it clear that Gordon is unable to report such an offence because the passport is 'the property of the state'. The police investigation reveals that Gordon's name has been used to set up a company which is registered with the Chamber of Commerce. This company has hired business premises and acquired goods. However, Gordon knows nothing about any of this and goes to the Chamber of Commerce to explain that someone is making unauthorised use of his passport and identity and that he has never registered a company. When Gordon's case comes up in court, he is able to persuade the judge of his innocence. He is acquitted and the case appears closed. However, when after the court case, Gordon continues to receive letters from companies making claims against him, he decides to go to the Chamber of Commerce to ask that the company registered in his name be taken off the records. The Chamber of Commerce tells Gordon that he is not authorised to deregister a company that he has not registered. This means that the company simply continues to exist. Gordon receives more and more claims and is registered as a defaulter and a criminal on various systems. The fact that no one seems to want to help Gordon causes him to become mentally confused. Highly insecure and depressed, he drops out of college, gets into financial trouble and becomes socially isolated.

Several years later, Gordon takes his case to the European Ombudsman, which investigates complaints about maladministration in the institutions and bodies of the European Union. It emerges from the ombudsman's investigation that four government bodies and the postal service were parties in Gordon's investigation. It also emerges that the various bodies failed to provide Gordon with accurate and timely information, that police knowledge of identity fraud leaves something to be desired, that the Chamber of Commerce failed to check the number of the passport properly (the stolen passport had been registered on the database) and that when Gordon called on the government for help he kept being passed from pillar to post. Real help was all but non-existent.

The Ombudsman has concluded that:

- the government is not sufficiently aware of the risks of identity fraud within the government itself, at companies and among citizens;
- inspectors have insufficient access to information regarding stolen documents;
- too little is done to track down users of false identity documents;
- there is a potential conflict between providing swift service to citizens on the one hand and careful checking for identity fraud on the other.

Thanks to the Ombudsman's investigation Gordon's life has reverted to normal again.

The case described is a real life case. In the interests of readability, the name of the individual and certain details were changed.

A Dutch investigation revealed that 7% of fingerprints…are linked to more than one identity.

Population records are used as a basis for issuing documents including so-called BMD (Birth, Marriage and Death) source documents. Unfortunately there are no (international) agreements concerning the standards source documents must comply with. The absence of such standards means that source documents are issued in a great number of varieties. This makes reliable checking of these documents virtually impossible and opens the door to identity fraud.

The use of new technologies is creating an increasing volume of data about people: biometric data derived from standard passport photographs, but also DNA and data generated by phone and computer usage. In relation to the application of new technologies in particular the search is on to find new ways of enabling government transparency. In many countries, the range of legal tools for protecting virtual identity is (still) inadequate or lacking altogether.

REGISTRATION ERRORS AND THE CONSEQUENCES FOR CITIZENS

Registration errors can be the result of administrative mistakes or deliberate deception. Civil servants who are responsible for population records have to be professionals who perform their duties with the utmost care. In today's world, birth registrations are increasingly being joined by registrations of people born in another country. A person born in another country is entered in the population records based on the documents provided. The question is whether the civil servant is familiar with these documents and is clear about the way in which the names and birth details appear on a source or other document. In practice, it emerges that name law varies considerably from country to country and so the registration officer may do things differently from how they are done in the country of origin. This means that when a person is asked for his/her identity data, he/she may provide data that differ from those in the registration. The same can happen with the registration of the date of birth.

When a date of birth is unclear, a protocol is often applied. This may also result in a person providing different data from those stated in the registration. While it goes without saying that care is of the utmost importance, in this type of situation, where there is no question of intent, we cannot speak of identity fraud. Because identity data from a registration are often subsequently used by many different parties it can happen that errors in a registration are inadvertently passed on to information users. Errors at the beginning of a process work their way through the rest of the chain. Any errors discovered in a registration must be investigated in detail and corrected. In practice, it turns out that correcting identity details is no easy matter and in many cases very time-consuming. Furthermore authorities often do not know how to correct information in the systems and so the inaccurate information continues to be used.

A Dutch investigation revealed that 7% of fingerprints held by the police are linked to more than one identity. Fingerprints have to be linked to an administrative identity. However, if there is no absolute certainty about the identity of the person whose fingerprints have been taken, this must be stated in the registration so that anyone verifying them realises that the identity details linked to the fingerprints may not be accurate.

CRIMINALS

Of course, there are also people for whom correct registration of their identity details is not in their interests. Criminals frequently use alternative identity details. If a criminal succeeds in tricking the police with incorrect identity details their criminal record will be created against a different name. Criminals have no interest whatsoever in assisting with the accuracy of their own criminal record. The result of this can be that someone who has never been in any trouble with the police (wrongfully) gets a criminal record against his/her name. This can have far-reaching consequences, as described in **Misuse of Identity Records**.

DOCUMENT AND IDENTITY FRAUD

Most fraud is currently committed in the physical world where checks are not always equally effective. But fraud is also subject to change. For example, in the past few years we have seen a drop in document fraud (fraud involving ID documents). In order to prevent this type of fraud, the document application and issuing process has been improved and there is an ongoing focus on document quality. However unlike document fraud, identity fraud is a growing phenomenon. Research conducted in Europe revealed that 20% of countries have specific legislation for dealing with identity fraud. Tackling identity fraud is more problematic in countries that have no such specific legislation. Combating this type of fraud is a spearhead of government policy in many countries, primarily because failure to take effective action against identity fraud undermines social and economic confidence.

MISUSE OF IDENTITY RECORDS

A criminal drug addict misused another person's identity for years. For many years, the person whose identity was being misused was wrongfully registered on the government's information systems as a drug criminal. When the citizen whose identity was being misused reported this to the government, the government did not succeed in removing the references to drugs, crimes and other criminal offences from its systems. When travelling, the citizen ran into trouble at airports because the systems had him down as a criminal. He was regularly apprehended by the police for non-payment of fines. All these incidents arising from errors entered into the systems prevented the citizen from leading a normal life.

VICTIMS OF IDENTITY FRAUD

Identity fraud and incorrect registrations often only come to light when the person concerned is confronted with the consequences, for example in the shape of fines or debt collectors. Often a lot has already happened by this stage, with information on various systems having been linked and exchanged. It is unclear what information was wrongly recorded or wrongly linked. The lack of transparency makes it extremely complicated and, in some cases, even impossible for a victim to reconstruct what went wrong. It is characteristic of identity fraud that the victim (the person whose identity is being misused) is often seen as the perpetrator. In cases of identity fraud, the burden of proof tends to lie with the citizen whose identity is being misused. The victim has to prove that he/she has done nothing wrong. It goes without saying that it is extremely difficult, if not impossible, for a victim to prove that he/she hasn't done something. Identity fraud has a huge impact on a victim's life. It is more than just a legal and technical issue, it has a major impact on a person's privacy. The nature of the issue means that some people may even end up with serious psychological and/or financial problems.

WHAT CAN BE DONE?

Better information about identity fraud is crucial. Because identity fraud frequently involves several parties, good coordination is needed in tackling it. Victims are often sent from pillar to post and feel misunderstood. In many cases, the consequences of identity fraud are very serious. We need to think about the conditions under which the burden of proof should be reversed in the case of identity fraud, giving the government with all its various levels and in all its complexity the active obligation to provide transparency regarding the information on a citizen it has collected, updated and stored as well as shared with other bodies.

It would appear that the division of roles is less clear in the digital world, with private companies as well as governments being involved in reliable identity verification in the digital domain. Does this development create opportunities or does it present risks? To what extent can the role of the government as the custodian of the identity infrastructure still be taken for granted? Should the government take regulatory action to protect its citizens against these developments in the private domain? Interesting questions to which there are no clear answers yet.

Expectations are that fraud involving identity data will increasingly manifest itself in the digital environment. Governments need to develop a vision and strategy aimed at tackling identity fraud—extending also to the digital environment. At the end of the day, identity fraud is a form of crime that cannot be stopped by borders and this means that international agreements will be needed on how to tackle it. ■

SMARTRAC

YOUR LEADING RFID
TRANSPONDER MANUFACTURER.

e-driver's licenses e-social security cards e-permanent resident cards
e-passports e-visa documents e-health cards e-national ID cards

e-ID@smartrac-group.com www.smartrac-group.com

WORKING TO SOLVE THE PASSPORT PROBLEM

Collaboration between psychologists and Australia Passports seeks to improve face verification accuracy

ABOUT DAVID WHITE

He is a Postdoctoral Research Fellow at the University of New South Wales. His primary research interest is human face recognition, although he has worked on a number of applied and theoretical problems related to visual cognition. These include distinctiveness and category membership in package design and individual differences in facial image comparison. Currently, he collaborates with Australia Passports to improve the effectiveness of facial image comparison training and FR workflow practices.

ABOUT SHASHI SAMPRATHI

He works with the Australian Passport Office, Department of Foreign Affairs and Trade in the Facial Recognition Unit. He has been with the Australian Government over a decade working with various agencies such as the Department of Immigration and Citizenship and Australian Customs and Border Protection Service. He has mainly worked in the identity management/security area for over 10 years including several years on biometrics. He is a member of the International Organization for Standardization (ISO) Sub Committee 37 – Biometrics Working Group.

ABOUT MICHAEL MATHESON

He works with the Australian Passport Office, Department of Foreign Affairs and Trade in the Facial Recognition Unit. He has been working in the biometrics area for nearly nine years. With a background in software development, he has worked on passport workflow for a number of years. Michael is a member of the International Organization for Standardization (ISO) Sub Committee 37 – Biometrics Working Group.

ABOUT RICHARD KEMP

He is Associate Professor of Forensic Psychology and Director of the Masters of Forensic Psychology program at the University of New South Wales. He undertakes applied research, particularly focusing on the applications of psychological knowledge to legal issues. Recent research topics have included the detection of fraud in passport applications, eyewitness memory and expert evidence.

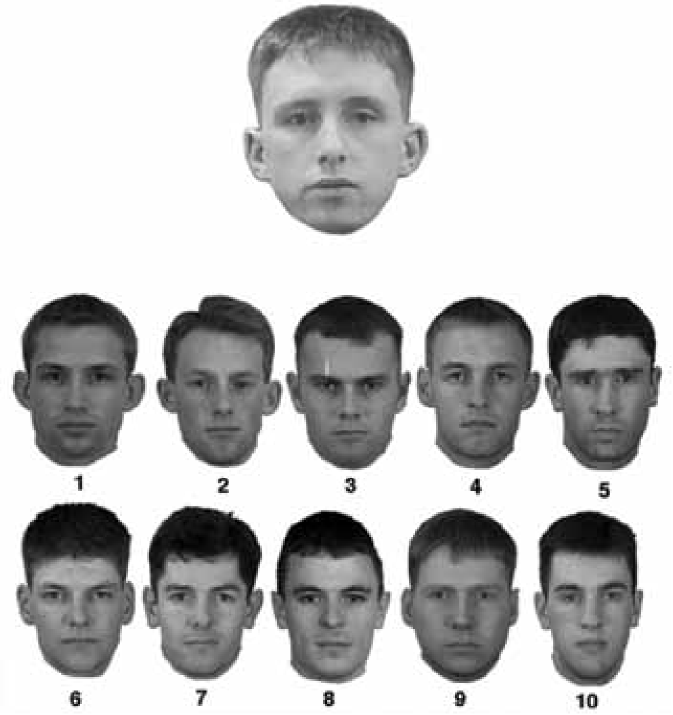
For the last few years, experimental psychologists David White and Richard Kemp from the University of New South Wales in Sydney, Australia have been working in partnership with Michael Matheson and Shashi Samprathi of the Australian Passport Office (APO). The objective of this collaboration is improve the ability of APO staff to detect potential identity fraud in passport applications by undertaking scientific research into unfamiliar face processing and using the findings to inform changes to passport application processing systems, training and staff development. In this article, they briefly describe the background to this collaboration and give some examples of early research findings and how these have informed changes at the APO.

In 2007, ICAO chose facial images as the Primary Biometric Identifier for use in ePassport documents. The ICAO Secretariat gave a number of compelling reasons for its decision. First, the facial image is a culturally accepted biometric that is less intrusive than alternatives. Second, the facial image has been used to identify people for a great many years and so the face affords continuity with legacy data. Finally, the ICAO Secretariat submitted:

> *Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.* (MRTD Report, 2 (1), p 16)

It is reassuring that ICAO considered the case of human identity verification in making its decision, given that humans are regularly required to verify identity from facial images in passport documents. However, although this might be a familiar task, the scientific literature tells us that human identity verification from facial images is difficult and error prone and less accurate than our intuition might have us believe.

Psychological research has established that people are surprisingly bad at identity verification tasks involving images of unfamiliar faces. This result has been replicated in a number of different conditions—both in 'live' simulations where a photograph is compared to a person, and in computer-based



In this 1-in-10 face matching task, people are asked to decide if the person shown at the top may or may not be one of the 10 below. Participants must decide if that person is present and, if so, which one he is. (Find out the answer in Acknowledgments.)

tasks where photographs are compared to one another. Even in optimal conditions, where images are taken on the same day and under similar lighting conditions, people typically make errors between 10% and 30%. (Refer to **Five Facts About Human Facial Image Comparison**). They refer to this as the Passport Problem.

One solution to the Passport Problem might be to replace human viewers with Automatic Face Recognition (AFR) systems and this has begun to happen in border control. However, while there have been significant improvements in the accuracy of AFR technology, it is still not perfect and the technology is only used to assist human operators. The net result is that staff is still required to make difficult facial image decisions.

Indeed, in some settings the introduction of AFR has increased the difficulty of the decisions made by humans, since only the most challenging face matching decisions cascade to their workstations. Whilst AFR technology might lessen the workload of humans at border control, this same technology has actually increased the burden in many instances, such as passport issuance. This is because AFR is able to search for duplicity in the passport system, returning arrays of very similar images which the human operator is then required to process. (Refer to **Human Face Matching Research Partnership Between the University of New South Wales and the Australian Passport Office**).

The collaboration between the Australian Passport Office and the University of New South Wales (supported by funding from the Australian Research Council) is aimed at improving human accuracy on face matching tasks. Given the extensive research and development work that has gone into the development of the latest AFR systems, it is perhaps surprising that this collaboration represents some of the first work designed to improve human verification.

Early indications suggest that research into human facial image comparison can provide substantial boosts to the accuracy of identity verification procedures. For example, they now know that there are large and stable individual differences in performance on this task. Some individuals perform very well making few errors, while others do not. Together with colleagues from Scotland, David White developed a standardised test of face matching performance called the Glasgow Face Matching Test (GFMT). The team has been using the GFMT to investigate these individual differences and the effect of training on performance. One objective for their work over the next few years is to develop a new generation of evidence-based tests which could be used to select staff on the basis of their ability on face verification tasks.

One reason for the poor performance in face verification tasks might relate to feedback. In general, humans improve performance in a task when they receive clear and direct feedback. One problem with face verification is that operators don't normally receive any feedback at all. In their research, they have found that they can significantly improve performance on verification tasks by giving training in the form of response feedback. The next step for this research is to test the longevity of feedback effects and determine how often they need to 'top-up' the training to maintain the benefit.

FIVE FACTS ABOUT HUMAN FACIAL IMAGE COMPARISON

1. Identity verification from facial images is harder and less accurate than most people realise.
2. Some people are much better at this task than others. It may be possible to select staff on this basis.
3. Facial image comparison is especially poor when comparing faces of different ethnicity to our own.
4. Unfamiliar face matching accuracy is greatly reduced by changes due to aging, lighting, camera and viewpoint.
5. Face matching is trivial with familiar faces—in this case matching is unaffected by superficial changes.

The research team runs lab-based studies with a passport Face Recognition workflow simulation.

> ...research has established that people are surprisingly bad at identity verification tasks involving images of unfamiliar faces.

They have also identified other successful training techniques. Based on their understanding of differences in the way people process familiar and unfamiliar faces, they predicted that they could improve performance by encouraging people to attend to the internal features (eyes, nose, mouth, etc.) rather than the external features (face shape, hair) of the face. Their studies have confirmed this hypothesis with a simple internal feature training programme resulting in modest but significant improvements in performance.

The team is aware of various facial verification training programmes developed by agencies around the world, but there is little or no evidence that these programmes are effective. They are keen to work with agencies to discover which elements of the training contribute to any improvement in performance. One of their PhD students, Alice Towler, is working on this question and they would be happy to work with any agencies who would like them to evaluate their training in this way.

The exciting challenge facing the team in the coming years is to discover how best to translate their laboratory research into changes in policy and practice at the Australia Passport Office and other similar agencies around the world. In this way, they hope that this research will help to solve the Passport Problem.

Space limitations mean that they can only outline some of their research here, but the team hopes that they have been able to show the benefits of the partnership between experimental psychology and government agencies using facial verification systems. They hope that this might encourage similar collaborations and they invite agencies to contact them if they wish to learn more about their work.

ACKNOWLEDGEMENTS

This research was supported by Australian Research Council grants to Richard Kemp (LX0083067 & LP110100448).
On request, the authors can supply references for the results discussed in the article. Contact David White at david.white@unsw.edu.au. Answer to the face matching task: the person shown at the top is not one of the 10 faces. ■

HUMAN FACE MATCHING RESEARCH PARTNERSHIP BETWEEN THE UNIVERSITY OF NEW SOUTH WALES AND THE AUSTRALIAN PASSPORT OFFICE

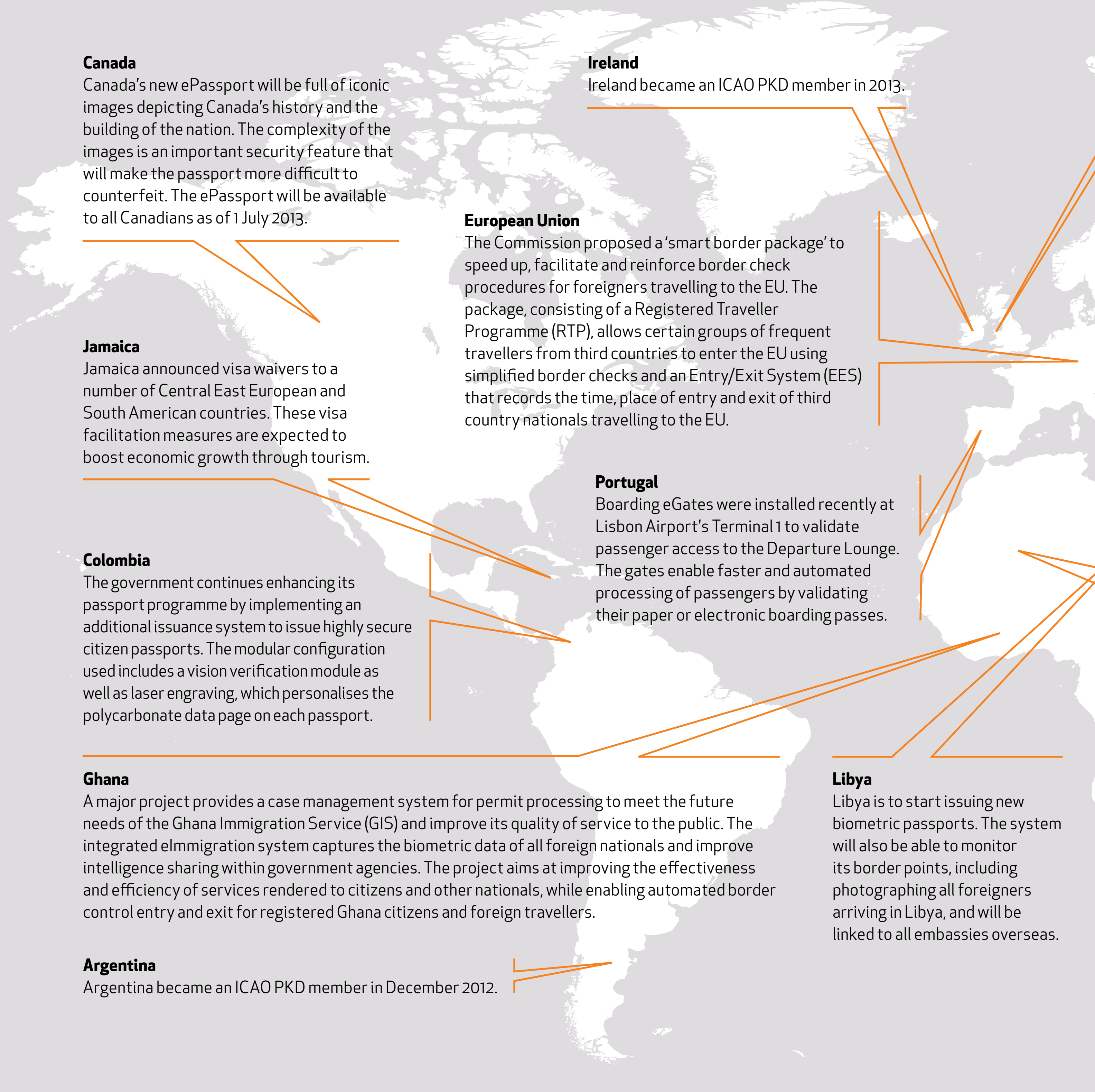
The research partnership between the APO and UNSW has already had a significant effect on the policy decisions made by the Australia Passport Office. APO has made significant changes to its Face Recognition (FR) training strategy and has also made several changes to the passport workflow and established a dedicated Identity Resolution Unit to resolve difficult identities. The new processes include providing feedback to operators about facial recognition outcomes which have improved staff performance in facial matching. APO continues to work with the UNSW to address current challenges including facial matching of aged images, effect of ageing on facial comparison decisions and the modification of FR training methods. The research collaboration has been very beneficial for the APO. Through the recently established Facial Biometric Centre of Expertise (FABCoE), APO will share the research outcomes with partner agencies nationally and internationally.

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

OVD Kinegram AG | Member of the KURZ Group | Zählerweg 12 | CH-6301 Zug | Switzerland
Tel. +41 41 724 47 00 | Fax +41 41 724 49 11 | mail@kinegram.com | www.kinegram.com

KINEGRAM

MRTD AND BORDER CONTROL NEWS



Canada
Canada's new ePassport will be full of iconic images depicting Canada's history and the building of the nation. The complexity of the images is an important security feature that will make the passport more difficult to counterfeit. The ePassport will be available to all Canadians as of 1 July 2013.

Jamaica
Jamaica announced visa waivers to a number of Central East European and South American countries. These visa facilitation measures are expected to boost economic growth through tourism.

Colombia
The government continues enhancing its passport programme by implementing an additional issuance system to issue highly secure citizen passports. The modular configuration used includes a vision verification module as well as laser engraving, which personalises the polycarbonate data page on each passport.

Ireland
Ireland became an ICAO PKD member in 2013.

European Union
The Commission proposed a 'smart border package' to speed up, facilitate and reinforce border check procedures for foreigners travelling to the EU. The package, consisting of a Registered Traveller Programme (RTP), allows certain groups of frequent travellers from third countries to enter the EU using simplified border checks and an Entry/Exit System (EES) that records the time, place of entry and exit of third country nationals travelling to the EU.

Portugal
Boarding eGates were installed recently at Lisbon Airport's Terminal 1 to validate passenger access to the Departure Lounge. The gates enable faster and automated processing of passengers by validating their paper or electronic boarding passes.

Ghana
A major project provides a case management system for permit processing to meet the future needs of the Ghana Immigration Service (GIS) and improve its quality of service to the public. The integrated eImmigration system captures the biometric data of all foreign nationals and improve intelligence sharing within government agencies. The project aims at improving the effectiveness and efficiency of services rendered to citizens and other nationals, while enabling automated border control entry and exit for registered Ghana citizens and foreign travellers.

Libya
Libya is to start issuing new biometric passports. The system will also be able to monitor its border points, including photographing all foreigners arriving in Libya, and will be linked to all embassies overseas.

Argentina
Argentina became an ICAO PKD member in December 2012.

United Kingdom
The UK government has launched consultations on new legislation aimed at stopping the supply of security printing equipment and materials to fraudsters.

Afghanistan
The Ministry of Interior started issuing for the first ever machine-readable ordinary passports and visas. A major technical assistance project was funded by the Australian government.

Ukraine
Ukraine's State Migration Service plans to complete all the work required to issue biometric passports by 2016.

Mongolia
Paving the way for new eGovernment services, Mongolia is to start issuing secure multi-service eID cards for its national ID programme. The new eID will contain biometric personal data, including the holder's digital photograph and fingerprints.

Thailand
Thailand became an ICAO PKD member in 2013.

Hong Kong
Stamping visitors' passports was recently abolished. All arriving visitors at immigration control points will be issued secure landing slips instead. The slip bears the visitor's English name, travel document number, arrival date, conditions and limit of stay in Hong Kong. Non-stamping immigration clearance is expected to improve services to visitors and facilitate the smooth flow of passengers at immigration control points.

West Africa
The West Africa Police Information System (WAPIS) is being developed by the EU alongside Interpol and the Economic Community of West African States (ECOWAS). WAPIS will facilitate the collection, management, analysis and sharing of police information on a national, regional and global level to more effectively tackle crime such as drug trafficking, illegal immigration, money laundering and weapons trafficking in West Africa. Immigration and customs will join soon.

Macao
The Macao Special Administrative Region of the People's Republic of China started introducing new generation multifunctional smart ID cards from October 2012. Security of the contactless data transfer is assured using the PACE (Password Authenticated Connection Establishment) security protocol developed by Germany's Federal Office for Information Security (BSI). Personal data and biometric features such as the holder's photo and fingerprints are stored securely on the chip in digital form.

Maldives
The Maldives started a major border capacity building project funded by the US government. The initiative provides a new border control system, training of personnel and maintenance of the system.

Malaysia
Malaysia became an ICAO PKD member in November 2012.

THE CHALLENGES AND ADVANTAGES OF ELECTRONIC TRAVEL DOCUMENTS

ABOUT CHRISTOPHER HORNEK
He was programme manager for Travel Document Security in the OSCE Transnational Threats Department/Action against Terrorism Unit (TNTD/ATU). With 10 years' experience in identity management practices, travel document security standards and border inspection techniques, he was responsible for developing the 2009 OSCE Ministerial Council Decision promoting the ICAO Public Key Directory. He has recently assumed the position of Project Co-ordinator in the OSCE Centre in Ashgabat, Turkmenistan (www.osce.org/ashgabat).

ABOUT PAUL PICARD
He joined the OSCE Transnational Threats Department in 2012 and manages the Travel Document Security programme. He worked previously with the OSCE in Tajikistan designing and delivering comprehensive tactical training programmes for border officials deployed on both sides of the Afghan/Tajik border and held various positions in Afghanistan and the Balkans.

The Action against Terrorism Unit of the Organization for Security and Co-operation in Europe (OSCE) Transnational Threats Department has developed a comprehensive programme on Travel Document Security (TDS). In this article, Christopher Hornek and Paul Picard, of the TDS programme, outline the rudiments of the programme, the workshops and seminars conducted in Central Asia and the OSCE's strategic goals to strengthen identity management and border control.

The TDS programme was initiated by OSCE participating States to prevent terrorist movement through the development of law enforcement tools that would address in a comprehensive manner concerns related to terrorism, policing and border management and fight other transnational threats such as illegal migration and illicit trafficking in all its forms. It comprises several interrelated components that promote the security of identities, documents and borders.

To help secure identities, the OSCE seeks to improve the documents, civil and population registration systems and other methods and processes used to verify and/or validate a citizen's identity during the travel document application process. Ensuring respect for human rights and the rule of law is an indispensable element in our work on securing identities.

To promote document security and commensurate border inspection, the OSCE supports the introduction by its participating States of electronic Machine Readable Travel Documents (eMRTDs) with biometric identifiers and their participation in the ICAO Public Key Directory (PKD), a vital tool for border control as it allows effective validation of the authenticity of electronic security features and biometric data stored in electronic travel documents.

To strengthen border security the OSCE facilitates access by its participating States to passport control databases, including the INTERPOL database for Stolen/Lost Travel Documents (SLTD), thereby enhancing border management systems in order to better capture, verify, share and analyse information on cross-border movements.

While new technologies are being increasingly used in travel and identity documents, in many OSCE participating States the capacities at the border for machine-assisted inspection still lag behind. The OSCE helps the countries to address this through technical assistance projects that modernise equipment, as well as by training border officers on identifying forged documents with the use of basic forensic tools.

ELECTRONIC TRAVEL DOCUMENTS: THE OSCE'S STRATEGIC GOALS

With a view to the future of travel documents, the OSCE has two clear strategic goals: strengthening identity management and bringing border control up to the speed of biometrically enabled travel documents.

IDENTITY MANAGEMENT

With the introduction of eMRTDs, the physical security of travel documents has noticeably increased. Moreover, through the proper use of Public Key Infrastructure the electronic, biographic and biometric data contained on electronically enabled travel documents can be validated with essentially 100% assurance of authenticity. Due to this 'lockdown' on the document, individuals or groups who want to use travel documents for terrorist activities or other illegal purposes apply for legitimate documents under false identities and pretences. The acquisition of false identities, through either deceit or corruption, is an underlying threat to all travel document issuing systems.

Another important negative factor in this area that the OSCE has witnessed is the *de novo* introduction of electronic passports without integration with or use of identity management data from existing passport issuing databases. This widely spread disconnect between passport systems exposes a newly introduced ePassport to vulnerabilities that can weaken identity management and border security. Therefore, when implementing an ePassport programme, a government should consider wider strategic concerns and take due account of the needs and requirements of all the various agencies and ministries involved in issuing and inspecting travel documents.

Almost every day we need to verify our identity for purposes other than travel. Claiming and establishing one's identity has become an ubiquitous task and one that will only grow, especially in cyberspace. To accommodate wider implications of the development of identity management systems and identity/travel documents, we work closely with the OSCE Office for Democratic Institutions and Human Rights (ODIHR) to promote a comprehensive approach to identity management, an approach that would incorporate human rights aspects into anti-terrorism work. ODIHR has sound experience in this area as it has been managing a programme promoting freedom of movement and migration in the OSCE area.

Founded in 1994, IRIS, the inventor of the world's first ePassport and first multi-application eID card, has more than 18 years of experience as a technology innovator, leading provider of solutions and advancements for trusted identity. Our comprehensive solutions comprises of smart card manufacturing, ePassport inlay production, personalization and systems integration to secure document management system. IRIS is passionate about developing quality, innovative solutions that aim to add trust, simplicity and value to a growing portfolio of clients with diverse needs and concerns around the world.

Enquiries: marketing@iris.com.my
www.iris.com.my

IRIS®
Trusted IDentification

Enhance your visibility

The world's most trusted MRTD Web site

The **MRTD Partnership Community** is the only globally recognized Web site that can help you reach all of ICAO's Contracting States. Major industry experts in the MRTD, Border Control, Security and Facilitation field use our Web site to deliver their corporate message to key players in the MRTD community worldwide.

For more information on our comprehensive media package and marketing tools, visit us at:

ICAO • OACI • ИКАО

www.icao.int/mrtdc

At an OSCE/ICAO Assessment in Tajikistan in 2010, from left to right, Robin Chalmers, OSCE Consultant; Christopher Hornek, Project Co-ordinator, Ashgabat, OSCE; Erik Slavenas, Programme Officer, MRTD Programme, ICAO; Lina Rimsaite, Document Expert, Lithuanian Ministry of Internal Affairs; Oliver Janser, Counter-Terrorism and Police Adviser, OSCE Office, Tajikistan.

BRINGING BORDER CONTROL UP TO SPEED

Comprehensive border control promotes border security and facilitates cross-border movement, the two principles underlying the travel documents inspection process.

Centralising information about passport bearers and travel documents is an excellent means of modernising a country's travel document inspection processes, as it permits accessing this information and carrying out an inspection via one machine-assisted transaction. The border control officer is able to ensure the authenticity of the passport, conduct law enforcement and database checks and critically verify identity by matching the document to the bearer. The machine-assisted check ensures consistency and standardisation of the data being checked and recorded and makes control procedures faster and more comprehensive. In fact, border control in the 21st century will revolve around the inspection of the traveller and the accompanying eMRTD.

Currently, however, passport control procedures in many countries of the OSCE region are lagging behind the capabilities offered by electronic travel documents and border services still require much modernisation to catch up with the new technologies being deployed by ePassports. This situation is compounded by the fact that eMRTD technology itself is a moving target with continuous introduction of new technologies such as Supplemental Access Control (SAC) and Logical Data Structure (LDS) 2.0—to name just two. Not only does this impact some issuing agencies, which are misled as to what is a minimum requirement and what an optional security benefit is, but it also creates clear interoperability issues at the border.

PROMOTING THE ICAO PUBLIC KEY DIRECTORY

The 2009 OSCE Ministerial Council Decision No. 11 takes note of ICAO's work to develop the ICAO Public Key Directory (PKD), a globally interoperable validation system for eMRTDs that significantly improves border security measures and thereby contributes to counter-terrorism and to the prevention of illegal cross-border activities. The Decision also notes that it is an ICAO recommended practice that States issuing or intending to issue ePassports and/or implementing automated checks on ePassports at border controls should participate in the PKD. It also calls on the participating States to consider becoming participants in the ICAO PKD, subject to administrative and financial resources, and thereby contribute to enabling border control and other relevant national authorities to validate digital signatures of eMRTDs.

In early 2009, when the OSCE began its initiative to promote the ICAO PKD, only six OSCE participating States had signed up to the directory. Since then this number has jumped to 20 and four OSCE Partners for Co-operation have also joined. Nonetheless, only 37 countries out of more than 100 States issuing ePassports are currently participants of the PKD.

The OSCE tries to bridge this gap by organising workshops to promote understanding of the benefits of participation and the administrative, financial and technical aspects of the PKD. In addition to the May 2010 OSCE wide workshop co-organised with ICAO and attended by 200 participants, such capacity building events have been held in Uzbekistan, Moldova, Kyrgyzstan and Albania.

In addition to promoting participation in the ICAO PKD, the OSCE is also encouraging the use of the PKD to validate eMRTDs at the border as a precondition for an integrated travel document control. After the travel document has been established as genuine through PKD, further checks can be conducted using a number of tools. They include, but are not limited to, INTERPOL databases, exit/entry

Example of a hit being generated against INTERPOL databases by passport control at the Moldovan border.

Example of a weak identity management system due to it being decentralised and paper-based.

records, travel history, visa databases, traveller screening through Passenger Name Records (PNR) and Advance Passenger Information (API) and biometric verification to ensure that the document, the identity and the traveller all match.

TRAVEL DOCUMENT SECURITY PROGRAMME: WHAT HAS BEEN DONE?

Since 2003, the OSCE has organised more than 55 workshops, seminars, training courses and study visits in the area covered by the Travel Document Security programme. The geographic focus was on Central Asia and a strong partnership was established with the region. More than half of the projects were completed there with more than 800 out of a total number of 1,600 participants coming from Central Asia.

A flagship example is **Uzbekistan**, which hosted three events and sent more representatives to OSCE travel document security events than any other participating State of the OSCE. In 2010, the OSCE together with ICAO developed a set of recommendations to accompany the roll-out of Uzbekistan's electronic passport system. Based on the OSCE/ICAO report, we delivered legal, technical and policy advice for the introduction of Uzbekistan's ePassport, donated 32 passport enrolment stations for the Uzbekistan Interior Ministry and held a seminar on ICAO PKD issues.

From 2007 to 2010, the OSCE managed a project in **Moldova** that provided the country's Border Service with the hardware and web services to access INTERPOL databases in real-time. Initially, access was rolled out to 16 border control points—on the borders to Romania and the Ukraine and at the Chisinau and Iasi international airports—and 11 police stations. Subsequently the Moldovan authorities took ownership of the project and extended INTERPOL database access to 23 border control points. At the conclusion of the project, INTERPOL experts trained Moldovan border, customs and police officials in using the equipment to access the databases. To enhance integrated passport control, the OSCE donated more than 50 electronically enabled passport scanners to enable the Moldovan Border Service to use the ICAO PKD in practice through verifying digital signatures of electronic passports.

The Moldova project has proved very effective, with statistics indicating the number of queries from the Moldovan border is very high, both in absolute and proportional terms. Equally impressive is that Moldovan authorities have shared more than 460,000 domestic records with INTERPOL's SLTD database and more than 1,000 records with the Stolen Motor Vehicle (SMV) database. This enables border control officers throughout the world to flag Moldovan documents or vehicles due to criminal use.

Building on the momentum developed in Moldova and on the lessons learned from this country, the OSCE and INTERPOL designed similar projects for **Kyrgyzstan** and **Tajikistan** to connect border control points in each country to INTERPOL's databases. The project objectives in these two Central Asian countries, which share a long and complex border, also included the development of domestic databases and enhancing inter-agency cooperation between relevant agencies.

FORGED DOCUMENT TRAINING

Many OSCE participating States still lack proper equipment at the border to effectively inspect the growing volume of electronic passports in circulation. Thus passport control officials in many places in the OSCE region still have to resort to hand-held physical detection methods. The OSCE repeatedly received feedback from its participating States that their border control officers who do not have recourse to machine-assisted optical verification of document

WHAT IS THE OSCE?

With 57 participating States from Europe, Central Asia and North America, the Organization for Security and Co-operation in Europe (OSCE) is the largest regional security organisation in the world.

The OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation. It has 16 missions or field operations in South-eastern Europe, Eastern Europe, South Caucasus and Central Asia.

The organisation deals with three dimensions of security: the politico-military, the economic and environmental and the human dimension. It addresses a wide range of security related concerns, including arms control, confidence- and security-building measures, human rights, national minorities, democratisation, policing and counter-terrorism. All 57 participating States of the OSCE enjoy equal status and decisions are taken by consensus on a politically, but not legally binding basis.

security features are unable to keep track of newly designed document security elements, as well as new forgery methods.

To help address the issue, the OSCE implemented a training programme entitled, Increasing Operational Awareness to Detect Forged Documents, developed by the Austrian Federal Interior Ministry. Since September 2007, the OSCE ran this course 18 times, including for border officials from Afghanistan at the OSCE Border Management Staff College in Dushanbe, Tajikistan. The course material was subsequently adopted by Frontex as a European best practice.

Training on forged documents identification as part of the OSCE Travel Document Security programme was identified by the OSCE office in Skopje, Republic of Macedonia, and is jointly implemented by the OSCE Transnational Threats Department's Action against Terrorism and Borders Units. Officials from passport, customs, drug control and forensic authorities take part in the course to strengthen their operational and analytical capacities and gain necessary skills to detect forged documents. The training course typically lasts two weeks, but can be tailored to the needs of the beneficiary. Training modules cover such issues as document printing, document security features and document forgery methods as well as their means of identification. To enhance the practical skills of the trainees and encourage interaction between the trainers and the students, the OSCE donates basic forensic equipment to help participants identify forgeries. Through a competitive examination at the end of the course, promising students are identified who are in a position to further disseminate these skills as national trainers and to maintain an international cooperative network on exchanging the latest forgery trends and methods.

To further promote international cooperation on this important topic, the OSCE is stepping up its collaboration with the Joint Interagency Counter Trafficking Center of United States European Command, which works to counter the spread of narcotics and other global threats, such as terrorism.

CONCLUSION

Within its geographic remit, the OSCE will continue its efforts on the cutting edge of travel document security by further developing existing programmes and projects and by identifying innovative responses to challenges in important growth areas, such as identity management and bringing border control up to speed. The basis for this lies in the OSCE's role as a force multiplier to provide a platform where standards, expertise and donor contributions come together to help participating States of the OSCE better protect their citizens' identities and their borders. ■

Discover the innovation driver for ID management.

We believe that complex data systems and outstanding security can go hand in hand. As a leading high-security systems supplier, we can provide you with comprehensive ID management that reduces data to the minimum required, makes communication channels secure on all levels and ensures that both you and your customers can authenticate yourselves in a trustworthy manner on the net. Discover a system that is much more than just the sum of its parts: www.bundesdruckerei.de

BUNDESDRUCKEREI

UPCOMING 9th MRTD SYMPOSIUM

The 9th MRTD Symposium and Exhibition on MRTDs, Biometrics and Security Standards takes place in Montreal, Canada, on 22-24 October 2013. This important annual event will explore ICAO's role and mandate in MRTDs, biometrics and identification management. Policy level presentations will include an overview of the global regulatory framework, an update on the results of the 2013 ICAO Assembly and new strategic directions for the proposed ICAO Traveller Identification Programme (ICAO TRIP) for the 2014 to 2016 triennium.

The 2013 Symposium's special focus will feature Automated Border Controls (ABCs), its objectives, practices and challenges of developing related standards and specifications. A broad range of considerations shaping state-of-the-art ABC developments will be explored, such as newly emerging technologies, trust, reliability, non-intrusiveness, biometrics, use of the PKD, costs, privacy and human rights. Other specialised topics include security and facilitation considerations in ABCs and the relevance of ABCs to the aviation industry and sustainable economic development.

The following article, **Border Checks of the Future: Vision 2020**, presents Frontex's new border control paradigm for the future development and deployment of ABC systems at borders.

Other informative articles on ABCs will be featured in the Fall 2013 issue of the *MRTD Report*, which is distributed during the Symposium. ■

INNOVATIONS IN SECURITY
IDENTITY SOLUTIONS, SWISS MADE

Secure documents in polycarbonate
Passport datapage
Identity card
Residence permit
Crew member certificate
Driving licence
Tachograph cards

tru/window™ LOCK
A new dimension in
photo-protection

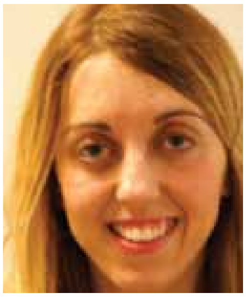
www.trueb.ch

Absolute Identity

TRÜB
SWITZERLAND

BORDER CHECKS OF THE FUTURE: VISION 2020

European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex)



ABOUT MARÍA DURO MANSILLA
She joined Frontex in October 2010. Her research interests include Automated Border Control systems, API/PNR, checks at land borders and ethical issues in relation to border controls. Previously she worked as a Policy Officer for the European Council on Refugees and Exiles on issues concerning European Union asylum and migration policies and for the European Commission Spokes person for Justice and Home Affairs.

ABOUT RASA KARBAUSKAITE
She joined Frontex RDU in 2006. She manages the Automated Border Control (ABC) project at Frontex and leads the ABC Working Group, which is tasked with the elaboration of best practice guidelines for ABC. Prior to joining Frontex, she worked at DePaul University (United States) on research projects related to US-Mexico migration and immigrants in the labour force.

ABOUT IGNACIO ZOZAYA
He joined Frontex as a Research Officer in January 2010. He has previously worked at The Boeing Company managing border security, homeland security and air traffic management research programmes. Previously he managed different projects in the space and telecommunications sectors. His areas of expertise and interest at Frontex involve Automated Border Control solutions, API/PNR systems, cost effectiveness analysis and breakthrough solutions for the facilitation of bona fide travellers.

The key dilemma of border management is balancing the growing numbers of travellers while maintaining security, explain María Duro Mansilla, Rasa Karbauskaite and Ignacio Zozaya of Frontex in this article. They present the rationale for a new border control paradigm that strikes a better balance between facilitation, security and cost effectiveness and outline a strategic vision for border checks of the future.

People are travelling more than ever before. Passenger forecasts estimate that by 2014 there will be 3.3 billion travellers worldwide only at airports—up by 800 million from 2.5 billion in 2009— and international passenger flows will continue to increase on average some 5% annually over the next 20 years, according to the IATA industry consensus forecast of 14 February 2011. This trend is here to stay and hence the pressure to process large volumes of people at the borders will also keep growing.

This is taking place against the backdrop of an unfavourable economic climate. In the European Union (EU), for example, a range of austerity measures has been introduced since 2009 and, alongside other public services, have reduced the resources available for border management. As a corollary to budget cuts, there is an increased vulnerability to cross-border illegal activities such as drug trafficking and trafficking in human beings, according to the Frontex Annual Risk Analysis 2012 (April 2012).

And herein lies the key dilemma of border management: how to balance the need to facilitate growing numbers of travellers at the border while at the same time maintaining security. Certainly, the traditional approach to border control, in which most travellers are to be checked at the border irrespective of the level of risk they present as individuals, is not sustainable in the long term. The ongoing trend towards increased mobility within a context of scarce human and material resources is resulting in massive congestion at international border crossing points, a problem that is bound to be exacerbated in the future. In addition, one-size-fits-all controls do not represent the most effective method to detect individuals who pose a genuine security risk at the border. There is a need for a new paradigm that better strikes a balance between facilitation, security and cost effectiveness.

AUTOMATED BORDER CONTROL AND NEW OPPORTUNITIES

The dual objective of facilitating travel and maintaining security requires the introduction of new approaches and solutions to border management. The use of electronic Machine Readable Travel Documents (eMRTDs) as the storage medium for traveller's personal data facilitates the introduction of automation in border control. The deployment of Automated Border Control (ABC) systems at a number of major airports in Europe and worldwide constitutes an integral part of this effort.

While the roll-out of ABC systems has expanded over recent years across countries and regions, it has so far taken place in a disconnected manner with different configurations and procedures in place. The variations in ABC processes may either discourage a traveller from using ABC or reduce the efficiency of ABC systems as envisioned. Global harmonisation and standardisation in terms of the technology used, operational requirements and user experience are the overarching factors of success. Furthermore, a coordinated and detailed exchange of experiences and lessons learned regarding the benefits and challenges of automation is crucial for the future development and deployment of ABC systems at the borders.

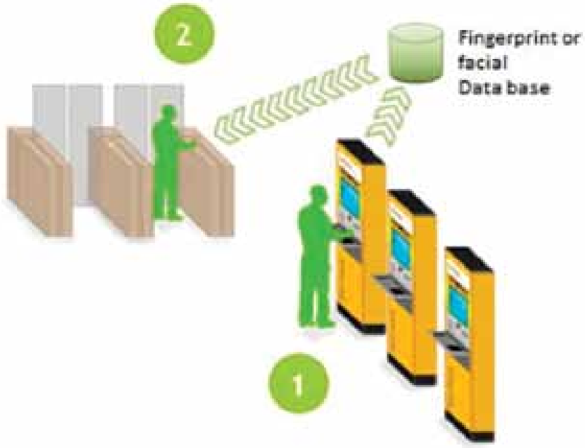
Frontex has undertaken a number of initiatives to promote end user driven harmonisation with a view to increase the efficiency and effectiveness of ABC at the external borders. The establishment of a Working Group on ABC, composed of experts from EU Member States' border management authorities, has been one of such initiatives and the outcome of this coordinated effort is the ABC Best Practice Guidelines Technical and Operational, Version 2.0, 31 August 2012. Furthermore, the October 2012 Global ABC Conference has been the first initiative on a global scale to foster discussion on harmonisation and interoperability needs for ABC solutions worldwide.

Yet, ABC is a point solution and as such cannot deliver end-to-end facilitation on its own. The integration of various facilitation initiatives into a broader border management concept of operations and their wide international roll-out are also prerequisites to providing additional facilitation opportunities. It is also important that facilitation initiatives are designed in a way so as to cater to as many travellers as possible, including not only a country's own citizens but also foreign nationals, travellers with special needs and other specific categories. Equally relevant is to

The Automated Border Control system at Helsinki Airport.

The Automated Border Control RAPID system at Portugal's Faro International Airport.

The Automated Border Control system at Heathrow Airport, Terminal 5.



The Automated Border Control two-step process.

Step 2 of the Automated Border Control two-step process.

EasyPASS at Frankfurt Airport, a two-step integrated process.

maximise levels of usage by making eligible travellers aware of existing solutions and of the advantages that they entail and by ensuring those solutions are easy to use and harmonised to the extent possible. Taking all these factors into consideration, Frontex has taken steps in developing a strategic vision of the 'Border Checks of the Future'.

BORDER CHECKS OF THE FUTURE: VISION 2020

In a 2020 vision, the main objective and, at the same time, the greatest challenge will be to decide whether an individual traveller is allowed to cross the border before arrival to the territory of the destination country. Therefore new mechanisms have to be put in place for identifying the traveller in a risk controlled manner. A more effective and efficient border checks process can be achieved by:

1. Verifying the traveller's identity in a reliable manner upon departure.
2. Carrying out checks in advance in order to identify low/high risk travellers.
3. Providing these travellers with facilitation along the travel process.

A first step will be to verify identity at the point of departure in a manner that is as reliable as the one carried out by a competent officer at the border. This can ideally take place as a supervised self-service, possibly integrated in the check-in process or in combination with security checks. Identity checks based on electronic passports and biometrics provide an excellent way of accomplishing this objective in a cost-effective and reliable manner.

The traveller's identity will then be used to carry out checks in advance in combination with other forms of advance information. In this manner, border management authorities will be able to verify whether the traveller meets entry criteria and carry out a tailored risk assessment in order to identify high risk travellers.

Most travellers will be allowed to cross the border and will benefit from the possibility of facilitated passage through biometric verification at ABC solutions. A minor fraction posing some interest to the authorities will first be required to meet a border officer upon arrival. There are more opportunities for facilitation and value added services that can be delivered using the same approach.

The benefits of this vision are far-reaching and can be summarised in the three main categories mentioned earlier: greater **facilitation** for the traveller, increased **security** for the border management authority and improved overall **cost effectiveness** for the relevant stakeholders involved.

The facilitation benefits for the traveller are quite straightforward: valuable time is saved, particularly if there is a connecting flight to be taken. On top of this, other services may be enjoyed, that contribute to a more satisfactory travel experience. Note that the facilitation benefit extends also to other travellers, as removing passengers from manual border control reduces queuing time at border crossing points.

Global harmonisation and standardisation in … the technology used, operational requirements and user experience are the overarching factors of success.

Security is also improved through different mechanisms. First, the automated authentication of the travel document and verification of the traveller's identity can be more reliable than a purely manual inspection. This is because the system makes extensive use of the embedded electronic chip and its many security features. Second, knowing reliably and early who is coming to the border gives the border management authority the possibility to devote more time to those travellers who may pose a higher security risk.

Lastly, each stakeholder involved can achieve greater cost effectiveness. The border management authority will save man-hours due to lower numbers of travellers manually processed and will be able to use resources more effectively. Carriers will incur less costs associated with sanctions and repatriation in case of rejection at the physical border since they are no longer responsible for checking travel documents and ascertaining identity. Providing the traveller with a positive travel experience is also crucial. Satisfied customers will tend to repeatedly choose those airports and carriers where they can benefit from the above advantages and will also have more time on their hands to spend in the commercial area before boarding, thus increasing revenue for the airport operator.

This vision for Border Checks of the Future is perfectly feasible from a business and technology perspective. However it has large implications to be addressed. It proposes not only changing the border checks process as we know it today, but more importantly changing the mindset of those decision makers who will ultimately decide how to face the future of cross-border travel. This can be achieved through cooperation and trust as well as leadership and planning. ■

STATE-OF-THE-ART TECHNOLOGY AND SOLUTIONS

Mühlbauer
High Tech International

- Use the advantages of the latest technology in government ID management
- Implement a national register that will contain all alpha numeric and biometric data as well as the complete document life cycle information
- Consolidate investments in infrastructure through the use of a systemized consolidation of all national identification and verification systems
- Increase national security with embedded and scalable applications, systems and solutions
- Integrate border control and national ID solutions and enable the seamless exchange of data
- From enrollment to identification / verification, Muehlbauer TECURITY® will enable you to manage the lifecycle of data comprehensively

Muehlbauer TECURITY® – state-of-the-art government ID management, issuance and verification solutions

www.muehlbauer.de

A RELIABLE DOCUMENT OF A STRONG COUNTRY
Issuance of the Russian ePassport

Reprinted by permission of the publisher: Reliable Document of Strong Country by Elena Kiseleva, which originally appeared in Watermark Digest, No.11/2012, *published by* Watermark Publishing House. *Copyright 2012. All rights reserved.*

In most countries, ordinary passports are being replaced by ones encrypted with biometric data. Russia wants to keep up with the times, however, ePassports only became the norm for Russians a short while ago. Aleksander Aksenov, Head of the Visa and Registration Department, Federal Migration Service of Russia, relates how that project developed, what problems they faced and what the citizens of Russia can expect in the future.

FINGERPRINTS AND PASSPORTS

Are passports of the next generation accepted by Russian citizens? Are there ways to strengthen biometric passports of the future?

Currently, ePassports are popular with the Russian people. At the moment, 71% of all issued passports are next generation with the percentage of ordinary passports decreasing annually. People understand it is more advantageous and convenient to get an ePassport as it is valid for 10 years—applications are made once every 10 years. In addition, the ePassport is well accepted by the world community as there have been no problems with it. The Russian ePassport is considered a reliable document of a strong country.

However, for some people, the price of ePassports is a deterrent as they cost considerably more than ordinary passports. If a person plans to make one trip and doesn't know when the next one will take place, he might apply for an ordinary passport rather than an ePassport. During the first half of 2012, about half a million ordinary passports were issued, but this number is constantly decreasing.

As for the future—like most countries of the world—we are working on increasing the security of passports by adding fingerprints.

NOW WE ARE DEVELOPING IN TWO WAYS

Several years ago, when we were at the transformational stage for passports and visas, a concept was devised. Documents with biometric data would include all types of international passports, including diplomatic and business passports, visas, refugee travel documents and residence permits for persons without citizenship—currently we are developing biometric documents for the latter two documents. Amendments to applicable legislation have already been developed and passed in a first reading. According to our forecast, 2013 will be the changeover year for new documents for foreigners with either 1 July 2013 or 1 January 2014 as the introduction date.

As for introducing fingerprints on ePassports, a decision was made to implement a pilot project. We developed a draft of the President's decree to announce the start of this pilot project and I believe the decree will be signed. The project's goal is to implement technologies that will be used all throughout Russia.

To initiate this pilot project, some of our branches located in Moscow, the Moscow region and Saint Petersburg were chosen. In these regions, a large number of people use the passport services offered and personnel qualifications and technological infrastructure are of a high calibre.

The main objective of the project is that Russia has to keep pace with the world community. Most countries already have electronic passports of the second generation (with fingerprints of the holder) and, from our point of view, we have to make progress, too, because it's a necessity.

How will fingerprints be captured?
We will follow Europe's example. Prints of the left and right index fingers will be captured by modern technology that scans a papillary picture so the hands remain clean and the fingerprints are stored on the chip of an ePassport. Once it has been checked that the fingerprints on the chip match the scanned fingerprints, all electronic data on these fingerprints are erased from all our databases.

The main reason for implementing fingerprints on documents is to raise the level of security. If a border guard is unsure about a person's identity—he could have grown a beard or become thinner or fatter—he can ask the traveller to put an index finger on the scanner, which will compare it to those on the chip. I want to reiterate that these fingerprints are not kept in any Russian databases.

However, fingerprints will be collected from all Russians but not for fighting crime. Law enforcement agents had envisioned such notions but we strongly refused to agree.

The most popular biometric data of a person include not only fingerprints but also iris recognition. Why were fingerprints chosen?
There are historical reasons. Fingerprints are the simplest way to identify a person biometrically. There are a lot of biometric markers and, of course, every country considers its own technological and financial resources, giving preference to one biometric parameter or another. In Russia, the experts who developed the idea of biometric data have concluded that, in our country, it would be more efficient to read fingerprints and we have agreed. Moreover, financially this project costs less as iris reading equipment costs more than fingerprint scanners.

The 10th million biometric passport was handed over to Pavel Kryukov, a Saint Petersburg citizen, by Elena Dunaeva, Head of the Department of the Federal Migration Service for the Saint Petersburg and Leningrad regions.

What if a passport becomes wet or burned on the edges?
Occasionally, when we didn't use a lamination membrane for passports, children damaged them by covering the photos with drawings or writing on the pages. Sometimes people were caught in a heavy rainfall with their passport or forgot it in a pocket and it got washed with their clothes. The pages became irregular and uneven and the stamps wore off. If the passport becomes unglued as a result of getting wet, both Russian and foreign border guards cannot allow that person to cross the border.

What do our ePassports look like compared to those of other countries?
The Russian Federation has developed ePassports more or less in the same way other countries have. In some countries, however, plastic pages are not used and a completely different technology employed. But all present day passports have one common feature: a chip with machine readable information to protect the ePassport from being forged.

Different countries also follow different distribution methods. Some issue ePassports locally, while some issue them centrally. We followed Germany's example, which, before our implementation, had instituted a central system. Compared to Russia, Germany is a small country that a car can crisscross in one day because of its excellent transportation infrastructure.

Regarding centralisation of ePassports, we are working on making the passport issuing process more convenient and efficient for our citizens. We need to find a solution to minimise the time for verifying all operational procedures. A current problem today is the inability to

> ...all present day passports have one common feature: a chip with machine readable information to protect the ePassport from being forged.

issue ePassports in three days for people who need to travel urgently. According to legislation, a citizen can obtain a passport in three days if there are force majeure circumstances. This problem remains unsolved and we are extensively looking for a solution—a range of technical measures and engineering solutions are required to issue a passport immediately. Ordinary passports therefore cannot be cancelled. However, we can't issue only ePassports and refuse to issue ordinary passports or we'll have to change the status of ordinary passports, which are issued for five years. Perhaps a short-term solution is to reduce the term of an ordinary passport to one year. But if an ordinary passport is valid for one year, the proportion of ordinary and ePassports that are purchased will change. Currently, 71% of all issued passports are ePassports. If the term of ordinary passports is shortened, the proportion of ePassports will increase to 95%–97%.

What additional security features are considered necessary for passports in the future?

Criminals make counterfeit passports by forging date stamps or visas. Some embassies based in Moscow complained about the counterfeiting of US and some European visas. But these counterfeit visas were found mainly on passports of foreign visitors from South-East Asia, but not on Russian ePassports.

No cases of counterfeit ePassports have been reported. There were several attempts to counterfeit previous generation electronic passports in 2005–2006. Criminals tried to change a photo by ungluing the lamination membrane or cutting a page. But all these attempts were caught by our border guards because the page with the lamination membrane changed its shape when it was cut. Since then, there have been no other attempts to counterfeit passports.

What will ePassports look like in the future?

I would not increase either the number of pages or the information recorded on the ePassports. I don't think it's necessary to weigh them down with additional information and design elements. But I would add scanned fingerprints.

In the future, the number of pages will probably diminish—most countries will have to cancel visas for short trips, which will be more convenient for travellers and the country itself. However, not all countries will agree to cancel visas. Currently, there are about 40 pages in an ePassport—more than a 10-year period requires. But it will remain at 40 pages because of border crossing stamps and it will also remain a paper document.

As for the passport validity period, in my opinion, a 10-year period is optimal. Most countries issue passports for five or 10 years.

Two passports or one?

Some people have proposed that domestic and international passports should be combined, creating a unique document, for example, a plastic card. In my opinion, it's not a feasible idea. The domestic passport is less protected as it's used within the country. Do we really need a chip in a domestic passport? And if we issue one passport, it will mean, for example, a senior citizen who never travels abroad will have to purchase an ePassport. Price is also a factor. If a domestic passport costs about 100 rubles and an ePassport costs 2,500, why would people buy an ePassport if they never travel abroad?

If the idea is implemented, it will occur many years from now because the world community is very diverse and it will become a problem if paper-based ePassports are rejected. So right now there's no point in discussing that idea.

I believe that it's better to modernise a domestic passport. One of the possible options is a plastic identity card that is distributed by our local departments. This plastic card could contain a chip for recording and storing the necessary information. The ID card also has to be easy to produce at a low cost. If a person loses this card, it must be easy for him to get a new card. Of course, we could include fingerprints on it and record their image on a chip, but not more than that.

In addition, it should only be an ID card. It should not be combined with a social services or bank card. The more information recorded on the chip, the more difficult technically it will be for each organisation to access information on the chip because each organisation has to obtain its data separately. Why should a person who goes to take out money at a bank have to show all his personal information? Why should a bank clerk know the Rh factor of a customer? Or why should a traffic cop have to access to information about bank accounts? ■

Mark Your Calendar

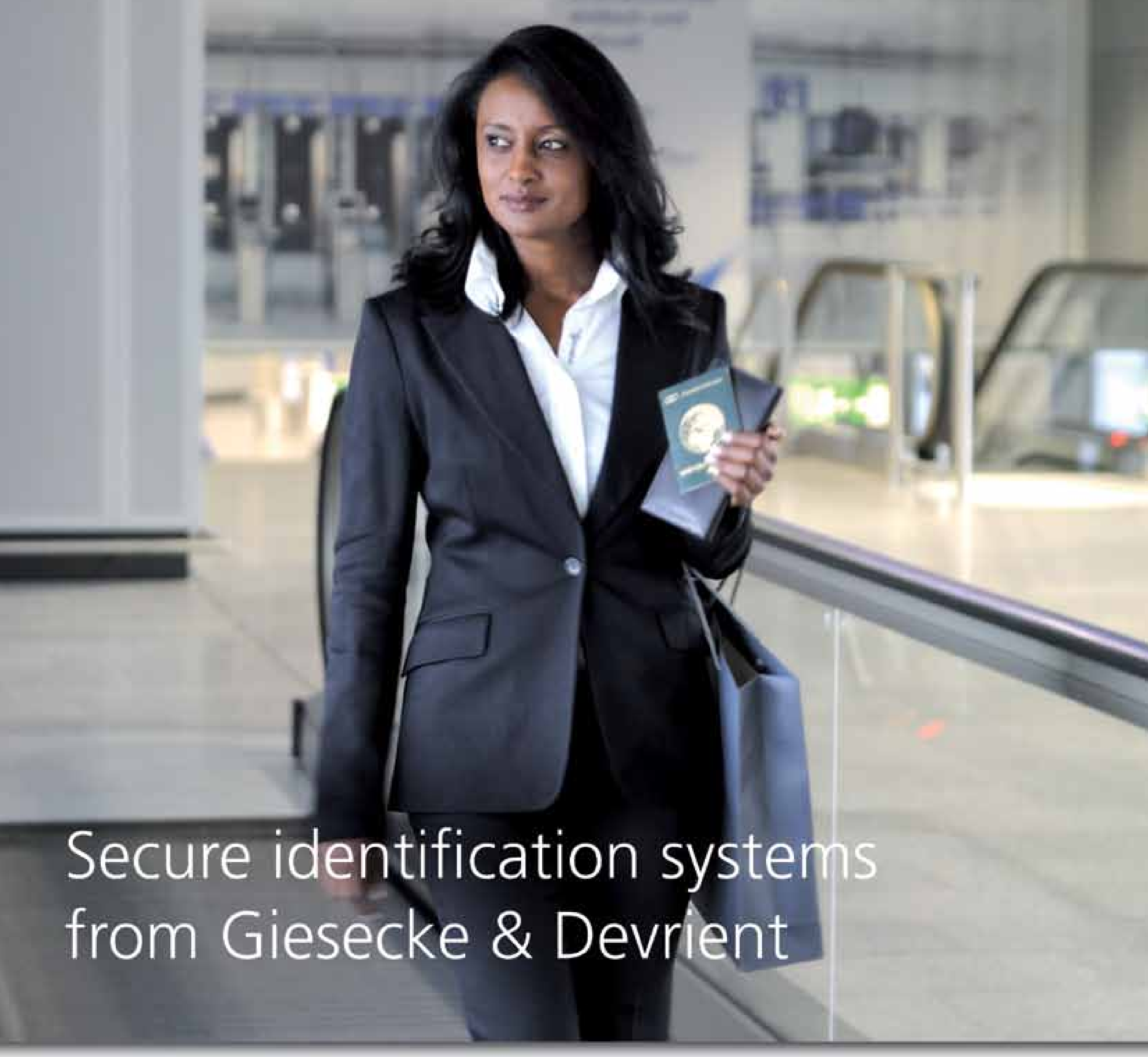
MRTD EVENTS 2013

Ninth Symposium and Exhibition on MRTDs, Biometrics and Security Standards

Montreal, Canada, 22 – 24 October 2013

For information and registration:

www.icao.int/meetings/mrtd-symposium-2013



Creating Confidence. G&D is a leading company in smart chip-based solutions for secure ID documents and passports, and boasts in-depth experience in the field of high-security documents. We supply entire nations with passport and border control systems, ID card solutions and have become a trusted adviser and supplier to governments. We also provide customized document features, card operating systems and technology for integrating state-of-the-art security features into ID documents. G&D will find the best solution for your individual needs. We define requirements together with you and offer tailor-made, effectively protected products that meet international standards. ID system implementation by G&D – individual, international and secure. **www.gi-de.com**

Giesecke & Devrient
Creating Confidence.