

# ICAO MRTD REPORT

NEWS AND FEATURES ON TRAVEL DOCUMENT AND IDENTIFICATION MANAGEMENT ISSUES - VOL.10 - NO.1

2015

## PASSPORT CONTROL

TRAVELLER IDENTITY VERIFICATION  
DATA SHARING  
THE IDENTITY TRIANGLE  
MOBILE SOLUTIONS

**AND:**

THE 10<sup>TH</sup> MRTD SYMPOSIUM –  
10 YEARS OF PROGRESS



ICAO

SECURITY & FACILITATION



**Graduated 1985**

30 years of consistency and innovation. The KINEGRAM® is the leading security device for visual authentication. More than 100 countries have placed their trust in the KINEGRAM®.

For banknotes: LEONHARD KURZ Stiftung & Co. KG  
Schwabacher Straße 482 | D-90763 Fuerth | [www.kurz.de](http://www.kurz.de) | [sales@kurz.de](mailto:sales@kurz.de)

For government documents: OVD Kinegram AG | Member of the KURZ Group  
Zaehlerweg 12 | CH-6301 Zug | Switzerland | [www.kinegram.com](http://www.kinegram.com) | [mail@kinegram.com](mailto:mail@kinegram.com)

**KINEGRAM®**



# ICAO

## ICAO MRTD REPORT VOLUME 10, NUMBER 1, 2015

### Editorial

MRTD Programme—Aviation Security  
and Facilitation Policy Section

Editor-in-Chief: Jim Marriott

Tel: +1 (514) 954-8219 ext. 5069

E-mail: fal@icao.int

Coordinator: Garleen McGann

Tel: +1 (514) 954 8219 ext. 6329

E-mail: fal@icao.int

MRTD/Border News updates: Omer Faruk Arinc

Tel: +1 (514) 954 8219 ext. 6515

E-mail: fal@icao.int

### Content Development

Senior Editor: Laurie Seline

Tel: +1 (514) 954-8219 ext. 5818

E-mail: lseline@icao.int

Associate Editor: Allison Dalzell

Tel: +1 (514) 954-8219 ext. 8108

E-mail: adalzell@icao.int

### 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

Harvey Wong, Advertising Representative

Tel: +1 (514) 954-8219, ext. 6181

Fax: +1 (514) 954 6769

E-mail: hwong@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 Narjess Abdennebi, Editor-in-Chief, at: fal@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 Robert-Bourassa Boulevard

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 © 2015

International Civil Aviation Organization

Printed by ICAO

## Contents

3

*MRTD Report* Editor-in-Chief Jim Marriott reflects on MRTD progress since the First Symposium took place a decade ago. While highlighting the positive developments, he draws attention to the work that still needs to be done to transform identification management and civil registration systems.

4

### 24 November 2015 Deadline

Alert to all States of the fast approaching deadline when all non-machine readable passports should be out of circulation.

6

### A Decade of MRTD Symposiums; A Commemorative Opening Address

Mr. Jim Marriott, Deputy Director, Aviation Security and Facilitation at ICAO, opened the Tenth Symposium and Exhibition on ICAO MRTD, Biometrics and Border Security with this speech.

9

### Civil Registration: The Need for a Common Terminology and Stakeholder Alignment

Sophie Taylor, industry advisor and programme leader at De La Rue, addresses the critical need for universal alignment in effectively recording vital events in civil registration systems and the impact an effective process has on the Traveller Identification Programme (TRIP) Strategy.

12

### The Case for Supporting Traveller Identity Verification with ePassport and Automated Data Sharing

Consultant, Ross Greenwood shares his expertise in passport issuance and civil registration, border control, biometrics and identity management and argues for stronger support of traveller identity verification at both arrival and exit control points.

16

### Passport Control Mechanisms: The Most Significant Challenges

Michael O'Connell, Director for Operational Police Support Directorate, INTERPOL articulates the major challenges faced by States and the many opportunities to unite, collaborate and seek to close the risk gap to reduce threats.

## 20 MRTD and Border Control News

24

### The Use of the Identity Triangle in Automated Border Control Systems

European ABC expert, Hans de Moel describes the Identity Triangle and its importance in delivering faster, more efficient border control systems that are equipped to handle increasing volumes of travellers.

28

### Interconnected Identity Verification: A Powerful Way to Stop Crime

Francisco J. Aranda, Principal Commissioner, Head of the National Identity Documents Division of the General Direction of National Police Force of Spain stresses the need for interconnected identity verification on a global scale.

32

### Mobile Solutions: Where Next?

Frank Smith, Chair of the European Union (EU) working group on mobile solutions for the police and immigration, e-MOBIDIG, offers his insight on developing a holistic and strategic approach to the use of mobile devices in front-line border control.

35

### Tenth MRTD Symposium: Summary and Conclusions

ISO and NTWG expert, Barry J. Kefauver provides a closing summary of the Tenth Symposium and Exhibition on ICAO MRTD, Biometrics and Border Security.

40

### Reforming the Identification Management System: The Georgian Experience

Levan Samadashvili and Nato Gagnidze offer insight as to how Georgia's new identification management system was shaped and developed according to the Georgian context.



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

Member	Nominated by	Member	Nominated by
Ms. A. Moores	Australia	Ms. G.M. Keijzer-Baldé	Netherlands
Ms. H. Richardson	Canada	Mr. D. Philp	New Zealand
Ms. M. Cabello	Chile	Mr. J. Wariya	Nigeria
Mr. W. Xiaobo	China	Vacant	Portugal
Mr. M. Vacek	Czech Republic	Mr. Y. Valentinovich Vzilter	Russian Federation
Vacant	France	Mr. F.J. Aranda	Spain
Mr. O. Götz	Germany	Mr. L. Bjöhle	Sweden
Mr. R. Swaminathan	India	Mr. R. Vanek	Switzerland
Mr. J. Nugent	Ireland	Mr. A. Brown	United Kingdom
Mr. Y. Ando	Japan	Mr. M. Holly	United States

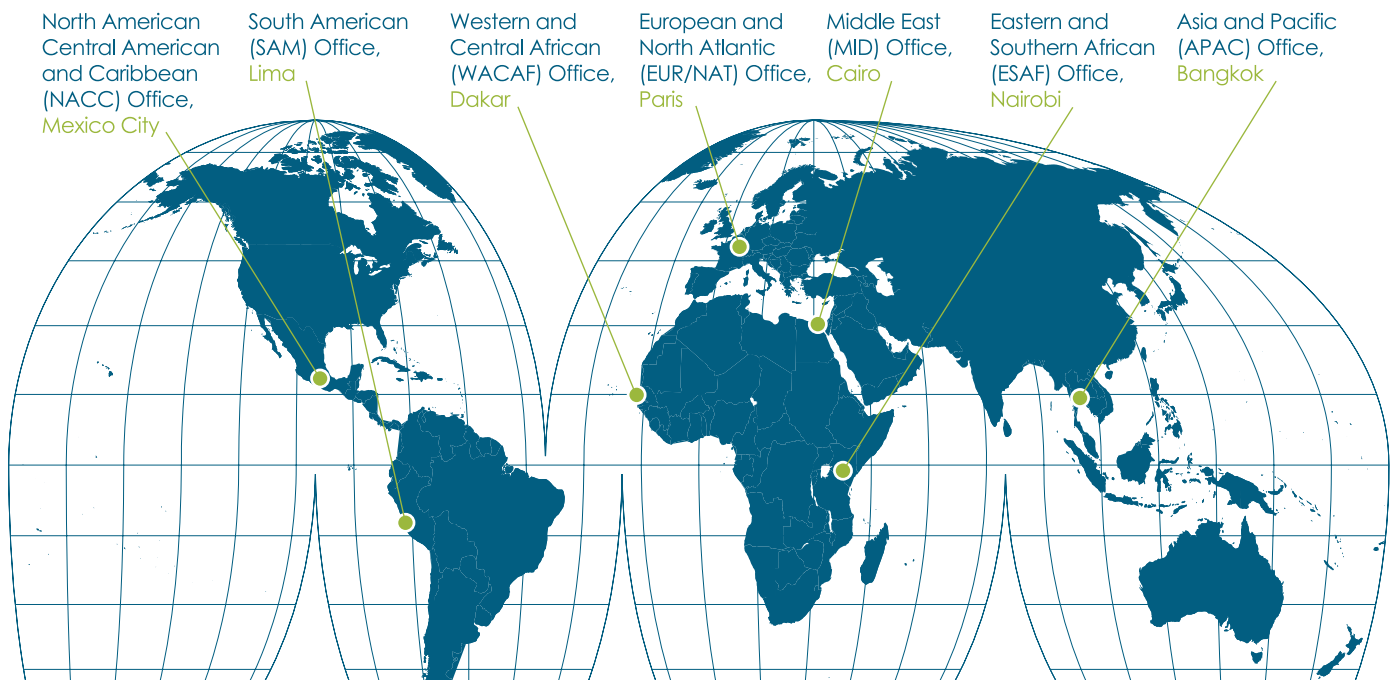
The TAG/MRTD is appointed by the Secretariat, which reports on its progress to the Air Transport Committee.

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



# WELCOME TO THE SPRING ISSUE OF THE MRTD REPORT



 Nearly 10 years have passed since ICAO welcomed 300 participants from 58 Member States to the first ICAO Standard Machine Readable Travel Documents (MRTD) and Biometric Enhancement Symposium held at ICAO Headquarters in Montréal.

In his opening address at the 2005 event, Dr. Assad Kotaite, President of the ICAO Council at the time, drew attention to the two billion passengers who would fly on scheduled air services that year and pointed to the civil aviation facilitation and security challenges that were greater than ever. The universal implementation of MRTDs had become one of the strategic objectives of the ICAO Aviation Security Plan of Action – ICAO was working to establish a border security standards and recommended practices framework; to develop specifications for travel documents; and to help Member States implement MRTDs and biometrics.

Fast forward to the Tenth Symposium and Exhibition on MRTDs, Biometrics and Border Security that was held at ICAO Headquarters in October 2014, where more than 500 participants from every region in the world came together to further strengthen the security of air transport.

And where the resolve to improve civil aviation security was never stronger.

In 2014 an estimated 3.2 billion passengers flew on scheduled international air services and there were an estimated, record number, 33 million aircraft departures. As passenger and aircraft movements have increased, security risks have multiplied and the nature and complexity of the threats have intensified.

Eliminating and mitigating these threats to air transport is a key global objective. While ICAO has developed Standards and Recommended Practices (SARPs) and related specifications for MRTDs (Document 9303) and biometrically-enabled documents (such as ePassports), our mandate calls for further advancements.

ICAO's MRTD programme has grown with the adoption of the ICAO Traveller Identification Programme (ICAO TRIP) Strategy. Coordinating identification management and integrating the issuance of travel documents and their inspection at borders featured prominently in the presentations at the MRTD Symposium and became the underlying theme of this issue of the MRTD Report.

In this issue, we focus on the need for interconnected Identification Management systems. Many of the contributors have stressed the need for unified identity verification on a global scale and have flagged a recurring concern that while the number of air passengers continues to increase, border control systems are not always effectively screening them. Improving inter-agency cooperation and international data sharing was a major focus of the Symposium and remains an ongoing priority.

Everyone is in agreement on one front: without accurate, secure and verified Evidence of Identity (Eoi) records, systems are flawed. This issue looks at the challenges one State experienced in effectively transforming their poorly-managed identification management and civil registration systems into the successful models they are today.

Also in this issue, the European Mobile Identification Interoperability Group touches on future technological trends and the need to consider human factors so that the people operating the systems and interfacing with passengers are fully effective in their roles, and connected to the most up-to-date national and international data.

Our work continues.

Let us all remember an important deadline. We are **months** away from the 24 November 2015 deadline when all non-Machine Readable Passports (non-MRPs) are to be out of circulation. Meeting this deadline and actively promoting global adoption of standardized biometrically-enhanced ePassports will do much more than merely facilitate border control – it will significantly reduce vulnerabilities on a global scale. ■





# ALERT:

## THE NON-MRP EXPIRY DEADLINE APPROACHES: 24 NOVEMBER 2015

ICAO Standards and Recommended Practices (SARPs) are contained in Annexes to the Chicago Convention, which is the main international law instrument regulating civil aviation matters globally. The 24 November 2015 deadline comes from Standard 3.10.1 in Annex 9 — Facilitation and refers to the date when all non-machine readable passports (non-MRPs) are to be out of circulation.



### WHAT IS A NON-MACHINE READABLE PASSPORT?

Passports that are handwritten, include additional family members or do not have a Machine Readable Zone (MRZ) are examples of non-Machine Readable Passports (non-MRPs). The requirement that non-MRPs expire by 24 November 2015 applies to all types of passports: Ordinary, Diplomatic and Service. However, it does not apply to temporary travel documents in cases of emergency, which usually have a short validity period and are issued by consulates to distressed nationals so that they can return to their home country.

### DOES STANDARD 3.10.1 CALL FOR OBLIGATORY BIOMETRIC PASSPORTS (ePASSPORTS)?

**No, it does not.** An ICAO Standard on obligatory ePassports does not exist, although it may become a requirement in the future.

### WHAT HAPPENS IF A MEMBER STATE DOES NOT COMPLY WITH THE DEADLINE?

**At this stage, ICAO has no official position or information on the possible consequences of not meeting the deadline.**

Therefore, any such debate is purely speculative. However, given the importance of potential consequences, the Implementation and Capacity Building Working Group (ICBWG) of ICAO's Technical Advisory Working Group on Machine Readable Travel Documents has been exploring possible scenarios in order to provide early warning and encourage measures that would assist States with meeting the deadline. After 24 November 2015, Member States may, for instance, refuse admittance to holders of non-MRPs or make visa processing more onerous and costly because of associated risks.

If such sanctions are introduced and applied after the deadline, they would bring costs and inconvenience to holders of non-MRPs. Consequences might include financial losses, increased costs, delays, refused entries, cancelled trips and disappointment.

### ARE THERE PRACTICES THAT CAN BE IMPLEMENTED TO MAKE MEETING THE DEADLINE EASIER?

**Member States face different challenges in meeting the 24 November 2015 deadline.** While no one solution fits all, a few guiding principles may provide assistance to Passport Offices in achieving compliance with Standard 3.10.1:

- The first step in managing the challenge is recognizing whether your State can meet the 24 November 2015 deadline.
- If your State is unable to meet the 24 November 2015 deadline, it is important to put together a constructive plan of action.
- Assess the extent of the problem. How many non-MRPs in your State expire after 24 November 2015? What is their expiration date?
- Inform ICAO by responding to the Questionnaire that is available upon request to government agencies (from

the ICAO Secretariat).

- If a State is unable to comply with Standard 3.10.1, the national civil aviation administration should 'file a difference' to give notice to the ICAO Council, as required by Article 38 of the Chicago Convention.
- **The most important step - carry out an information campaign to inform your citizens about the 24 November 2015 deadline. Encourage them to apply for machine-readable passports.**
- Avoid negative messages. Stress the importance of meeting the deadline and how compliance with the ICAO Standard is your State's international obligation and will facilitate travel and make it more secure.
- If practicable, implement facilitated processing for non-MRP renewal applications, such as a separate counter with shorter waiting times, a reduced renewal fee or similar such measures, which are entirely at the discretion of the issuing authority.

### IS ANY ASSISTANCE OR TECHNICAL ADVICE AVAILABLE FROM ICAO?

Government officials are welcome to contact the ICAO Secretariat for inquiries and further advice concerning the deadline or to file a difference: [fa1@icao.int](mailto:fa1@icao.int) ■

## An ICAO Standard on obligatory ePassports does not exist, although it may become a requirement in the future.



**Express Document Verification**

**Advanced Document Verification**

**Machine Assistant Document Verification**

**Information Reference Systems of Travel Documents**

**Special Equipment and Customized Solutions for Border Control**



[www.regulaforensics.com](http://www.regulaforensics.com)

# A DECADE OF MRTD SYMPOSIUMS: A COMMEMORATIVE OPENING ADDRESS



## ABOUT JIM MARRIOTT

He has served as the Deputy Director, Aviation Security and Facilitation for ICAO since May 2010. He leads ICAO activities in aviation security and facilitation assistance, policy, standards development and capacity-building. He also manages the Universal Security Audit Programme and the Public Key Directory and ICAO Machine Readable Travel Documents and Traveller Identification Programmes. With his extensive experience in international relations, critical incident management and policy, organization and regulations development, he is an internationally recognized expert in the field of aviation security.

✈ The Tenth Symposium and Exhibition on Machine Readable Travel Documents (MRTDs), Biometrics and Border Security took place on 7-9 October 2014 in Montréal, Canada. The global annual event reflected on the early MRTD milestones and showcased the latest developments in MRTD and traveller identification management – the ICAO Traveller Identification Programme. Mr. Jim Marriott, the Deputy Director, of Aviation Security and Facilitation at ICAO, opened the special event with this speech.

*Excellencies,  
Dear colleagues,  
Ladies and gentlemen,*

It is a great pleasure to welcome you to ICAO's Tenth Symposium and Exhibition on MRTDs, Biometrics and Border Security.

The tenth anniversary is a defining milestone for the MRTD Symposium. The event's programme provides an overview of the progress that has been made from early MRTD specifications to today's ICAO policy framework on holistic traveller identification management. The **ICAO Traveller Identification Programme**, known in short as **ICAO TRIP**, and its **Strategy**, were endorsed by the 39<sup>th</sup> Session of the ICAO Assembly last autumn. Many of you in the audience are MRTD veterans who have attended every Symposium in the past. You are well placed to grasp the dramatic expansion of the scope, ambition and results of the ICAO TRIP Strategy.

The adoption of the ICAO TRIP Strategy, and its main objectives, is already yesterday's news. Today's focus is on the Strategy's implementation in practice. Regardless of how relevant and timely the TRIP Strategy is, it will remain just a policy document – unless its ambitions for holistic traveller identification are embraced and implemented by Member States. These changes, when put into practice, will enhance both security and facilitation benefits for ICAO Member States, and their citizens.

Let me provide you with a brief overview of developments meant to ensure that the ICAO TRIP Strategy delivers practical benefits. The Secretariat, in close coordination with members of the Technical Advisory Group on Machine Readable



Travel Documents, is developing the TRIP Strategy work programme. This structured action plan will articulate results, targets and the estimated resources and activities that are required for achieving the strategic outcomes. The plan will also identify the indicators for measuring success and the designation of responsibilities for all activities.

The new Facilitation Section is currently being established within the ICAO Secretariat and will encompass the ICAO TRIP Programme. In addition to optimizing ICAO's resources, this restructuring will better align the Secretariat with Annex 9 – *Facilitation* provisions, and with the needs and expectations of the global aviation community.

A recurring theme in our TRIP Strategy work is the assistance that is provided to States. Let me provide you with a few highlights and challenges in TRIP implementation:

- **The importance of properly reading ePassports at border control points.** Specifications for issuing ICAO-compliant ePassports provide for the most secure and robust travel document ever issued. Over 120 States claim that they are currently issuing ePassports. There are nearly half a billion ePassports in circulation and these numbers continue to increase.
- **States still need to do significant work to ensure ePassports provide their full security and facilitation benefits.** Not all ePassports are fully compliant with ICAO specifications – and not all use the ICAO Public Key Directory (PKD) as a means of distributing the public key infrastructure information that is required to verify and authenticate ePassports. This prevents issuing States from capitalizing on the full security and facilitation benefits that ePassports are meant to deliver.
- **ICAO PKD membership has reached 45 States and continues to grow.** However, this number covers less than half of the

States that claim to issue ePassports. This calls for intensified advocacy efforts to underscore that the ICAO PKD is a must-have as far as border integrity is concerned.

- **ICAO is currently developing the ePassport Roadmap** – a policy planning and strategy tool that guides State and global efforts towards the universal implementation of ePassports.
- **A major machine readable passport compliance challenge is meeting the 24 November 2015 deadline by which time all non-machine readable passports should expire.** States must encourage their citizens to renew any non-compliant passports before the deadline.

Remaining and newly-emerging challenges stress an important point – having a good policy is vital – but it is not enough. It is the implementation of the TRIP Strategy in practice that really matters. Some States will inevitably struggle with turning ambitions into reality and this calls for intensifying capacity-building assistance efforts; intensifying technical dialogue with States in need as well as regional partners; and it calls for mobilizing assistance funding from the donor community.

ICAO TRIP implementation assistance has already started with Phase I in the African (Sahel) Region. Assistance projects have been developed in close cooperation with several Economic Communities in the African Union: The Community of Sahel-Saharan States (CEN-SAD), the Common Market for Eastern and Southern Africa (COMESA), the Economic Community of Central African States (ECCAS), and the Economic Community of West African States (ECOWAS).

The pilot assistance project for Phase I is a Canada-funded initiative on *Strengthening Travel Document Security in the Sahel*. Project activities include a workshop and training and technical assessment missions that address capacity gaps. I would like to highlight the Sahel Project as a shining example



**SEMLEX**  
G R O U P

IDENTIFICATION  
BIOMETRIQUE

Semlex fournit des solutions sécurisées pour l'identification des populations par la biométrie.

Semlex finance les projets et opère selon les besoins des gouvernements.

Contrôle frontière

Personnalisation  
des documents

111100000000G

MAPUTO

CIDADE MAPUTO

Manuel Aguiar

# Regardless of how relevant and timely the TRIP Strategy is, it will remain just a policy document – unless its ambitions for holistic traveller identification are embraced and implemented by Member States.

of joint efforts linking the needs of States, ICAO expertise and resources provided by the donor community, and to thank the Government of Canada for its generous support.

In this spirit, we continue developing TRIP implementation project proposals for other regions in Africa, Central Asia and the Americas, while also continuing our regular assistance activities. This year, two MRTD Regional Seminars in Uzbekistan and Spain attracted an unprecedented number of participants. These Seminars provided a first-ever opportunity to explore the TRIP Strategy with our colleagues in Europe and Central Asia, as well as to conduct the first ICAO passport interoperability tests. In addition, we have been implementing MRTD gap assessments in beneficiary States, particularly in South and Central America, which was again supported by contributions from Canada.

These short-term measures focus on intensifying and enhancing existing assistance activities. Our main interest is the potential of mid- and long-term prospects of ICAO's TRIP Strategy assistance. Options explored include establishing an ICAO-UN

Counter-Terrorism Committee (UNCTC) framework that is dedicated to providing technical assistance to States in implementing the TRIP Strategy. This framework would offer a one-stop shop for States that require access to the funds and expertise that are required for TRIP capacity building.

The presence of the UN Security Council Counter Terrorism Committee Chairperson and UN Counter-Terrorism Executive Directorate (UNCTED) leadership today is a symbolic reminder of the close synergies between the ICAO TRIP Strategy and the global counter-terrorism agenda. Our emerging vision would see ICAO, the UNCTC and partner organizations and Member States joining forces in consolidating their capacity to provide assistance in implementing the ICAO TRIP Strategy to all Member States in need, as an integral part of the Global Counter-Terrorism Strategy.

Finally, a few words about the Symposium programme. As always, we will address the latest developments in MRTD standards and specifications, as well as identification management and border control issues. This year's Symposium focuses on border integrity and border control management. It will explore inspection systems and tools and the interoperable applications that enhance security and facilitation benefits to Member States, with particular reference to their use in combatting terrorism and trans-border crime.

Watchlists, passport readers and border information systems, the ICAO PKD, intelligence-led border controls and inter-agency and cross-border information sharing will be examined in detail. Experts' presentations will also explore the integrity of the passport issuance process during a dedicated session. Document Issuance and Control, a component of the ICAO TRIP Strategy, offers concepts and good practices in preventing the fraudulent use of MRTDs by individuals who are not entitled to them.

The Symposium speakers and facilitators, who are drawn from ICAO working groups and partner international organizations, are top experts in their field. Special appreciation is extended to the government and industry experts who make up the Technical Advisory Group on Machine Readable Travel Documents (formerly known as the TAG/MRTD).

I invite you all to make the most of the Symposium and the expertise available here. Ask questions, share your challenges and experiences, question established views and contribute your knowledge to our on-going professional dialogue. I also encourage you to visit the many booths outside this meeting room to explore the range of products and services showcased in the Exhibition.


This Symposium offers a challenging and exciting programme that will capture your full attention for the coming three days. I sincerely thank you for having taken the time to join us here, and wish you a very successful and productive Symposium. ■

# CIVIL REGISTRATION: THE NEED FOR A COMMON TERMINOLOGY AND STAKEHOLDER ALIGNMENT



## ABOUT SOPHIE TAYLOR

*She is a key industry advisor on the requirements of a full Civil Registration and Vital Statistics solution. Having worked at De La Rue for 6 years, Sophie assists governments around the globe in securing their documents and also manages key regional and global stakeholder relationships. Sophie travels internationally, driving best practices and engaging with governments and stakeholders on strategies to help ensure that vital events and statistics are officially, efficiently and effectively recorded.*

 **Civil Registration is the act of recording and documenting the vital events in a person's life (including Birth, Marriage, Divorce, Adoption and Death). It should be continuous, permanent, universal and compulsory. It is a fundamental function of all governments. Within governments, civil registration systems are the responsibility of a number of ministries or departments, including Ministries of Health, Ministries of Interior, Ministries of Justice and National Statistical Offices.**

## WHY IS CIVIL REGISTRATION SO IMPORTANT?

Civil Registration contributes to public administration and governance by generating vital statistics information that underpins the wider population data for use in public service planning. Civil Registration and Vital Statistics (CRVS) is also a key factor in the Sustainable Development Goals being agreed to by all UN Member States in the post-2015 agenda. It is a subject that is going to become more central to the Identity and Development discussions in the coming months and years.

According to UNICEF, there are currently only 55 lower and middle income States in the world that have the basis of a CRVS system. Other States are still relying on sample surveys, household surveys and a ten-yearly census. More than 100 States still do not have functioning and efficient CRVS systems. Therefore, they cannot fully understand the needs of their population or, indeed, provide their people with the documents that allow them to have a legal identity and the consequent roles and responsibilities they are entitled to.

Without a birth certificate and the identity recorded within a secure and trusted database, a person does not officially exist and therefore cannot vote, cannot inherit from one's parents or access services available to them.

An estimated 57 million children who were born in Sub-Saharan Africa in 2012 were not registered. This is on top of all child and adult populations in these countries that have never had their identities registered.

## AN ESCALATING PROBLEM

With the world's population growing at the rate it is, this problem is only going to get worse. In our sphere of passports and ID cards, this is a problem that will grow into an unbearable security risk.

A hundred years ago, one might have been able to argue that these unregistered people wouldn't have travelled across international borders; therefore the risk would not have been tangible. However, with the world's economies growing to match the population rise, and these populations now gaining access to disposable incomes, it means that those born today **will** become wealthier; they **will** have access to travel and so **will** be crossing borders. Many of the children born in 2012 will expect to travel and will obtain





Children show off their birth certificates in Bangladesh.  
(Photo supplied by and reproduced with the kind permission of Plan International and their *Every Child Counts* initiative.)

An estimated 57 million children who were born in Sub-Saharan Africa in 2012 were not registered. This is on top of all child and adult populations in these countries that have never had their identities registered.

travel documents through whatever means available. Right now, globally, every 60 seconds, 5,700 passengers board aircraft and 52 aircraft take off. How do we know who they are?

What we are talking about here is Evidence of Identity (Eoi). ICAO is already aware of this and has set up the Traveller Identification Programme (TRIP) Strategy, to begin to support governments to improve their CRVS processes. As we all know, Eoi is **the foundation** of this strategy.

#### WHAT IS THE BUSINESS PROCESS FOR REGISTERING VITAL EVENTS?

Required is a secure business process to: a) *notify* an event has taken place. It is: b) *recorded and verified*, c) put into a *secure register*, from where it can be: d) *pulled anonymously* for data purposes.

This is an accepted approach already adopted by many. The rest of the world is working to address this.



## WHAT ARE THE PITFALLS?

Everyone agrees on how important this process is, but it is not as simple as we would like to think it is. There are many challenges:

1. **Multiple stakeholders.** We all know how complicated it can be to deal with multiple government agencies and juggle their conflicting priorities and needs.

There are international and national stakeholders – health, justice, interior, statistics, education, immigration and the aid community to name just a few. While we automatically gravitate towards those that we are comfortable with and with which we have existing business, these are only part of the bigger picture. A strong CRVS solution must align to all ministries who will **contribute** and **use** the data that is held in the system. The onus must be on the data, not the system containing it for this to work.

2. **A lack of best practices.** There is currently no Document 9303 equivalent for CRVS. Despite 55 low and middle income governments already managing CRVS systems, each country's challenges and requirements are very different in terms of execution and implementation of a successful CRVS system. However, there are some basic principles where all should be aligned to ensure that it is done properly. Two such examples are as follows:

- **Biometrics.** It is widely agreed that fingerprint biometric information does not stabilize in the human body before the age of 14 or 15 years, and therefore the use of biometrics is not appropriate when registering children. Neither is the use of a footprint. However, both are currently being used in certain countries. Is there alternative technology that would genuinely be suitable and, importantly, would be financially and geographically feasible in the country?
- **The verification process.** There is a lot of ambiguity about what constitutes best practice for verifying the identity of a parent and of a child at the point of birth registration. There are many questions that need to be answered. What documentation should be shown or submitted to the registrar? How should the evidence be stored electronically? What processes should be in place to check the authenticity of these documents? Is it enough for a parent to be there in person to register their newborn child if no documentation exists? Again, what is feasible and what is financially implementable in countries trying to set up a CRVS system?

Without these and other key standards, national CRVS processes can and will vary dramatically, and will therefore ultimately mean that one country's documents will be trusted over another country's documents. This could lead to an undermining of national systems and further inequality of secure issuance down the line for passports and National ID cards.

3. **The lack of a standardized terminology.** There are many different stakeholders who have all approached the topic of CRVS from their own angle (healthcare, statistics for government planning, passport authentication etc.). We are all using our own language to describe challenges and needs. An obvious example of this is the ICAO term – *breeder documents*. Only the ICAO community understands this term. Other stakeholders refer to these as *cardinal documents*, *certificates*, *tokens*, *evidence of identity documents* or *vital event records*.

Other examples of terms that are used within the forum but have several meanings are *interoperability*, *notification*, *registration* and *mobile registration*. It is really important that we all learn to speak the same language so that a requirement can be clearly defined and understood and a suitable solution can be created.

The UN Department of Economic and Social Affairs has drafted documentation on the glossary and terminology of CRVS systems and documents. This should be the basis of our engagement as well. We should also engage to discuss additional terminology which we can adopt from our respective areas of expertise, namely technology and system delivery.

## THE WAY FORWARD

We need universal alignment. We need to engage with all stakeholders, not just the passport and border control authorities. We need procedural and technical best practices that will ensure that systems will work in the long term and will help to both collect and protect the CRVS *data* as the government and citizen's key asset.

The ICAO community is very well placed to be able to support the Global CRVS improvement trend. But we need to do this responsibly. This is an opportunity to allow governments to build long lasting databases which will become a tool to improve their States through understanding of their populations.

We must not engage without fully understanding the requirements of **all** the stakeholders in the State, and we must not take the short term view. These data sets should be owned by governments and should last for decades, if not centuries.

I believe that interested parties from our ICAO community should engage collaboratively with these key national and international stakeholders to support the technology discussions and help create a trusted environment for governments to interact and liaise with the private sector.

This is to our benefit as well. Without a strong CRVS process, the TRIP strategy is not achievable.

Please contact me if your company would like to be involved. You can reach me at: [sophie.taylor@uk.delarue.com](mailto:sophie.taylor@uk.delarue.com) ■

# THE CASE FOR SUPPORTING TRAVELLER IDENTITY VERIFICATION WITH ePASSPORT AND AUTOMATED DATA SHARING



## ABOUT ROSS GREENWOOD

*He works as a consultant undertaking assessments for IOM, ICAO, OSCE and other international organizations and providing advice to agencies and vendors involved in passport issuance and civil registration, border control, biometrics and identity management. Until 2010, Ross was a senior executive in the Australian Passport Office with responsibility for the design of Australian passports; the application of biometrics in passport issuance; and preventing deterring and investigating passport fraud. Ross was Australia's delegate to the ICAO Machine Readable Travel Document TAG from 2007 to 2010 and the inaugural Chairperson of ICAO's Public Key Directory Board.*

Events in 2014 exposed inadequate, and in some cases, absent traveller exit control arrangements at airports globally.

The UN Security Council responded to the emergence of the foreign terrorist fighter threat by drafting and adopting Resolution 2178. It is now up to States, UN agencies and other international organizations to develop proposals for substantive initiatives that support the Security Council Resolution.

Effective identity verification is the foundation on which more effective responses to the threat of terrorism can be built. Watch lists and other mechanisms can only be effective in identifying travellers of concern when traveller identities are reliably verified.

Existing travel document specifications (ePassports) and communication infrastructure and protocols (Advance Passenger Information (API)) can be used in combination with Interpol databases and applied to exit control. Creating an automated platform for identity verification at exit control will generate data that can be seamlessly shared with border control agencies in transit and destination countries to support interventions that prevent travel, thus providing a foundation supporting the global implementation of the travel-related elements of UN-SCR-2178.



## INTRODUCTION

Expressing, *inter alia*, grave concern for the global threat posed by the travel of foreign terrorist fighters, the scope of the regulation of travel in earlier Security Council Resolutions was significantly expanded with the adoption of Resolution 2178 (SCR-2178) on 24 September 2014. The various elements of UN-SCR-2178, taken together, require States to evaluate and share information about travellers in order to identify terrorists and their supporters for the purpose of supporting interventions by States to prevent their travel, whether at departure, in transit or on arrival.

UN-SCR-2178 also references earlier Security Council Resolutions 1267 and 1989, which established, and then extended, the scope of an Al-Qaida sanctions list. UN-SCR-2178 notes that the activities of foreign terrorist fighters, and those who support them, may make them eligible for inclusion on the sanctions list.

The International Civil Aviation Organization (ICAO) is the United Nations Specialized Agency that has the mandate and responsibility for establishing, maintaining and promoting Standards and Recommended Practices (SARPs) related to the issuance

and verification of Machine Readable Travel Documents, and related border control issues, to ensure interoperability, enhance facilitation, and to contribute to international security.

To achieve its mandate in regulating air travellers, ICAO has adopted the Traveller Identification Programme (TRIP) Strategy. The Strategy involves the development of frameworks and standards for interoperable applications and the inspections systems and tools used at border control.

ICAO has partnered with the World Customs Organization (WCO) and the International Air Transport Association (IATA) to establish standard message formats for the transmission of traveller information, and is working towards the inclusion, in the Interpol SLTD database, of information on lost and stolen travel documents in national border control solutions.

Effective implementation of the travel-related elements in UN-SCR-2178 will call for fully engaged partnerships. ICAO, Interpol and the WCO are working together in the UN Counter-Terrorism Implementation Task Force (CTITF) with other UN partners, such as the Counter-Terrorism Committee Executive Directorate (CTED), and the United Nations Office on Drugs and Crime (UNODC).

#### THE CHALLENGE OF IMPLEMENTING UN-SCR-2178

The identification of travellers of concern depends, in part, on searches against watch lists such as Interpol's database of Stolen and Lost Travel Documents (SLTD) and the UN's Al-Qaida sanctions list. The effectiveness of these searches depends on the reliability and accuracy of the verification of traveller identity (i.e. 1:1 comparisons) when the search is initiated.

Traditionally, the focus of national border control agencies has been on travellers arriving at their airports, seaports and land borders. In more sophisticated jurisdictions, entry screening is flagged by information that is obtained in advance about travellers. UN-SCR-2178 calls upon UN Member States to use Advance Passenger Information (API) to inform national risk and threat assessments. API data includes data relating to each individual passenger, corresponding to those items of data that appear on the passenger's machine readable passports and other official travel documents, such as visas. "Interactive API" is an advanced API system. Here, API data elements are collected by an airline and transmitted, during check-in, to public authorities. The latter, within existing business processing times for check-in, return to the airline a "Board/No Board" (or similar) response message for each passenger, thereby preventing potentially high-risk passengers from boarding flights at the place of departure.

At most airports, the border control formalities applied at exit control are less extensive than those applied at arrival. In some States, departing travellers exit without any border control formalities while in others, the recording of departing travellers is undertaken by airlines, without the on-hand support of border control authorities.

#### SECURITY OF AIR TRAVEL IS DETERMINED BY "WHO" TRAVELS AND "WHAT" IS CARRIED ON AIRCRAFT.

The assessment of most traveller risks and threats remains a national responsibility, to be managed by States according to their sovereign judgement. UN-SCR-2178 makes the threat posed by foreign terrorist fighters a shared responsibility and requires States to manage border control interventions at entry, exit and transit.

Effective, automated identity verification at exit control, together with international data sharing, is critical for the future security of air travel and critical for the effective implementation of UN-SCR-2178.

More than 120 States are issuing ePassports. Currently, 45 States are members of ICAO's PKD, the global broker for ePassport public key infrastructure (PKI) verification. 166 States contributed to Interpol's SLTD database in 2013 and the database was checked 800 million times. Some 70 States send or receive API information and an additional 30 have indicated to the WCO their intention to use API in the future.

Integrated automated border control systems utilizing eGates, which commonly incorporate ePassport PKI verification, and checks of national and/or Interpol SLTD databases, are growing. Less obvious to casual observation, the globally installed base of PKI-enabled passport readers, which have the capability to perform verification of ePassports, is growing strongly; the older, optical-only passport readers are no longer sold by vendors.

There is, therefore, an opportunity to adapt, adopt and integrate existing infrastructure and apply it at exit control to enable enhanced data to be shared with transit and destination countries.

#### THE CONCEPT: A GLOBAL FRAMEWORK FOR AUTOMATED DATA SHARING TO SUPPORT TRAVELLER IDENTITY VERIFICATION

Verification of traveller identity has always been a shared, international responsibility – national passports were standardized in their current form in the first half of the twentieth century to provide a reliable basis for determining the identity and nationality of their holders. Identity verification provides a foundation for both

---

Effective identity verification is the foundation on which more effective responses to the threat of terrorism can be built.

## FIGURE 1 - POSSIBLE TECHNICAL FRAMEWORK FOR AUTOMATED DATA SHARING TO SUPPORT ENHANCED TRAVELLER IDENTITY VERIFICATION

<p>The available additional, <u>automated</u> traveller identity verification information can include:</p> <ul style="list-style-type: none"> <li>✓ ePassport PKI verification to confirm that the passport was genuinely issued, and that the passport data page has not been fraudulently altered;</li> <li>✓ checks of Interpol's SLTD database to confirm that the passport has not been reported lost or stolen; and</li> <li>✓ confirmation that a biometric identity verification has been completed (e.g. at an eGate).</li> </ul>	
<b>TRAVELLER INTERFACE - EXISTING</b> ePassport PKI enabled document readers (including eGates)	<ul style="list-style-type: none"> <li>✓ using existing infrastructure</li> <li>✓ leverages national investments in ePassports, eGates and document readers</li> </ul>
<b>COMMUNICATION INTERFACE - EXISTING</b> Airline Reservation Systems	<ul style="list-style-type: none"> <li>✓ using existing infrastructure</li> <li>✓ using existing data protocols (UN-EDIFACT)</li> <li>✓ using verified biographical data (i.e. iAPI)</li> </ul>
<b>TRANSACTION DATA (PRIMARY PROCESSING) - NEW</b>  <b>PKI verification</b> <ul style="list-style-type: none"> <li>■ checked Y/N</li> <li>■ detail of CSCA or Master List relied on</li> <li>■ detail of CRL relied on</li> <li>■ check result OK/refer</li> </ul> <b>SLTD checked</b> <ul style="list-style-type: none"> <li>■ checked Y/N</li> <li>■ Interpol SLTD and/or national compilation</li> <li>■ check result clear/match</li> </ul> <b>Biometric ID verification</b> <ul style="list-style-type: none"> <li>■ checked Y/N</li> <li>■ modality (face/iris/fingerprint)</li> <li>■ source of reference image (ePassport, Trusted Traveller Programme, other national enrolment)</li> <li>■ check result match/no match</li> </ul>	<ul style="list-style-type: none"> <li>✓ Automated collection</li> <li>✓ No additional personal information</li> <li>✓ Minimal additional data</li> </ul>
<b>SUPPORT (FOR HUMAN SECONDARY EXAMINATION) - NEW</b> Offline referral interface - to support <u>identity verification related</u> follow up enquiries from transit and destination countries <u>according to agreed protocols</u> .  Secure Online Reference Library – describing, in a standardized technical specification and narrative format, national identity verification arrangements at Exit Control for the information of transit and destination countries.	<ul style="list-style-type: none"> <li>✓ 24/7 support (e.g. as per Interpol SLTD model)</li> <li>✓ Data shared might include images of passport datapage and/or facial image read from ePassport chip.</li> <li>✓ Context to provide additional assurance to transit and destination countries of the quality of identity verification undertaken at exit.</li> </ul>





the assessment of risk, and the identification of threats posed by travellers. Verification of traveller identity is objective and evidence-based, and therefore lends itself to automation.

There are international airports in some States with existing data protocols and communications infrastructure at entry control. These need to be adapted for application at exit control as well. This would leverage, and give further impetus to, national investments in ePassport issuance, eGates and PKI-enabled document readers, and the integration of Interpol's SLTD database to improve assurance of identity verification at exit control, which would result in a systemic basis for integrated, automated watch list checks and allow for interventions by border authorities to prevent travel. The iAPI platform could be used to share the results of automated identity verification checks with transit and destination countries, to inform their assessments of risk and threat, and trigger their interventions to prevent onward travel.

#### THE CONCEPT CREATES A FRAMEWORK THAT SUPPORTS THE INTENDED USE OF ePASSPORTS AS A RELIABLE ENABLER OF AUTOMATED TRAVELLER IDENTITY VERIFICATION.

Improved assurance of traveller identity means more reliable traveller risk and threat assessments can be undertaken. In addition to providing a framework for interventions by States to prevent travel, the framework might, in the future, support pre-clearance arrangements for the benefit of travellers and the commercial operations of airlines.

The future security of air travel depends as much on the arrangements in place for travel from Dakar to Dubai, as those that apply between Paris and New York. The concept would create a global, interoperable, backwards compatible, standards-based, verified traveller identity framework that can accommodate more sophisticated bilateral and regional biometric data sharing initiatives. While these initiatives are already being planned and



developed in more sophisticated jurisdictions, improved identity verification must be available to all, so that no State is left behind.

A basic technical architecture describing the concept is at Figure 1.

#### STAKEHOLDER INTERESTS

International civil aviation operates on a commercial basis, for the economic and social benefit of travellers and the States to which they travel. It is therefore critical that the security of air travel is not achieved at the expense of the commercial viability of airlines, the efficient functioning of border clearance processes, or the traveller experience.

The additional data that is proposed to be collected is limited, minimizing the impact on the extra data to be transmitted by airline systems to just a few bytes per passenger.

The proposal is for an automated solution. The additional data that would be shared, if the proposal is adopted, is collected in traveller self-service (eGate) and assisted service (PKI document readers) processing solutions that require no additional human input.

The concept is privacy and data protection friendly. No additional personal data of travellers is collected or shared, and the concept has the potential to leverage, not only hardware and ICT infrastructure, but also the existing international agreements and protocols for the sharing of API and passenger name record (PNR) data.

The concept supports the sovereignty of national border control arrangements while introducing a more reliable basis for the application of travel-based sanctions authorized under international law.

#### NEXT STEPS?

Because the concept involves integrating and adapting existing infrastructure, communication, co-operation and co-ordination between ICAO, the WCO and Interpol would be required.

The concept is likely to attract the attention of commercial interests such as airlines, consumer advocates and regional and other international organizations, so an active communication plan to identify and engage with external stakeholders will be required if the concept receives support from UN Member States.

The question of whether the concept advances for evaluation will depend on the level of interest and support at ICAO, the WCO and Interpol. ■

# PASSPORT CONTROL MECHANISMS: THE MOST SIGNIFICANT CHALLENGES



**ABOUT MICHAEL O'CONNELL**  
He is the Director for Operational Police Support Directorate, based at INTERPOL, Lyon, France. He commands a diverse directorate that includes police forensics, police information management, fugitives and 24/7 operational and crisis / major incident support capabilities. He also leads on the INTERPOL Integrated Border Management Task Force, delivering innovative operational responses to border security threats. This article summarizes his address to the Tenth MRTD Symposium.

✈️ Around the world, there are mass movements of travellers through established and regulated air transport sectors who will carry out terrorist acts and other serious crimes.

Border controls, travel document security and identification management are central to combatting terrorism and trans-border crime. The use of false identities and fraudulent travel documents, in addition to exploiting systematic weak points in the identification management frameworks of many States, create global vulnerabilities that are exploited by criminal and terrorist networks.

In 2013, throughout ICAO's 191 Contracting States, over 1.3 billion passengers travelled on more than 32 million flights. Among these passengers were thousands of foreign fighters who moved from Europe, North America and beyond, to be trained, equipped and deployed in the Syrian theatre.

Despite extraordinary efforts devoted to improving safe and secure air travel and better identifying passengers, the threat remains as present, as clear, and as deadly today as it was yesterday. More importantly, the threat remains capable of dynamically exploiting any cracks in our defenses and any gaps in our vigilance.

Naturally, we celebrate the global resolve as evidenced by the activation of United Nations Security Council travel bans and other targeted sanctions against individuals and entities, but criminals and terrorists know that these sanctions are linked to their identity. Therefore, they hide behind shields, usually in the form of stolen or fraudulently obtained passports and other travel documents.

The international community has long recognized the need to remove these shields. Through the United Nations, we have established:

- **UN Security Council Resolution 1373** requiring all UN Member States to prevent the movement of terrorists or terror groups through border control points and to employ more effective controls on the issuance of identity papers and travel documents, as well as through enhanced measures to prevent counterfeiting, forgery and the fraudulent use of identity papers and travel documents;

- **UN Security Council Resolution 1624** which calls upon all States to cooperate in the strengthening of the security of their international borders, including combating fraudulent travel documents and, to the extent available, enhancing screening and passenger security procedures; and
- **UN Security Council Resolution 2178** which encourages INTERPOL to intensify its efforts against the foreign terrorist fighter threat including wider use of its threat tracking tools of Special Notices, and its Stolen and Lost Travel Document Database (SLTD).

ICAO, one of INTERPOL's key partners in this fight, has shown further resolve with:

- The mandatory introduction of ICAO-compliant Machine Readable Travel Documents since 2010;
- The *Declaration on Aviation Security* endorsed at the 37<sup>th</sup> Session of the ICAO Assembly in 2010 that encourages States to report, on a regular basis, all lost and stolen passports to the INTERPOL SLTD;
- The creation of second generation MRTDs in the Traveller Identification Programme (TRIP) Strategy with 'ePassports' – the most secure and robust travel documents ever issued; and
- 120 of ICAO'S 191 Member States now issuing ePassports, over 500 million of these documents in circulation and the growing use of additional security features such as the Public Key Directory (PKD).

### IS THIS ENOUGH?

For more than a decade, INTERPOL has emphasized the urgent need for efficient passport control mechanisms and strong identity management. Yet this urgency did not seem to grab the public and media's attention until March 2014.

The world was shocked to learn that two passengers had used stolen Austrian and Italian passports which were registered in INTERPOL's databases to board a flight. Speculation ensued as to possible terrorist links to these passports and their holders. No such links have been uncovered to date.

Less known, but perhaps even more shocking, is that on 7 April, just four weeks later, three other passengers were able to board two different airplanes at the very same airport, using stolen Turkish passports – also recorded in INTERPOL's databases. This time however, these passengers were exposed as the result of routine checks against the INTERPOL databases.

Yes, it is still possible to use stolen passports to board international flights. It is happening today in the almost 170 States that do not make use of the ePassport and PKD systems that are at their disposal.

**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
- Biometrics
- Border Management Systems
- Digital Identification
- Professional Services

Through a unique consultative approach, CBN develops and implements tailored solutions that address the diverse challenges encountered by its customers.

[www.cbnco.com](http://www.cbnco.com)  
[identification@cbnco.com](mailto:identification@cbnco.com)

## IT ONLY TAKES ONE PASSENGER TO GO UNDETECTED FOR TERRORISM TO SUCCEED

We are seeing new threats emerge in response to the introduction of sophisticated, modern MRTD's and ePassports. Today, there is a significant increase in individuals obtaining authentic passports by using false documents or real identity documents that do not represent the true identity of the bearer. Birth certificates are a good example of this because they are neither secure nor standardized and are often created based on incomplete national population records.

We continue to see the corruption of passport issuing officials and the inability of border control officials to distinguish between authentic and counterfeit documents. Unfortunately, the latter is often the result of limited access to the modern tools that can help in this regard.

## ARE WE MAKING PROGRESS?

Yes. But there is so much more to do.

ICAO has adopted the TRIP Strategy, that was endorsed by the ICAO General Assembly in October 2013, and its *strategic framework* for achieving maximum benefits from future travel documents through *Security and Facilitation enhancement* with ICAO's PKD.

The next generation of MRTD's will link the five key elements together – evidence of identification; document issuance and control; MRTDs; inspection systems and tools; and interoperable applications.

At INTERPOL, we have advanced the *INTERPOL – Travel Document Initiative (Travel Document and ID Reference Centre)* which includes the following suite of border security data tools to help detect and mitigate risk:

- **SLTD** which was launched in 2002 and now has in excess of 43,412,291 records in its database;
- **Travel Documents Associated with Notices (TDAWN)** which launched in 2009 and now has in excess of 64,153 records stored;
- **Electronic Documentation and Information System On investigation Networks with information on Travel Document (EdisonTD)** which was launched in 1992 and now has more than 3,700 documents from over 200 countries available;
- **Digital Interpol Alert Library (Dial-Doc)** with alerts on false and counterfeit travel documents; and
- **Document Identification System for Civil Services (DISCS)** the sister database to EdisonTD for civil status documents with 2,500 documents from 164 States.

Through the deployment of INTERPOL's Integrated Border Management Task Force, INTERPOL operationalizes the use

of these tools and services for border protection. An example of this operational capability will be seen as INTERPOL and ICAO join forces on the ICAO Project *Strengthening Travel Document Security in the Sahel and neighboring States – 2014-2015*.

## STEPS FORWARD

Although many challenges are global and complex, there are many opportunities for us to unite, collaborate and seek to close the risk gap to reduce threats. In the view of INTERPOL, preventing international terrorist movement and opportunity for trans-national crime is about helping border control officers on the front lines to make the right decisions about who to allow to continue their journeys, who to question and who to detain.

Through the use of our border detection systems, which have been accessed more than 800 million times to screen passengers, we can close the gap on these risks and help to reduce the availability of the 40 million plus stolen and lost travel documents that are available for misuse.

Developing the DISCS database and working with governments and industry, we seek to develop robust standards for civil status documents (such as MRTDs and ePassports) to make it more difficult for criminals to source genuine passports.

Used in combination, these tools have the capability to achieve our goal: stopping criminals and terrorists before they hide behind yet another passport to harm others. Better still, the use of technology can turn the passport into a powerful weapon against them - a weapon that can be deployed time and again in the field.

While many threats remain, they can be successfully neutralized on one condition: that we seize all the opportunities before us and that we systematically use every means available to our Member States. An instructive example is screening for prohibited items before flight travel: having to remove clothing, belts and shoes; emptying our water bottles; exposing our belongings to x-rays; and walking through magnometers over and over again.

We now need to deploy the same rigor to the systematic screening of passports. The threat has changed; it is now very much about the person, the terrorist and not just the prohibited item. We must continue to consider all developments when creating safe and secure travel documents that better facilitate passenger movement. If we stand still and let glaring global security gaps remain open by not policing the use of passports with more rigor, one day, once again, many will ask: "Why did we not stop them when we could have?"

If we act now, we can and will succeed. We know that our borders and the travelling public will be more secure if we unite our strengths – for international peace and security, and for a safer world. ■



# GAIN EXPOSURE & VISIBILITY

## ADVERTISING, SPONSORSHIP & EXHIBITION OPPORTUNITIES

Contact us to learn about marketing your products at our events and our advertising opportunities in the upcoming MRTD Report.



[events.icao.int](http://events.icao.int)



[mem@icao.int](mailto:mem@icao.int)

# MRTD AND BORDER CONTROL NEWS



## ICAO

The approaching 24 November 2015 deadline to take all non-machine readable passports (non-MRPs) out of circulation was the subject of much discussion during MRTD working meetings and conferences in 2014. The November 2015 deadline contained in Annex 9 – Facilitation Standards is not a deadline for the introduction of ePassports. For more information, please visit ICAO's website: <http://www.icao.int/Security/mrtd/Pages/24-NOV-2015.aspx>

## EU

A new European R&D project, Automated Border Control Gates for Europe (ABC4EU) will enhance automated border control systems at European airports. The aim is to make border control more flexible and integrated by enhancing workflow and harmonizing the functionalities of ABC gates. The project, initiated in 2014, will take 3.5 years to complete.

## Cuba

The Cuban government will implement a new ID card that is more durable and consistent with new technologies. The card will include biometric data of individuals and allow for the data collection and identification of persons by any Identity Card Office in the country. The Interior Ministry said that the ID card can store voice prints, iris scans and DNA data for greater security.

## Caribbean

Both Lynden Pindling International Airport in The Bahamas and Queen Beatrix International Airport in Aruba have joined the ranks of 25 North American airports using Automated Passport Control (APC) kiosks. Aruba Airport APC kiosks were introduced at the international airport in December 2014. The Bahamas' 20 APC self-serve kiosks for eligible passengers became operational in February 2015.



## Italy

Rome's Fiumicino-Leonardo da Vinci International Airport has installed a trial of an automated border control e-gate system. More than 3,000 passengers a day are being cleared at the airport through the self-service e-gates that can be used by ePassport holders from EU Member States. The e-gate system uses a combination of fingerprint and facial recognition technology to verify a passenger's identity.

## Bosnia Herzegovina

Bosnia Herzegovina has officially begun to issue third generation biometric passports as of October 2014. The Supplemental Access Control (SAC) passports allow for safer registration and the protection of chip data. The distribution of these personalized passports is in progress.

## Azerbaijan

An agreement between the European Union and the Republic of Azerbaijan on the issuance of visas entered into force on 1 September 2014. The agreement aims to facilitate issuing visas on a reciprocal basis for an intended stay of no more than 90 days in a 180 day period.

## COMESA

The Common Market for Eastern and Southern Africa (COMESA) delegations from 20 Member States met in Zambia to discuss a proposal to introduce an ID card to be used by dignitaries for official travel in the region. The new COMESA Machine Readable Travel (CMRT) document will replace the current COMESA Laissez-Passer which is not accepted in some countries.

# MRTD AND BORDER CONTROL NEWS

## USA

U.S. Customs and Border Protection (CBP) has launched Mobile Passport Control (MPC), the first authorized mobile application to expedite the entry process for travellers entering the United States. The MPC system allows travellers to submit their passport control and customs declaration via their smartphone or tablet. It is currently in operation at Hartsfield-Jackson Atlanta International Airport.

## Nigeria

The President of Nigeria has formally launched a new national electronic ID card, which all Nigerians will be required to have by 2019 in order to vote. The new ID card will combine identity verification with many other applications including electronic payments functionality. The new electronic ID card stores a holder's biometric data including 10 fingerprints and iris data from scans taken during enrolment.

## Uganda

To enhance border security, Uganda plans to issue new ePassports integrating two new technologies: radio-frequency identification (RFID), and biometric data from fingerprints and iris scans. Uganda has also begun to issue Machine Readable Passports (MRPs) for refugees living in Uganda to help facilitate their movement to other countries. The new documents are UNHCR compliant and also in line with ICAO specifications.





### Spain

Spain's Ministry of Security plans to install a new biometric border control management system between the Province of Cadiz and the British colony of Gibraltar by 31 May 2015. The new system, which features ABC Gates, is already functional in the Madrid, Barcelona and Malaga airports. It will be equipped with an access control system that will capture fingerprints and facial images, and two modern biometric system posts. It will be integrated with the ABC System databases and information systems of the National Police.

### Spain - ICAO

ICAO organized and conducted Interoperability Tests during the MRTD Regional Seminar held in Madrid, Spain from 25 to 27 June 2014. The tests were based on the EU States' mandatory implementation of the ICAO Supplemental Access Control (SAC) mechanism for machine readable travel documents. The focus of the tests was to evaluate whether ePassports and inspection systems with SAC communicate securely with each other. The tests were led and supervised by an ICAO team of experts and a member of the ISO group. During the interoperability tests, 52 ePassport samples and 11 inspection systems were tested. The results presented at the conclusion of the Seminar are available on ICAO's website: [http://www.icao.int/Meetings/mrtd-madrid-2014/Documents/31\\_InteropResults\\_Test2014.pdf](http://www.icao.int/Meetings/mrtd-madrid-2014/Documents/31_InteropResults_Test2014.pdf)

### Turkey

Turkey unveiled new biometric ID cards, which can combine confirmation of identity with other applications such as banking, access to online e-Government services and law enforcement. The new ID cards store fingerprint and palm vein print data. They are designed to facilitate a variety of procedures, from birth registration to name and address changes. The distribution process will be completed in three years.

### Japan

To reduce waiting time, facial recognition machines will be installed for screening of passengers at Japanese airports in 2017. The Justice Ministry made the decision based on the results of the experimental use of such systems at Narita and Haneda airports from 4 August 2014 through 5 September 2014. Biometric recognition machines compare images of arriving passengers' faces with facial photo data encrypted in their passports. Japan currently has automated border control kiosks using fingerprint checks for Japanese passport holders and some foreigners living in Japan.

### Kenya

The government plans to introduce digital ID cards for all Kenyan citizens to strengthen national security. Existing ID card holders aged 12 and older will register for the new generation cards beginning in February 2015 and will receive the new cards in October 2015. The new ID cards will capture key biometric features such as fingerprints and iris scans.

# THE USE OF THE IDENTITY TRIANGLE IN AUTOMATED BORDER CONTROL SYSTEMS



## ABOUT HANS DE MOEL

A chemical engineer (B.Sc.), Hans became a forensic document examiner at the Netherlands Forensic Institute (NFI) and moved on to the Royal Netherlands Marechaussee where he used his knowledge of biometrics, computer systems and documents design to create the first dedicated user interface for the document scanners used by the Marechaussee. He was involved in designing, testing and implementing the Self Service Passport Control at Amsterdam Airport Schiphol, developing the EU-VIS system, and setup, testing and analysis of the FRONTEX Document Challenge in Lisbon in September 2013. Currently, he is working on intelligent camera surveillance and the Smart Borders concept of the European Commission.

✈ The popular Australian television series *Border Security* gives the viewer insight into the tasks different entities perform at the border. These vary from the customs officer in the quarantine hall who detects undeclared food; to the dogs sniffing for drugs; to the immigration officers and border guards who prevent illegal entries. The face of border control all over the world is changing, and most especially, at airports.

The conventional practice of checkpoint lanes with a border guard at a desk is gradually being augmented by self-service gates for travellers that function using ePassports or other tokens. The border guard is responsible for checking a person's identity and for determining whether he is admissible or not. In Automated Border Control (ABC) systems the same tasks have to be performed, with the added vulnerabilities inherent in automation.

## THE BASICS OF IDENTITY

When a person is openly asked about his or her identity, the response may differ greatly depending on cultural background. One person may tell you his life story beginning from birth, one may describe his physical presence or his social status and another may simply present an identity document that has been officially issued by their government.

What actually is an identity? In a world where identity fraud is a growing menace, identity claims have to be proven. Is an identity linked to a real-live person, to a name, to the data that is stored in official records, or is it a combination of these? Should we distinguish identities on the basis of the physical properties of a person (face, fingerprint, iris, DNA, etc.) or can we stick with labels (name, date and place of birth; residence; social security number)? What do we need to classify a person as unique in a border management system?

Identity has two aspects: biographical data that includes administrative details, numbers and labels and biometrical data that uses face, finger, iris, DNA, ear print, hand palm, vein structures (physical properties) or key stroke, signature, speech, etc.



Who is 'the KING'?  
Same biographical data



Who is this man?  
Same biometrical data

(behavioral properties). The combination of these two characteristics makes a person unique. Even identical twins with the same DNA will have differences in physical and behavioral properties, and hopefully, will have different names.

Most automated identification systems used for large populations work with biographical data because the queries are fast and easy. On the other hand, the high security facilities usually used for smaller populations often employ biometric data to ensure only the true person is admitted. In an Identity Triangle System, both biographical and biometric data play a crucial role. The system is dependent on the level of required reliability, the data required, and the restrictions encountered when gathering the data.

#### THE CHARACTERISTICS OF THE IDENTITY TRIANGLE

In identity management, three elements often appear: the real-life person; recorded information about the individual; and the person's identity document. These three elements become the foundation - the cornerstones - of the Identity Triangle. Integral to the Identity Triangle concept are two main procedures (Shown in Figure 1):

In the **Enrolling Cycle** the three main processes are defined as *Registration*, *Validation* and *Verification*. Each arrow on the side of the Triangle represents a process.

In the **Checking Cycle**, the main processes are defined as *Verification*, *Authentication* and *Identification*. This is where a person is verified against a claimed identity.

#### ENROLLING CYCLE

The processes for enrolling an identity can be explained with the example of a baby born in the Netherlands. After a birth, within four working days, one of the parents will go to the municipality to declare the birth. In this process, the parent registers the

An image has the advantage of universal usage, but lacks the accuracy of a template. A template, on the other hand, has a much larger discriminatory value, but lacks interoperability due to algorithm dependency.

newborn: gender; date and place of birth; given names; and the names of the parents. In this registration process only biographical data is stored in the birth and population registers.

At a later stage, when an identity document is required, the process of *Validation* is performed. In this step, biometrical data (face and fingerprints), are added to the population register to complete the identity of this person. Both biographical and biometrical data are included in the identity document.

To ensure the identity document is issued to the right person, the process of *Verification* is performed on issuance. In the Netherlands, the passport must be collected in person. The

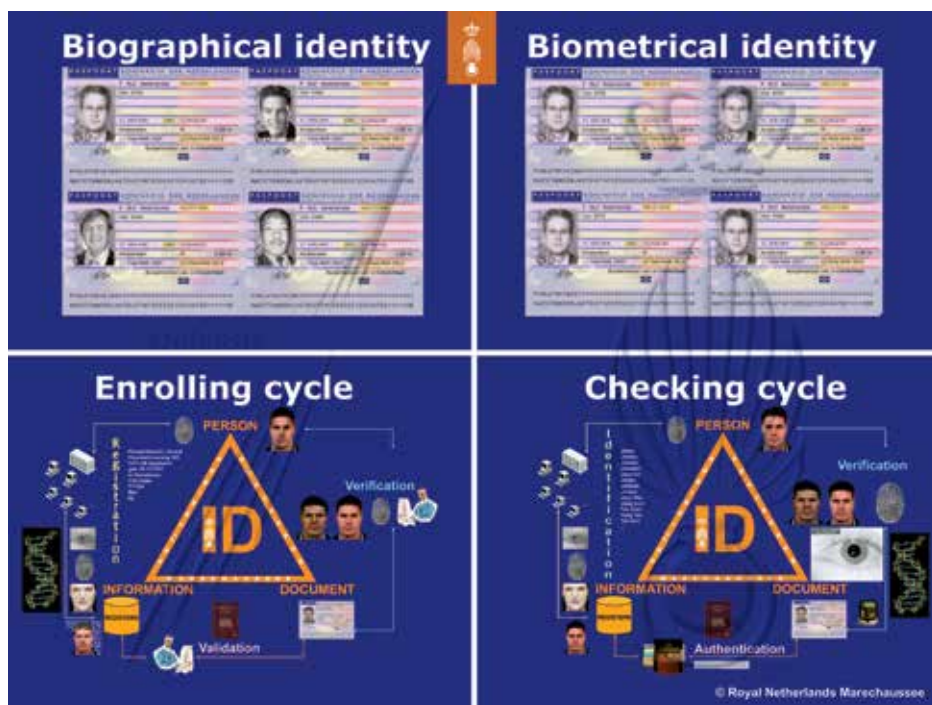


Figure 1: Aspects of the Identity Triangle

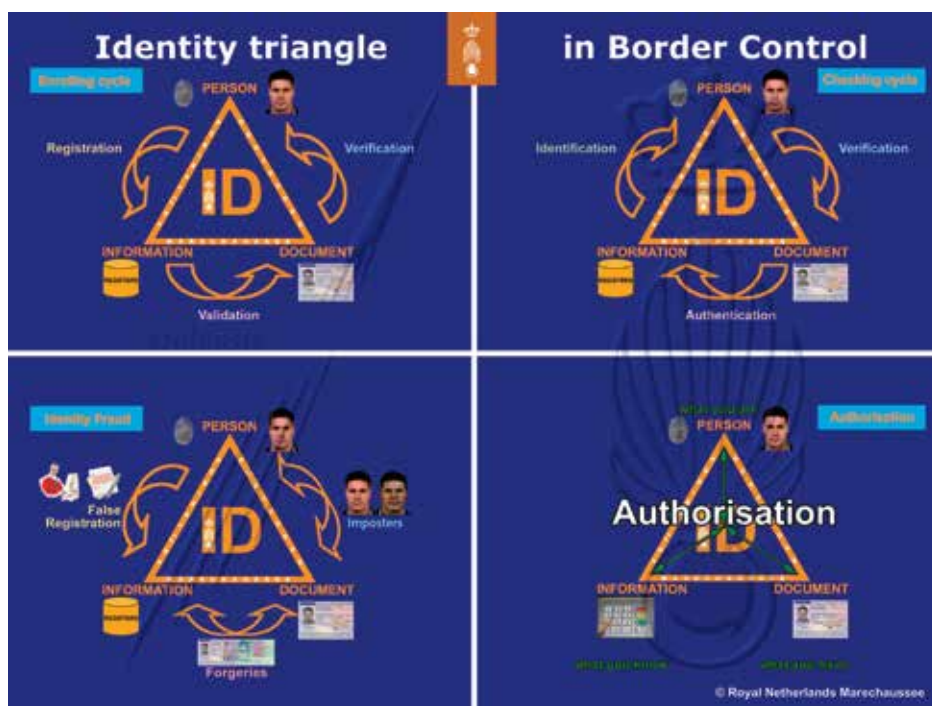


Figure 2: Identity Triangle processes

enrolment cycle is graphically represented by the top left corner in **Figure 2**. The checking cycle is displayed in the top right corner.

### CHECKING CYCLE

To verify whether the identity claim of a person is valid, the checking cycle must be performed. Traditionally, every State

operates with its own set of rules for admitting foreigners. In a standard border crossing, the following processes must be executed:

- **Verification:** the person must be verified against the travel document.
- **Authentication:** the travel document must be checked for authenticity to ensure there have been no alterations or forgeries.
- **Identification:** the person and document must be checked against (inter)national databases.

Following the identification check, the final process consists of:

- **Authorization:** the border guard verifies that the rules of admittance for the purpose of the stay (including the duration and means of support) have been met.

These processes are not necessarily performed in the same order. In the Netherlands, the first step is *Verification*. In Australia the first step is normally *Identification*, with searches split between known persons (Australians, New Zealanders and all other travellers in the visa register) and unknowns (undocumented and incorrectly documented). However, in most ABC systems the first step is *Authentication*, where the validity of the travel document is checked. In principle, it doesn't matter in which order checks are performed as long as the whole checking cycle is executed.

### CONVERTING TRADITIONAL BORDER CONTROL TO ABC

In most cases, a border guard will begin with *Verification* to ensure the traveller is the same person in the identity document. Traditionally this is done by comparing the photo in the document with the person providing the document to the border guard. In an ABC system, this process is

replaced with biometric verification, where there is facial comparison between the photo on the chip and the live picture of the person. Some ABC systems compare the photo printed in the document with the photo on the chip, while in others, the verification process is conducted using an alternative biometric such as fingerprint comparisons.



# In an Identity Triangle System, both biographical and biometric data play a crucial role. The system is dependent on the level of required reliability, the data required, and the restrictions encountered when gathering the data.

In currently used ABC systems, there is a known biometric vulnerability. Although ICAO clearly defines Datagroups in the Logical Data Structure of the chip in Doc 9303 (where the mandatory Datagroup 2 is defined as Encoded Face and Datagroup 5 as an optional Displayed Portrait), currently, throughout the world, Datagroup 2 is filled with an image of the holder as the global interoperable biometric template of the face.

An image has the advantage of universal usage, but lacks the accuracy of a template. A template, on the other hand, has a much larger discriminatory value, but lacks interoperability due to algorithm dependency. For biometric comparison, there is always a margin of error. Depending on the threshold of this margin, the right person may be refused or the wrong person may be approved.

The *Authentication* process is traditionally carried out by the border guard who checks for certain physical security features in the travel document (such as a watermark or an optical variable element). In most ABC systems, the authentication process is not based on the physical security features, but primarily on the electronic security features where the full chain of certificates has to be checked (as described in Doc 9303). This is why most ABC systems are for ePassports only.

The *Identification* process differs by State depending on the watchlists and clearances that are used. Traditionally, the border

guard enters the data into a computer system manually. In ABC, the query is done automatically using search strings derived from the Machine Readable Zone (MRZ). This limits the search strings since not every data field on the biopage (like place of birth) is represented in the MRZ.

Another vulnerability occurs when names from different character sets (such as Arabic, Chinese, Cyrillic or Thai) are converted to Latin characters, and when special characters (such as diacritics) are converted.

**Input mistakes** Royal Netherlands Marechaussee

**Typo (by ear)**  
 Joke van der Steen (NLD)  
 Joke Vandersteen (BEL)  
 Yoka Fonda Stayne (USA)

**Transcription**  
 Muller = MULLER  
 Möller = MOELLER  
 Müller = MUELLER  
 Møllær = MOELLAER  
 Mullär = MULLAAR

**Order**  
 Ping Li  
 or  
 Li Ping  
 Li = 李 = LEE

**Diacritics**  
 محمد  
 Mahmed  
 Mechmet  
 Mohamad  
 Mohammed  
 Muhamad

Ali Ben Mohamed  
 or  
 Mohamed Ben Ali

力历初立荳彦  
 礼淚俚婁曆梨

One of the most common Arabic names is the single Arabic ligature 'MHMD'. This name represents Mahmed, Mechmet, Mohamad, Mohammed, Muhamad; converting it is not simple. Li is a common name in Chinese. When the Chinese characters for Li are entered in the Netherlands, Germany or France, the name will convert to LI. But in English-speaking States it may convert to LEE. In both Arabic and Chinese there is an extra input issue dependent on the order of the first name and surname. Is it Ping Li or Li Ping? The name MULLER occurs in several languages and even though it is more or less pronounced the same way, it can be written in many different ways.

One of my German contacts is called Hößl, a surname that should be properly converted to HOESSL in the MRZ. But a fellow officer, who may not be aware of the proper conversion rules of ICAO, who is transcribing it in the Visual Inspection Zone, may enter it into the watchlist as HOBL, HOSSL or HOEBL.

Properly applied, Automated Border Control does not compromise national security or public safety. It does streamline a portion of the border clearance process by verifying, authenticating and identifying travellers. Given the increasing need for faster, more efficient border control systems, the Identity Triangle makes us better equipped to handle the 'abc's of ABC. ■



# INTERCONNECTED IDENTITY VERIFICATION: A POWERFUL WAY TO STOP CRIME



## ABOUT FRANCISCO J. ARANDA

He is Principal Commissioner, Head of the National Identity Documents Division of the General Direction of National Police Force. His previous titles include: Head of the International Police Cooperation Service (Interpol-Europol-Sirene), Head of Interpol, Counselor of the Spanish Embassy in the United States, 2<sup>nd</sup> Chief of the Central Foreign Intelligence Unit, and Head of the Basque Country Judicial Police. He has also been a member of the Central Narcotics Squad. His work has been focused on combating illicit drug trafficking and international terrorism through international cooperation.



**In the globalized world in which we live, documents are an essential part of life. They define the social, political and economic aspects of everything we do. They are our passports to safety and security.**

Sadly, documents are also a gateway to crime, much of it major. Many criminal acts, from theft to terrorism, involve falsifying identity. Credit cards, identity cards and passports all fall prey to criminals. It is far easier to steal an identity than it is to hold up a bank.

Air travel, by its very nature, represents an excellent opportunity for wrongdoing. Thus the great need for vigilance in every aspect of the industry.

Anyone actively involved in any field of security will look at air travel from a unique perspective. They observe baggage and document checks and scrutinize the passengers who will board an aircraft. Those with a security background will analyse every area in an airport looking for vulnerabilities and weighing potential risks.



Whether for business, leisure or migration, millions of people travel every day using the fastest means of long-distance transportation: flying. Speed defines our fast-paced society, and as the world speeds up, so too does criminal activity.

The most important item travellers will pack is their passport. The document certifies the identity and citizenship of the person who holds it, or at least it is *supposed* to certify the identity of the person who holds it.

Terrorists and other criminals use fraudulent identity and travel documents to hide their real identities, to elude justice and to create new personas for themselves.



## Good documents with sophisticated security features are of little use if there is not a strong, secure system of issuance, management and control.

An atmosphere, such as an airport where families are off to holiday and business people are rushing to catch flights is fertile ground for criminal activity, particularly given the increasing need for speed and efficiency in airport operations.

### THE NEED FOR STRONG, SECURE, INTERCONNECTED SYSTEMS

Good documents with sophisticated security features are of little use if there is not a strong, secure system of issuance, management and control. It is essential that the control system receives timely and accurate information when identity and travel documents are lost or stolen. There must be a solid link between national and international databases.

If a car is stolen from a parking lot at an airport on a Friday and the person who owns this car doesn't realize or report it missing

before Sunday night, the criminal who takes it has enough time to move the car through controls and borders without it being listed as stolen. The same thing happens with stolen and false identity and travel documents; information may not move through security chains fast enough. Criminals, whether they are involved in petty crime or organized crime and terrorism, will take advantage of system vulnerabilities.

Systems implemented for reading travel documents require continuous improvement. Many States have incorporated Machine Readable Travel Document (MRTD) and Public Key Directory (PKD) technologies in their security systems, which has led to obvious improvements in many airports. However, States must consider a variety of factors, from cost savings to elevated risk, when exchanging documents with other States – some of which are located in areas that are high risk or engaged in conflict.

## A State-wide, 24-hour verification centre (CEN 24) with national, dedicated points of contact would be an ideal system solution.

### CEN 24

A State-wide, 24-hour verification centre (CEN 24) with national, dedicated points of contact would be an ideal system solution. This system would need to be linked to similar agencies in other States responsible for managing and controlling identity and travel documents and would have to be able to verify any State document, whether a passport or an identity card, in less than thirty minutes.

Having one verification centre per State would create an international collaboration network that would answer, on a reciprocal basis, every query on documents requested by another State, and simultaneously, would act as a national contact point for requests to other States made by it. The net result would be fast channeling of secure and reliable information.

The most essential element in any verification is the quick and direct comparison of data, images and original documents that are stored in databases at the time of issue. In a case where there is positive identification of a fraud or reason for criminal concern, the verification could be expanded to include criminal records and could trigger State and/or police intervention (depending on the national and international regulations applicable in each case).



In specific situations (such as acts of terrorism), the verification system would prevent the holder of the identity card or passport from boarding a plane or ship; from escaping justice; from compromising the safety of people and property. A CEN 24 system would take security to a new level, particularly in situations where urgent and accurate checks on the authenticity of documents and their holders must be carried out.

### EFFICIENT AND AFFORDABLE

This type of verification system would not require costly infrastructure, a large communal database with expensive maintenance, and data transfers to a bank of servers that would require valuable resources and additional expense.

Individual States would be responsible for their own data, with each State managing its own database, but the databases would be linked together in one international network. All States would need to use a standard format for scanning and transmission - both the State requesting information and the State providing the passport/travel document. We don't believe that interoperability would pose a major problem.

Moving forward with a system like this, because it would not require costly investments in extensive infrastructure, would enable States with limited resources to align their systems with neighbouring States to resolve identity compromise problems and keep their databases up to date.

### CONCLUSION

Enhanced security can significantly decrease human and material losses. As human beings and as aviation professionals, we are obliged to fight criminality wherever possible and make aviation safe and secure.

Security should not end with baggage and identification checks. But it should start with an interconnected identity verification system. ■





ICAO

## ICAO TRIP 2015 EVENTS

The ICAO TRIP / MRTD Symposium and Regional Seminar will be of particular interest to government officials from national identity and travel document issuance authorities, civil registries, passport offices, immigration, customs and other border inspection and law enforcement agencies; Ministries of Interior and Foreign Affairs, as well as embassy Consular staff.

### 11th TRIP / MRTD Symposium

ICAO Headquarters, Montreal, 14 – 16 October 2015

ICAO will hold the Eleventh Traveller Identification Programme Symposium and Exhibition on MRTDs, Biometrics and Border Security, following last year's successful event, attended by over 500 participants from States, international organizations, companies and other institutions.

This global annual event will address ICAO MRTD standards and specifications, identification management best practices and related border security issues. In addition, the Symposium will provide an overview of milestones in moving from the early MRTD specifications to a coherent ICAO policy framework on holistic traveller identification management - the ICAO Traveller Identification Programme.

### TRIP / MRTD Regional Seminar

Nairobi, Kenya, 10 – 12 November 2015

The Regional Seminar will assist Member States in implementing ICAO MRTD specifications and related ICAO Standards and Recommended Practices (SARPs). In addition, it will specifically address the needs of States to further enhance the integrity of the passport issuance process and ensure robust identification management, in order to maximize border security and facilitation benefits.

An industry exhibition will complement the Seminar with a broad range of products and services. Participate for an opportunity to interact with ICAO industry partners and experts to discuss the latest available traveller identification technologies.

For more information, visit [events.icao.int](http://events.icao.int) and contact [MRTDevents@icao.int](mailto:MRTDevents@icao.int)

# MOBILE SOLUTIONS: WHERE NEXT?



## ABOUT FRANK SMITH

Frank is Chair of the European Union (EU) working group on mobile solutions for the police and immigration, e-MOBIDIG (see [www.e-mobidig.eu](http://www.e-mobidig.eu)). He will continue in this role after retiring from the UK Home Office at the end of March 2015 as Deputy Director and Strategy Co-ordinator for the Home Office Biometric Programme. He has also worked part-time for the UK Border Force delivering front-line border control.

✈ No better area demonstrates the fast pace at which technology is advancing than mobile technology. When you consider the range – tablets, mini-tablets, smart phones and even smarter phones, 4G mobile broadband, mass availability of cheap consumer apps, the vast and increasing scale of use, social media, internet access, biometric verification, satellite-based geo-positioning – radical development is clearly taking place.

Where does this leave the police officer or officer enforcing immigration control who is on mobile patrol? Puzzled? Impatient? Empowered?

## WHAT IS E-MOBIDIG?

The European Mobile Identification Interoperability Group (e-MOBIDIG) brings together active innovators in the mobile solution field, including representatives of government, police, immigration, industry and standards bodies. The group considers how the technology is evolving, how to build good solutions and how to avoid expensive mistakes.

Best practice ideas distilled from the discussions are published on the e-MOBIDIG website. Current papers include strategy, requirements writing, benefits and standards. Notes of the meetings are also published openly on the website.

## WHAT ARE THE KEY TAKEAWAYS FROM THE GROUP?

**Even the latest and most exciting mobile device is just that - a device, not a complete solution.** Sound measures must be in place to connect a device efficiently and securely to the back-end systems and to the information the front-line officer needs.

**Analyze the advantages of joining up secure access to multiple existing systems in other agencies, as many organizations are increasingly doing.** Experiences from countries that have implemented mobile solutions with good connections to existing infrastructure have shown that this is a big advantage; a mobile project cannot easily overcome the limitations of a system if connected access does not already exist.

**Effective searches are not merely a means of detecting possible offenders.** This may also be the best way to establish that someone is who they say they are quickly and efficiently, without taking a long time and causing officers and those they need to question a great deal of unnecessary inconvenience.

**It is important to plan for the benefits you expect and to follow through to ensure they are achieved** (see e-MOBIDIG paper on benefits). Also key is to ensure that access is in accordance with the legal provisions of the country in question, with strict access control, proper procedure, and an appropriate understanding of the information returned.





**Can you justify sending officers out on mobile patrol without providing the technology for them to be as effective on the front-line as they are at the police station?** Waiting for technology to improve is no longer a good justification. If you are not already well along this path, now is a good time to begin.

**What blocks game-changing mobile solutions from being rolled out?** Delivering solutions may represent significant change, not just in terms of technology, but in actual working practice. **Good change management** is a necessity. At a recent meeting of e-MOBIDIG, a representative from IBM undertook a small survey with participants to feed back results at the next meeting. The study was linked to the results of a large global survey IBM had undertaken: *Making change work...while the work keeps changing.*

The results of the informal survey showed strong attention to technical issues. However, the need for more focus on key aspects of change management, while flagged as critical, was often not so well attended to. The issues identified included: leadership at all levels; making change matter to the organization; and building the skills and capability to make change happen in the organization.

**Avoiding over-dependence on any mobile device is wise.** With the pace of change in the market, making it as easy as possible to move on from yesterday's favourite device to a newer solution at

minimum cost and delay is smart. Having to replace the device is inevitable, but this should not call for the whole solution to be re-designed. One device is unlikely to be ideal for every user – **a range of sizes, formats and peripherals** will be likely to meet everyone's needs better – provided they can be actively renewed as the technology improves.

**Are mobile communications yesterday's problem? Does 4G solve problems of connectivity and bandwidth?** 5G is starting to be thought about, for the long term. Services continue to improve as new networks roll out, but never assume they will be ideal everywhere. **Test robustly** so you understand what connectivity you have. If your new solution offers great potential advantages but only if the devices remain online with a fast connection and officers need to use them where connectivity is poor, you may be heading for bad user reaction once the devices are rolled out. Watch out! Off-line capability with data replication to and from the device before and after operational use may be necessary.

**Finally, monitor usage closely and engage with users and local management** to ensure the device is working well and is being used as much as you expect. As one e-MOBIDIG participant explained, you must do a **particularly** good job of designing a good solution if it is mobile: once the officer takes the device out on patrol, he is only going to use it enthusiastically if he **wants** to; because he believes it **helps** him do his job better.

**MÜHLBAUER TECURITY®**  
COMPREHENSIVE GOVERNMENT 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](http://www.muehlbauer.de)



### LEARNING BY EXAMPLE

In e-MOBIDIG we have discussed many good examples of mobile solutions and have many others to table at future meetings. Examples have included solutions in Finland, France, Germany, Netherlands, Switzerland, UK and Poland; where there is a long history of experience with on-train mobile border control (the Polish Border Guard is already developing their third generation solution). Another country is developing plans for a very large-scale rollout of mobile devices for the police. We are aware of best practice examples in Australia, New Zealand and the US and we expect there are many others.

The United Kingdom has experience with immigration and the police using mobile fingerprint search devices, body worn video and tablet devices with access to case records in the field. The next challenge (and the UK is not alone) is to bring all this

experience together more effectively and coherently into a more strategic approach.

### TODAY'S HOT TOPICS

The e-MOBIDIG meeting in September 2014 hosted by the Swiss Border Guard and Swiss Customs was very productive. Participation by 10 European countries; a presentation sent by colleagues in Australia; representatives of 7 industrial interests, FRONTEX, ENLETS and the Fraunhofer Institute from Germany contributed to the success of the meeting as did the following topics of discussion:

- **Replacement of end-of-life devices** (without re-designing entire solutions), and **change management** (described earlier);
- **Fully effective strategic mobile solutions** for officers working remotely on a mobile basis;
- **Understanding examples of best practices** from different countries and industries;
- **Better design of the user front-end** to be able to provide the best experience for the operational officer. Why? To improve efficiency and to persuade a user to exploit the device as fully as possible. The German Border Guard has engaged the Fraunhofer Institute to research the ergonomics of mobile user interfaces and we hope to learn more from this work;
- **The US National Institute of Science and Technology (NIST) is reviewing its *Best Practice Guidance on Mobile ID*** from 2009. We look forward to sharing ideas with the Institute; and
- **An address by FBI specialist Jim Loudermilk at the Biometrics 2014 Conference in London** held in October, which emphasized the strong convergence of biometrics and mobile solutions.

### WHAT DOES THE FUTURE HOLD?

We have not seen the end of innovation and new surprises in the mass market for mobiles. There are definitely more to come in terms of power, miniaturization, new applications and better, faster, more pervasive mobile communications.

Over the next few years, we would expect mobile solutions for police and immigration to become a much more standard piece of equipment, just as the personal radio did a generation ago.

### HOW TO PROCEED?

Don't wait for the revolution to happen, get out there and make it happen. Better to start with a modest beginning than none at all, but aim to progress taking a holistic and strategic approach. The more experience you gain, the clearer you'll be about how to continue.

Expect resistance to change if you are doing something unconventional, so business change is important.

We leave the last word to Ujjwal Sabharwal of Morpho, India, speaking at the Biometrics 2014 conference in London:

**"Participate... the world belongs to those who show up". ■**



# TENTH MRTD SYMPOSIUM: SUMMARY AND CONCLUSIONS

✈ Next steps following the introduction of the ICAO Traveller Identification Programme (TRIP) Strategy were the focus of the Tenth Symposium and Exhibition on ICAO MRTD, Biometrics and Border Security. Barry J. Kefauver, ISO and NTWG expert, delivered the closing address at the Symposium. The following is a condensed summary of his remarks.





I am honored to be with you here today and very pleased that I have been asked to summarize this Symposium as we look to the future. In the nearly twelve months that have passed since we last met together here we have witnessed many changes, and unfortunately, some with tragic consequences.

In the largest sense, events over the recent past have affected our goals and objectives in a couple of highly tangible ways. First, our long-standing emphasis on sound and comprehensive identity management, which remains a very important component of this and previous Symposia, has been underscored and must assume even greater priority. Secondly, the interest in more effectively utilizing the tools (that is the "e" in the ePassport) over which we have labored for so long, has now moved from important to urgent.

---

**Enhanced tools of identity management will pay huge dividends in depriving the terrorist or international criminal of their most cherished asset: the ability to move freely in travel.**

These past three days have been filled with many issues, concerns, successes, failures, needs and realities. Previous Symposia have tended to coalesce around a core group of identifiable thematic variables that, within tolerances, allowed themselves to be discretely identifiable and definable.

This year's Symposium assumes a slightly different form and format. The concentration on the Traveller Identification Programme (TRIP) Strategy and the kinds of initiatives that this Strategy urges, call for other focal areas to assume a subset relationship to TRIP's umbrella breadth and depth.

#### **THE ICAO TRAVELLER IDENTIFICATION PROGRAMME (ICAO TRIP) STRATEGY**

With the formal and complete adoption of the TRIP Strategy, ICAO has taken a light-years leap forward and has chosen direction and purpose that no longer evoke head-scratching; that crossroad has been crossed and ICAO is on a more clearly defined, and substantially broadened, course.

As Jim Marriott reported, the 38<sup>th</sup> Session of Assembly adopted the ICAO TRIP Strategy in order to establish the goals and objectives of traveller identification management; to lead and reinforce a global approach; and to provide direction for action to ICAO, States and the many international, regional and industry partners in identification management.

ICAO's leadership in pursuing these Strategic Objectives is a platform from which all other travel document and border management activities will more effectively flow, to bring together the five (or seven as one presenter suggested) elements of identification management, and to acknowledge the singular importance of partnerships. This framework yields a new approach to the next thematic focus: global issues.

### THE CHALLENGE OF IMMENSE GROWTH IN NUMBERS AND THE COMPLEXITY IN THE GLOBAL MOVEMENT OF PEOPLE

In the twelve months since the last symposium, terrorism has worn an increasingly barbaric cloak of acts that are viewed as unthinkable by virtually the entire world. The terrorist's arm of evil has reached levels that clearly demonstrate that these hatreds know no geographic boundaries, nor is there respect for any aspect of humanity. Indeed, much of the world has been touched by heinous acts of barbarism seldom seen, if ever encountered, before.

Enhanced tools of identity management will pay huge dividends in depriving the terrorist or international criminal of their most cherished asset: the ability to move freely in travel. The use of false identity has been with us since before the advent of the ePassport and remains with us today. However, the nature of this deception has shifted from being one that is driven by document fraud to what is now predominantly identity fraud.

The current generation of biometric enabled passports has forced criminals to use new and different ways to exploit the cracks in our ability to determine true identity. One of the gaping holes is the growth of real passports issued with false identities, which is a dangerous mockery of the ePassport. Always elusive, the identity judgments associated with passport entitlement are the

foundation of our MRTD issuance processes and will affect the trust and confidence that inspection authorities can hold in linking the bearer and the document.

Since the last symposium, we have seen the successful use of stolen passports that have grabbed widespread public attention and brought new meaning to the Stolen and Lost Travel Documents (SLTD) programme and the critical need to use it. Also, as the volume of air travel moves toward an anticipated annual six billion, issuers and inspectors must remain steadfast in never allowing volume to compromise standards.

### THE PROPER USE OF ELECTRONIC VERIFICATION AND INTEGRITY TOOLS IN ePASSPORTS

Unless and until these tools are effectively used, the energy, time and money we have invested in ePassport advancements will not be realized, and perhaps of greater concern, the use of inadequately inspected documents will yield a dangerous and false sense of credibility and security.

In realizing border control as definitively facilitating those who are genuine and deterring the fraudulent, we have heard indelibly that the use of the Public Key Directory (PKD) is a key tool, but that it is only one aspect of a properly managed border control system. This Symposium, even more strongly than others in the







past, underscored the importance of PKD membership. Also, the message became clear that it is not enough to have 45 States as members of the PKD, because only when those 45 States and others with ePassport capability USE the document, can we declare success. There are over half a billion eDocuments in circulation and the numbers grow each day.

---

The heightening stakes of terrorism and the shifting face of threats like document fraud, which is now segueing into identity fraud, create new and perhaps unknown methods of making mischief.

#### CIVIL REGISTRATION AND VITAL STATISTICS ARE ESSENTIAL COMPONENTS IN AN OVERALL TRIP STRATEGY

Obtaining a birth certificate of another person, living or dead, is a lot easier than falsifying a passport. While the uniform application of standards and enhanced technologies have dramatically improved the quality of travel documents, doing the same for evidence of identity - such as breeder documents like birth certificates - requires a broader and more comprehensive approach, frequently known as the social footprint. It is no longer enough for issuers to strive to produce a secure passport; we must now endeavor to determine true identity.

The transition from where the world stands now with regard to identity management and the quality of civil registration programmes must be viewed as a planned and systematic consciously-sought effort over time; it cannot be done all at once. We know bad people do bad things. However, we must ensure that every individual is afforded his or her fundamental right to a civil identity and to ensure that the information is collected accurately and reflects the existence of a unique, living human being.

#### INTEGRITY AND TRUST

Ranging from sound and effective initial procurement practices; through the ways in which we handle the raw materials that eventually comprise a passport book; through to the ways in which we deal with human resources, storage and processing facilities and legal frameworks for breaches such as passport and identity fraud; the issue of integrity is fundamental and absolute.



The heightening stakes of terrorism and the shifting face of threats like document fraud, which is now segueing into identity fraud, create new and perhaps unknown methods of making mischief. Just as we have rallied together to develop the world's most secure passport, we must now join forces to ensure the systems on which those documents rely for their credibility, are equally sound and effective.

### CONCLUSIONS

With the 38<sup>th</sup> Assembly adoption of the ICAO TRIP Strategy forming a cornerstone of last year's Symposium, the groundwork has been laid such that this year's Symposium can look toward the demands and opportunities we now must face in fulfilling the promise of TRIP.

With ICAO as the catalyst to bring together the multidimensional efforts of States and the many international, regional and industry partners, we now have that framework and we are beginning to reap the respect that these functions deserve.

Ambitious yet feasible global solution initiatives such as ABC can now confidently rely on ICAO TRIP for the solid worldwide foundation on which to flourish.

I don't think we have left a previous Symposium where the challenges of the global future were as daunting, nor did the future look as bright and as exciting as it does today. I thank all of you for your time and attention throughout the Symposium and I look forward to our collective next steps. ■





# REFORMING THE IDENTIFICATION MANAGEMENT SYSTEM: THE GEORGIAN EXPERIENCE



#### ABOUT LEVAN SAMADASHVILI

He served in the Public Services Development Agency (PSDA) between 2009 and 2014 as Project Manager, Deputy Chairman and Chairman. His current international consultancies involve organizational management and registration system reforms. He also works at the Innovations and Reforms Centre and the Georgian Institute of Public Affairs.

#### ABOUT NATO GAGNIDZE

She served as Deputy Chairman of the Civil Registry Agency and the Deputy Minister of Justice from 2004 to 2007. Later, she founded the Innovations and Reforms Centre, which as an NGO, implements projects in the fields of personal data protection, good governance and migration. (Photo not available.)



Identification management has become a key concern of the modern world. Efficient systems of personal identification are crucial for national and international security given the role they play in acts of terrorism, identity theft, border management and migration.

The world's response to the identity management challenge is no surprise. Since 9/11, billions of dollars have been invested worldwide in new technologies and the market for security has increased significantly as governments integrate biometrics in their systems.

However, governments often miss the target by investing in highly technological solutions that are linked to inadequate identification systems. Fancy documentation is not a solution; a national system of identification must ensure that the information recorded is the actual data of the document holder.

### TRANSFORMATION CHALLENGES

Georgia is one example of a State that was able to transform a poorly managed identification system into a better functioning model. Some obstacles included:

**Rampant corruption and bureaucracy** - Passport offices were known for corruption, artificial burdens and questionable service. Passports and national identification documents were often forged. False records were created and legitimate ones destroyed. Everything was possible.

**Poor inter-agency collaboration** - Prior to the reform in 2006, civil status registration was the responsibility of the Ministry of Justice (MoJ), while issuance of identification documents and address registration was the function of the Ministry of Interior (Moi). These ministries did not have electronic databases and did not exchange information properly. Civil acts and certificates were filed manually. Changes in birth, death and other personal data were not made in a timely fashion and, therefore, not reflected in identification documents.

Following the relocation of Passport and ID Issuance under the MoJ, another serious problem emerged due to delays in receiving updates from the Moi on *wanted persons*. This resulted in passports being granted to internationally wanted persons and cases of travel documents being refused to individuals who had been cleared of any wrongdoing.

**Poor databases** - While there was scattered foreign passport data available electronically, most data was recorded on paper and stored in local and regional service offices. The system was dependent on paper archives and was unreliable. The regional offices (registering bodies) often disregarded notifications or submitted them late to the archives. Storage conditions in the archives were very poor and valuable information was sometimes destroyed by mould, moisture and even fire.

Later, while digitizing older records in order to form the first electronic database, major problems were encountered. An estimated 1.2 million entries were missing and more than 370,000 errors were identified in newly entered data. Moreover, there was profile duplication in cases where two people had the same PIN. In order to correct these issues, over two million photos were scanned from older applications and loaded in the database for identification purposes.

**Deceased people voting and receiving pensions** - In difficult socio-economic times, it was in the interests of families to conceal deaths so they could further benefit from State



assistance and, as such, many deaths were not registered with the MoJ. Additionally, because the data exchange between Passport Offices and Civil Status Registration bodies was poor, death records were often not transferred.

**Unregistered births** - Similar to death registration, birth registration was also dependent on the will of the citizen. Many citizens only applied to the MoJ for education or health-related needs and did not bother to document new births. Births that occurred outside of medical institutions had their own problems and deterrents since registering them involved lengthy procedures in court and additional costs.

**An overwhelming number of undocumented citizens** - With so many unregistered citizens and so many holding documents from the Soviet Union, identities had to be properly documented. To be granted identification documents, individuals had to first prove their citizenship, which was difficult in the absence of reliable data archives. In many instances, the birth had to be established before the citizenship could be. This, in itself, was a drawn-out process.

### THE CRITERIA FOR SUCCESSFUL REFORM

Three important conditions were established as the foundation for successful reform:

**A single entity in charge** – Unification of reforming areas under a single umbrella was crucial for improved coordination and efficient decision-making. This was critical, because the ideal condition for true reform is a dynamic environment where issues that require adaptive, quick solutions can be effectively dealt with. Outdated and corrupt registration systems require radical changes and agile decision-making. This is particularly important in States with bureaucratic traditions where agencies are not cooperative in sharing information.

**A unified database** – Obviously, a reliable database is the foundation of any identification system. The data must be timely, secure and accessible. In Georgia, unifying scattered data in a national database also allowed for better monitoring and control of regional offices.

**A single standard** – Establishing a universal standard was essential to quality, service, procedures, timelines, etc. Technology and process automation played an instrumental role as a monitoring mechanism and in practically enforcing changes brought on by legislation.

### HOW THE GEORGIAN MODEL WORKS

**Three functions under one department** – One department is responsible for three key identification management functions: document identification and address registration; civil status registration; and the formation of a population registry.

**Front office - back office division** – Though a front-and-back office model is not common in post-Soviet government services, the separation of functions was crucial in that it:



- *Reduces corruption* by eliminating personal interaction with decision-makers so there are fewer opportunities for unlawful activity. In Georgia, front office employees do not know which officer in the back office will process an application, because the software does not allow the front office employee to select a back-officer.
- *Promotes work efficiency* since front office employees focus on service and ensure a pleasant experience for the applicant, while back offices are called upon to perform lawful and accurate decision-making. These are two different functions that require different competencies.

**State-wide single-source identification** – In the absence of properly functioning registries, government agencies create their own databases to support passport issuance, elections, social assistance administration, etc. Because these databases are not connected, information isn't always reconciled – one individual may have a different name, surname, address or PIN attached to his profile. Given the inter-relations between governmental functions, this creates practical problems.

Therefore, avoiding overlaps and developing a single source for identification management was critical. In the first place, it eliminated confusion over who bore the responsibility for providing secure, accurate identification services. This promoted improvements and helped to mobilize resources to improve data. Secondly, a single source of identification provided opportunities for other agencies to detect inaccuracies and provide feedback to the responsible body. As additional agencies became users of this single source, more inaccuracies were identified and flagged for further investigation and correction. Third, to a great extent, it solved problems with discrepancies among databases. Finally, agencies saved resources by not duplicating functions.

**Electronic exchange of information** – Comprehensive identification management requires efficient information exchange among government entities. At a minimum, the following information had to be processed effectively:

- *Birth registration* – in Georgia, birth centres are obliged to submit medical notice within five days of birth or face penalties. Additionally, when births occur outside medical institutions, local government entities are obliged to notify the registering body;
- *Death registration* – medical institutions are obliged to submit medical notice within five days of a death or face penalties;
- *Change of personal data* – a change in first or last names, or other personal data, automatically disables identification documents and forces document holders to have them corrected;
- *Criminal records, counterfeit documents and wanted persons' database* – triggers automatic system verification with the respective database.

The increased use of electronic data exchange offers many benefits: security – because data is verified between responsible

... governments often miss the target by investing in highly technological solutions that are linked to inadequate identification systems.

State bodies, discouraging fraudulent documents; convenience – because citizens are no longer obliged to produce multiple documents since administrative bodies already have them recorded; speed – because the process is faster; and integrity – because it reduces personal interaction with government bodies, thereby minimizing opportunities for corruption.

**Address registration policy** – Obviously, address registry must accurately reflect factual, permanent residences. However, several circumstances, typical to post-Soviet countries, created problems. During the Soviet era, registration (called “propiska”) provided registered individuals with certain rights on the property. Even today, because of experiences like these, owners often feel reluctant to grant renters or other factual dwellers the right to use an address for registration. The other problem is that many properties were not formally legalized, which made it impossible to provide a proof of ownership. Therefore, legislative amendments have been enacted to allow residents to register at an address with two signatory witnesses (who bear criminal liability).

**Documents and biometrics** – In Georgia, photos are used in biometrics and all active profiles stored in the database have photos attached to them. A Face Recognition System (FRS) and an ICAO compliant software is automatically used in the document issuance processes. Since 2010, Georgia has been issuing ICAO compliant Biometric Passports which incorporate fingerprints and other data. In 2011, Georgia introduced a polycarbonate, secure, national identification card with a built-in chip that contains a biometric photo and other personal data.

#### SYSTEM DRAWBACKS

The main criticism of the Georgian model is in the use of personal data. Centralized, massive databases, unique PINs,



With the initial focus on tackling rampant corruption and inefficiencies, the issue of privacy protection was not effectively addressed.

quick information exchanges, and other characteristics that result in greater efficiencies, create risks of personal data abuse. With the initial focus on tackling rampant corruption and inefficiencies, the issue of privacy protection was not effectively addressed. Governments must successfully solve the efficiency-privacy trade-off.

Another major challenge involves the accuracy of the address registry. Problems associated with street names and numbers, address duplication and properties without addresses remain the weakest link in the Georgian identification system to date.

#### FINAL POINTS

While every State must identify its own priorities, Georgia's identification system was shaped and developed according to the Georgian context – a pressing need for efficiency and quality service free of corruption. The reform of the Georgian identity management system that began in 2006 yielded tremendous results:

- The Unified Database of Population Registration responds to an estimated 30,000 daily requests from public and private institutions;
- Average service time is six to seven minutes;
- Average waiting time is five minutes;
- The largest service center in Tbilisi services up to 8,000 individuals daily; and
- Client satisfaction has been rated at over 92% for the last several years.

While these results are impressive, there always remains room for further improvements. In the contemporary world, as new threats and challenges emerge, and technology and know-how develops, States are expected to respond appropriately, refine their systems and make them as efficient, convenient and secure as they can be. ■







# AN INDUSTRY LEADER IN SECURE TRAVEL DOCUMENTS ISSUANCE

Providing seamless, cutting edge thermal retransfer printing technology, GET Group continues to provide governments and institutions around the world with innovative, high-secure document personalization.

Using non-organic pigment inks, the documents personalized by GET- Toppan technology have a unique "forensic fingerprint" with proprietary dot-on-dot printing and special holography while assuring color fidelity, stability and resistance to UV light/fading.

# VERIDOS

IDENTITY SOLUTIONS

by Giesecke & Devrient  
and Bundesdruckerei



## Veridos Secures Identities

**Identity Solutions.** Veridos is a joint venture between Germany's best-known providers of secure government identity solutions. Created by pooling together the international government solutions portfolios of Munich-based Giesecke & Devrient and the Berlin-based Bundesdruckerei, governments are served with the most secure and innovative identity solutions, making it their best choice for protecting and safeguarding their citizens. Find out more about how Veridos can help you make the most secure decision at SDW 2015 in London.

[www.veridos.com](http://www.veridos.com)