

# ICAO TRIP

NEWS AND FEATURES ON THE ICAO TRAVELLER IDENTIFICATION PROGRAMME - VOL.11 - NO.2

## ASSURED IDENTIFICATION

IDENTITY MANAGEMENT BEST PRACTICES  
IMPLEMENTING NEW SPECIFICATIONS  
IMPROVING THE SECURITY OF ePASSPORTS  
INCORPORATING INTERNATIONAL STANDARDS  
SHAPING FACILITATION FRAMEWORKS



| ICAO

SECURITY & FACILITATION

# VERIDOS

IDENTITY SOLUTIONS

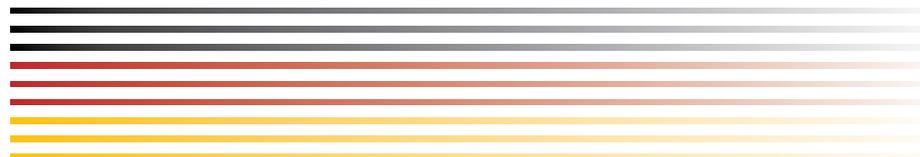
by Giesecke & Devrient  
and Bundesdruckerei



## Veridos protects identities

**Identity Solutions.** Veridos is a joint venture between Germany's best-known providers of secure government identity solutions. Veridos was created to pool the international government solution portfolios of Munich-based Giesecke & Devrient and the Berlin-based Bundesdruckerei. With its unique, highly secure and innovative identity solutions it is the best choice for governments worldwide in their efforts to keep borders and citizens safe. Find out more about how Veridos can help you make the most secure decision at Booth 11 and [www.veridos.com](http://www.veridos.com).

Join Veridos at Booth 11  
ICAO TRIP Symposium 2016  
November 15 to 17, Montréal, Canada





# ICAO

ICAO TRIP MAGAZINE  
VOLUME 11, NUMBER 2, 2016

#### Editorial

TRIP Programme—Aviation Security  
and Facilitation Policy Section

Editor-in-Chief: Narjess Abdennebi

Tel: +1 (514) 954-8219 ext. 8374

E-mail: fal@icao.int

Coordinator: Garleen McGann

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

E-mail: fal@icao.int

#### Content Development

Senior Editor: Allisun Dalzell

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

E-mail: ICAOTRIPmagazine@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 *TRIP Magazine* 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 *TRIP Magazine*, please contact ICAOTRIPmagazine@icao.int.

Opinions expressed in signed articles or in advertisements appearing in the *ICAO TRIP Magazine* 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 TRIP Magazine* 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 © 2016

International Civil Aviation Organization

Printed by ICAO

## Contents

3

### Message from the Editor-in-Chief

Narjess Abdennebi highlights recent developments in aviation security and facilitation.

5

### The OSCE Surveys its States to Identify Best Identity Management Practices

The Organization for Security and Co-operation in Europe has taken steps to improve global information sharing in identity management by surveying its 57 States

8

### Enhanced Use of ePassports

IATA's Christopher Hornek looks at why States, airlines and airport operators need to optimize the use of the ePassport as a tool for shaping facilitation framework.

12

### International Standards for Civil Registration and Vital Statistics

Srdjan Mrkić, Chief of the UN Statistics Division, explains the critical need for incorporating international standards for civil registration and vital statistics at a national level.

16

### The OECS Single Domestic Space for Travel: Underpinning the OECS Economic Union

Lorraine Nicholas, describes the progress the Organisation of Eastern Caribbean States has made in establishing a single domestic space for travel that will facilitate travel for OECS citizens travelling in EU States.

20

### ICAO New Technologies Working Group (NTWG) - Request for Information (RFI)

ICAO's Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP) and its NTWG issued an RFI to all interested parties.

24

### The Origin of Origins

As biometrics continue to improve the security of ePassports, Charles de Coussèin looks at the weakest link in the identity chain: the evidence of identity.

27

### The Roadmap for Implementing New Specifications

As travel documents advance and new security specifications are adopted, getting information to States is critical. Tom Kinneging describes how guidance and implementation strategies can be shared.

31

### The Evolution of the Japanese Passport

A look at how the passport has progressed in the last 150 years.

32

### The Search for Host States

34

### The Validation Process for a Standardized Training Package

The development of the *Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1* training course.

38

### ICAO's New infoTRIP Platform

Renee Ong-de-Jong describes the work of the Implementation and Capacity Building Working Group and its sub-working group in establishing the online TRIP Platform, the secure portal for storing, using and maintaining information.

41

### Guidance for Circulating Specimen Travel Documents

To facilitate international travel, States must share their new or updated passport specimens with other States – processes need to be followed to achieve the minimum standards and ensure the features are communicated.



## TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG/MRTD)\*

### Member States

Argentina	Indonesia	New Zealand	Sweden
Australia	Iraq	Nigeria	Switzerland
Canada	Ireland	Portugal	The Former Yugoslav Republic of Macedonia
Chile	Italy	Qatar	Ukraine
China	Japan	Republic of Moldova	United Arab Emirates
Colombia	Kenya	Russian Federation	United Kingdom
Egypt	Kyrgyzstan	South Africa	United States
France	Luxembourg	Spain	Uruguay
Germany	Netherlands	Sudan	
India			

\*The above listing of the State Members of the TAG/MRTD were nominated after ICAO State Letter EC 6/8 – 16/48 dated 3 June 2016 was issued, where all ICAO Member States and select international organizations were invited to nominate qualified and experienced experts to sit as Members and Observers of the new Technical Advisory Group on the Traveller Identification Implementation Programme (TAG/TRIP).

## OBSERVER INTERNATIONAL ORGANIZATIONS

Airports Council International (ACI)  
Banjul Accord Group Aviation Safety Oversight Organisation (BAGASOO)  
Civil Aviation Safety and Security Oversight Agency (CASSOA)  
European Civil Aviation Conference (ECAC)  
European Union (EU)  
International Air Transport Association (IATA)  
International Coordination Council of Aerospace Industries Associations (ICCAIA)  
International Criminal Police Organization (INTERPOL)  
International Labour Organization (ILO)  
International Organization for Migration (IOM)  
International Organization for Standardization (ISO)  
Organization for Security and Cooperation for Europe (OSCE)  
Organization of American States (OAS)/  
Inter-American Committee on Terrorism (CICTE)  
United Nations Counter Terrorism Executive Directorate (UNCTED)  
United Nations (Department of Management)  
United Nations High Commissioner for Refugees (UNHCR)  
United Nations Office on Drugs and Crime (UNODC)  
World Tourism Organization (UNWTO)



# IMPROVING FACILITATION WITH STANDARDS, GUIDANCE AND INFORMATION SHARING



✈ In October the 39<sup>th</sup> ICAO General Assembly came to a successful conclusion in Montréal. Under the Strategic Objective of Aviation Security and Facilitation, the Assembly adopted the United Nations Security Council Resolution on Aviation Security and endorsed the continued development and implementation of the ICAO Traveller

Identification Programme (TRIP) Strategy, including travel documents, the ICAO Public Key Directory (PKD), and the provision of related assistance and training to States.

The week before the Assembly convened, another historic landmark was achieved when the UN Security Council (UNSC) unanimously adopted Resolution 2309 (2016), following a briefing by ICAO's Secretary General. Dr. Fang Liu called for closer collaboration in ensuring the security of global air services, including the prevention of terrorist attacks against civil aviation. Along with enhanced screening, security checks and facilitation, the UN Security Council called for strengthened cooperation and information-sharing among States, and for airlines to provide Advance Passenger Information (API) to national authorities in order to track the movement of individuals identified by counter-terrorism committees.

These recent developments help shape and support the leadership work of ICAO by linking aviation security and facilitation. The importance of traveller identification has been emphasized, and a renewed impetus is given to the implementation of all aspects of the ICAO TRIP Strategy.

As we look to build on ICAO's leadership role in the field of traveler identification management, including providing implementation support and guidance to States, this issue features a number of articles related to this theme.

In consideration of the advances in travel document technologies and the need for ensuring that stakeholders configure their systems to fully leverage any security and facilitation advantages offered by new or enhanced international specifications, we recently published new guidance material on the TRIP Strategy for implementers of both inspection systems and MRTDs. In addition to the new *Roadmap for Implementation of New Specifications for MRTDs*, we're sharing guidance that helps States with the task of circulating specimens of new passports to other States to make them aware of new designs

and features, and to support the broader objective of facilitating international travel.

The link between evidence of identity and travel documents is key to achieving the ICAO TRIP objective of enabling States to uniquely identify individual travellers. In this issue we look at the work being done by the Organization for Security and Co-operation in Europe (OSCE) to strengthen the critical links between civil registry systems and travel document issuance processes to combat fraudulent practices.

An important role of the TRIP Strategy involves examining how ePassports are being developed and used around the world and IATA has provided a good account of how facilitation benefits can be optimized thanks to the use of automation.

Developments at both the regional and national levels are highlighted in this edition as we review the progress being made in the implementation of the Single Domestic Space by the Organisation of Eastern Caribbean States (OECS), and look at how the Japanese passport has evolved over the last 150 years.

As part of ICAO's work to provide TRIP-related technical assistance to States, we recently launched a new ICAO Training Package (ITP) entitled 'Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1'. This is a great example of international collaboration and cooperation in the field of traveller identification and ICAO genuinely appreciates the support and work of all concerned.

One of the most important ways in which ICAO provides assistance to Member States is through the ICAO TRIP Regional Seminars which take place twice a year at different locations around the world. The next seminar will be held in St. John's, Antigua and Barbuda from 31 January to 2 February 2017. As we plan ahead, ICAO would be keen to hear from States with an interest in hosting a regional seminar in the future. Further details regarding hosting a regional seminar – and the related benefits – are provided in this edition, and more information on ICAO TRIP events worldwide can be found on our updated Facilitation webpages at [www.icao.int/Security/FAL/TRIP/Pages/default.aspx](http://www.icao.int/Security/FAL/TRIP/Pages/default.aspx)

We welcome your feedback and suggestions for articles for future issues. We want to hear from States and industry about the developments and challenges you're working on – please direct your contributions and comments to [ICAOTRIPmagazine@icao.int](mailto:ICAOTRIPmagazine@icao.int)

Until then – happy reading! ■



## ICAO TRIP REGIONAL SEMINAR ANTIGUA 2017

The Seminar, hosted by The Ministry of Public Utilities, Civil Aviation and Transportation of the Government of Antigua and Barbuda, will address the five elements of the ICAO Traveller Identification Programme (ICAO TRIP) Strategy, including: machine readable travel document (MRTD) standards, specifications and best practices; secure travel document issuance; robust evidence of identity processes; and information sharing technologies highly relevant to the execution of the United Nations Security Council Resolutions 2178 (2014) and 2309 (2016) on combatting foreign terrorist fighters, with a special focus on effective border control management.

An exhibition will complement the Seminar, showcasing a broad range of products and services related notably to travel document security applications, border inspection and automated border control systems. Seminar participants will have an opportunity to interact with ICAO industry partners and experts to discuss the latest available traveller identification technologies.

Register online and visit [icao.int/Meetings/TRIP-Antigua-2017](http://icao.int/Meetings/TRIP-Antigua-2017) for more information.



ICAO

SECURITY & FACILITATION

# THE OSCE SURVEYS ITS STATES TO IDENTIFY BEST IDENTITY MANAGEMENT PRACTICES



## ZORAN DOKOVIĆ

He joined the OSCE's Office for Democratic Institutions and Human Rights (ODIHR) in 2008, where he works as Migration/Freedom of Movement Adviser. His work focuses on providing assistance to the OSCE participating States in developing and adapting their administrative and legislative frameworks for population registration to facilitate citizens' access to state-guaranteed social and political rights. His work also supports participating States in promoting wider cross-border travel and person-to-person contacts within the OSCE region.



## SIMON DEIGNAN

He manages the OSCE's Travel Document Security Programme within the Transnational Threats Department, work that includes document security, identity security, access to databases, training in the physical inspection of travel documents, and expanding the use of Advance Passenger Information. He has been working on OSCE issues since 2010 including as a Political Advisor for both the Irish and Swiss Chairmanships. Prior to the OSCE, Simon worked in the private sector for an international management consultancy.

## ✈ THE RISKS

Several years ago a US investigator was able to obtain four genuine passports using fake names and fraudulent documents. In one case, he used the Social Security number of a man who had been deceased since 1965. In another, he used the Social Security number of a fictitious five-year-old child created for a previous investigation, along with an identification that showed he was 53 years old. The investigator then used one of the fake passports to buy a plane ticket, obtain a boarding pass, and pass through a security checkpoint at a major airport.

Earlier this year, it was discovered that thousands of Indian citizens had paid a criminal gang for false birth and marriage certificates from the former Portuguese colonies of Goa, Diu and Daman. According to Portuguese law, Indibwgans born in these areas before 1961, or their children and grandchildren, can apply for Portuguese passports because these were colonies of Portugal until that year. However, British and Portuguese police learned that this loophole was being systematically abused in order to obtain a genuine EU passport using false breeder documents.

These two widely reported examples<sup>1</sup> illustrate how gaps in the identity management process can be exploited to acquire genuine passports through fraudulent breeder documents.

Following UN Security Council Resolution (UNSCR) 2178, which expressed grave concern about those who attempt to travel to become foreign terrorist fighters, there is a major focus in preventing the cross-border movement of terrorists and terrorist groups. Since the Resolution was adopted, States have undertaken measures to strengthen border controls, increase information sharing, and enhance the use of watch-lists. The increased restrictions will force terrorists to examine other means of crossing borders.

Despite the fact that border controls are tightening, and that we have highly secure passports with biometric chips, the processes for acquiring a genuine passport remain open to abuse by criminal and terrorist groups.

Identity deceptions are particularly prevalent when there are disconnects between passport and civil registry identity management systems - with civil registry systems often being the weaker link.

## INTERNATIONAL EFFORTS

The ICAO TRIP strategy clearly recognizes that travellers' identity verification is about more than ensuring a secure travel document. The strategy outlines the so-called five dimensions of traveller identification management, of which Evidence of Identity is one of the key parts. The ICAO Implementation and Capacity Building Working Group (ICBWG), to which the Organization for Security and Co-operation in Europe (OSCE) is an observer, has been working steadily on the issue, and has produced excellent guidance on Evidence of Identity. The ICBWG, in co-operation with regional partners, also remains available to assist States with assessments and developing robust evidence of identity



processes. The EU and others are also engaged in initiatives to improve the security of breeder documents.

Though the good news is that this gap is now recognized and efforts are being made to address it, to date there is little reliable data on the depth and scale of the problem.

#### WHAT HAS THE OSCE BEEN DOING?

As the world's largest regional security organization, with 57 participating States spanning five continents from Vancouver to Vladivostok, the OSCE is well-positioned to support global efforts to improve identity management processes. OSCE participating States have agreed to comply fully with the recommended ICAO minimum security standards for the handling and issuance of passports.

Following the adoption of UNSCR 2178, there was a call from the OSCE Ministerial Council to prevent the movement of foreign terrorist fighters through effective border controls and controls on the issuance of identity papers and travel documents. In addition, OSCE participating States have also adopted a range of commitments aimed at facilitating freer and wider travel in the OSCE region, and improvements in the security of travel documents has a direct and positive effect on visa facilitation processes. In line with these dual mandates, the OSCE Executive Structures actively co-operates to support participating States in both the security of borders, and the facilitation of cross-border mobility.

In November 2013, in order to support the ICAO TRIP Strategy, the OSCE organized an Expert Roundtable on *Addressing the Link between Travel Document Security and Population Registration/Civil Registration Documents and Processes*. It is worth repeating one of the primary recommendations that emerged from this roundtable:

“Given the diversity of civil registry systems in operation and national discrepancies in how well they are linked to travel document issuance, the OSCE should develop a compendium of best practices on effectively linking the most common civil registration systems in the OSCE region with travel document issuance systems. This compendium would allow OSCE participating States to compare their own system to best practice examples that are most similar to their own system, thereby allowing them to spot potential weaknesses. Likewise, this compendium could be used for capacity-building purposes in the OSCE area.”

In response to calls from the expert community to contribute to improved information sharing on good practices in identity management, in 2014 the OSCE initiated a consultative process involving joint work by its Vienna-based unit working on international travel security, and its Warsaw-based unit working on population registration and freedom of movement. Coming at the problem from both the perspective of security, and of rights to human contacts across borders, these joint efforts agreed the aim of developing a *Compendium of Good Practices in Identity Management in the OSCE Region* was important. Moving forward, the OSCE organized an expert group meeting in March 2016 to determine the content of a draft questionnaire to be sent to the relevant authorities of OSCE participating States. The experts also discussed other aspects of identity management systems which should be further researched and reflected in the planned Compendium, steps that included taking stock and reflecting on existing good practices.

#### DATA COLLECTION AND GOOD PRACTICE PROMOTION

Baseline data on the identity management systems of OSCE participating States is currently being obtained by means of a questionnaire that was developed with the assistance of a select group of identity management experts. This questionnaire was distributed to the relevant travel and identity documents issuance authorities in 57 OSCE participating States during the summer, and responses are now being collated as one element of preparation in the Compendium publication.

It is hoped that by responding to carefully designed questions, the authorities will provide feedback on the main characteristics of their national identity management system, looking specifically

into the characteristics of their civil registration system, their ID and travel document issuance system, data sharing between the two systems, verification of the identity of both citizens and resident non-citizens, internal audit, and staff vetting procedures.

As part of the development process, the OSCE will also organize regional expert meetings to present preliminary results and findings obtained from the questionnaires and facilitate expert discussions aimed at reaching a shared agreement on specific identity management policies that constitute cases of good practice and contribute to increased security of the identity management framework.

The development of this Compendium has several important objectives:

- First, it will support increased data collection on existing policies on identity management and use of evidence of identity as part of the travel documents issuance process;
- Second, it will help increase awareness among State authorities on the best practices related to secure identity management and the issuance of travel documents;
- Finally, it will provide guidance when developing procedures for issuance of travel documents based on verifiable evidence of identity.

### NEXT STEPS

The development of the Compendium goes hand in hand with the global initiatives that are led by ICAO to promote evidence of identity as part of the ICAO TRIP Strategy. The OSCE intends to work with the ICBWG to explore how the Compendium can be both further disseminated and further utilized beyond the OSCE region, as well as whether there are opportunities for its development in support of capacity-building activities.

In addition to supporting the security angle of traveller identification, the Compendium initiative and the OSCE's promotion of good practices in identity management more generally, also, aims to support citizens' access to civil and political rights; the implementation of e-government services; accurate voter registration; and the protection of a range of other human rights. ■

<sup>1</sup> Authors provided seven source references that included:

<http://www.gao.gov/products/GAO-10-922T> and

<http://portugalresident.com/over-1000-indians-%E2%80%99Cbuy%E2%80%99D-portuguese-nationalities-on-black-market>

Additional links provided upon request to: [ICAOTRIPmagazine@icao.int](mailto:ICAOTRIPmagazine@icao.int).

Listen

Develop

Deliver

**WORLD CLASS BORDER SECURITY  
FOR A WORLD THAT'S  
ON THE MOVE.**

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

**cbn**  
CANADIAN  
BANK NOTE  
COMPANY, LIMITED

PRINCIPLED SECURE SOLUTIONS SINCE 1897

# THE ENHANCED USE OF ePASSPORTS



## CHRISTOPHER HORNEK

He is a Manager for Aviation Facilitation at IATA, where he works on passenger data exchange programmes, border control, travel documents and general facilitation issues. In this function, Christopher contributes to the IATA/Control Authorities Working Group (CAWG), ICAO Facilitation Panel, ICAO Technical Advisory Group (TAG)/Traveller Identification Programme (TRIP), as well as its New Technologies Working Group (NTWG). From 2003-2015 Christopher was with the Organization for Security and Co-operation in Europe (OSCE), where he served in different positions in Turkmenistan, Uzbekistan and as Travel Document Security (TDS) programme manager.

✈ The increasingly universal use of biometrics and other new technologies are shaping the future of the global border security framework as we speak. At the International Air Transport Association (IATA), we are working to define that framework on behalf of our member airlines, in partnership with airports and governments, and in close cooperation with international organizations, including the International Civil Aviation Organization (ICAO).

The driver for these advancements is as much security, as it is facilitation. The need for improvements is clear. Airport infrastructure status quo will not be able to absorb the ever increasing number of passengers that are projected for 2030 and beyond, when loads are estimated to rise above six billion annually.

This article will focus primarily on enhancing throughput on international flights when passport control and other sovereign entry requirements are involved.

To help rectify the situation, States, airlines and airport operators should take better advantage of the many facilitation tools available to improve border and aviation security, as well as the End-to-End (E2E) passenger experience. These tools consist of electronic passports, biometric verification, passenger data exchange, Registered Traveller Programmes (RTP), pre-clearance arrangements, Automated Border Control (ABC), Smart Security as well as the automation of other procedures that are associated with international travel by air.

While the ICAO Traveller Identification Programme (TRIP) has assembled many facilitation elements into a general strategy, neither Governments nor the private sector have aligned all of these tools into a consistent framework that can be applied across jurisdictions. As we look to the future, an ICAO Global Aviation Facilitation Plan (GAFP) could play the role of a unifying and integrating factor in this regard.

## ePASSPORTS

The ePassport is now more than 10 years old and almost a billion exemplars have been issued worldwide. Though the mandatory issuance of ePassports is not a standard of ICAO Annex 9 – *Facilitation*, the majority of ePassports have been issued in the largest aviation markets which include Asia and Pacific, Europe, North America and the Middle East. Global issuance of ePassports have now reached a critical mass which allows for international travel with improved facilitation through airline, airport and Government processes. But the results are still meagre.

The reality is that the ePassport is overwhelmingly treated as a traditional passport, which means that the main security and facilitation benefits of the passport chip: 1) authenticating electronic security features through digital certificates and 2) matching the passenger with the passport through the use of biometric verification – are not being utilized to their full extent. As a result, international passengers are often required to produce their passport for examination up to five times at the airport before boarding. This is not only time consuming, but also inefficient because every process, whether it be check-in, security, immigration or boarding, treats the passenger as an unknown entity.



When considering the ePassport and its functional capabilities, chip validation and biometric verification at the outset of the passenger experience can be used to continually identify the passenger at each consecutive airport touchpoint through a biometric comparison. This is clearly faster, and ultimately more secure than passport re-examination. Of course this necessitates authenticating the ePassport and matching the passenger with the presented identity credential through biometric verification. This is being explored by the Aruba Happy Flow project, which is being run by KLM, the Aruba Airport Authority, the Schiphol Group, the Government of Aruba and is supported by the IATA Passenger Experience Management Group (PEMG).

IATA has emphasized that obtaining the required technology to integrate chip validation using the ICAO Public Key Directory (PKD) to support the reading and validation of ePassport chips during check-in might be a significant, but is also a worthwhile investment in both security and facilitation for the traveller. In building a business case to pursue this objective, the global aviation community would need to recognize that all parties in the stakeholder chain – Governments, airlines and airports – will share the benefits.

#### **PASSENGER DATA**

Despite the rapidly growing number of electronic passports and the increasing demand from Governments for passenger data transmitted by airlines, IATA continues to question the need

for redundant paper processes to collect the same information that a passport can provide. We wonder why information beyond the ICAO standard is still required by some authorities. Why are electronic travel authorizations only offered by 8% of States and why, with all the information provided by airlines in advance, do we still have long immigration queues.

Acknowledging the earlier work of the IATA/Control Authorities Working Group (IATA/CAWG), IATA lobbied for the introduction of Recommended Practices for Electronic Travel Systems (ETS) at the 9<sup>th</sup> ICAO Facilitation Panel. This came in response to increased border security measures, including requirements that passengers apply for travel authorizations or otherwise register online prior to boarding a flight for travel. In many cases States were using mixed terminology such as “electronic visa”, “electronic travel authority”, or “visa on arrival” to describe their online programmes. Given the wide disparities in language and use, there was a need to standardize this terminology and to place this function in the appropriate regulatory framework within ICAO.

IATA successfully argued that ETS travel authorizations, when required by a State, need to be implemented with a fully automated validation system embedded in interactive Advance Passenger Information (iAPI) exchanges. When systems are constructed in this way, travel authorizations can be validated in real-time by automated means integrated into the airline check-in process.

“the ePassport is overwhelmingly treated as a traditional passport, which means that the main security and facilitation benefits of the passport chip...are not being utilized to their full extent. As a result, international passengers are often required to produce their passport for examination up to five times at the airport before boarding”

#### FUTURE PERSPECTIVES

With the increasing prevalence of ePassports, it is inevitable that key air travel stakeholders will require more from the document. Currently, there are a number of scenarios that are conceivable:

- It is possible that States may require airlines to capture biographic API data from Data Group 1 of the ePassport chip as opposed to the Machine Readable Zone (MRZ). This would presuppose that PKI validation has, or will be integrated into the check-in procedure.
- Following the Aruba Happy Flow example, in which PKI validation is a pre-requisite when establishing identity, automated self-boarding would be supported by biometric verification, matching the physical traveler with the authenticated identity. This has the advantage of corroborating with the highest of assurances that the identity of the passenger matches the transmitted passport data.

- Clearly biometric matching at boarding enhances API data quality, but this begs the question: what facilitation impact would this process enhancement have at the arrival airport, and at what cost to the industry?
- If the biometric boarding check were a shared Airline/ Government function it would further improve API data quality and, critically, offer an opportunity to enhance data sharing and trust between Sending and Receiving States.
- A key way to improve trust between Governments relating to each other’s traveling nationals would be through the establishment of multilateral Registered Traveller Programmes (RTP). Essentially this would create a multi-national trust platform in which Governments continuously vet and share data of citizens who have agreed to register.
- Increased ePassport chip validation in the airport environment would also require greater use of the ICAO PKD by the aviation industry when they begin to download public keys and associated certificates needed to validate digital signatures.
- Large-scale implementation of ABC gates are also a strong argument for making greater use of Logical Data Structure (LDS) 2.0 technology, namely allowing for data to be added to the chip after the document has been issued in three specific Data Groups:
  - *Travel Records* – Travel stamps could be entered electronically onto the ePassport’s chip, including when they are processed at ABC gates. The benefit of adding this travel data in digital format includes greater consistency; enhanced security; ease of access and viewing.
  - *Digital Visas* – Storing a consular-issued visa on the chip of an ePassport would allow for that national to be processed through ABC gates, despite the visa requirement.
  - *Additional Biometrics* – The ability to add secondary biometrics (iris and fingerprint) significantly enhances the LDS2 value proposition. It provides States with more



choices in national policy regarding secondary biometric storage, allowing for “as-needed” storage of secondary biometrics. States may tailor their exit/entry controls to allow travellers with documents storing secondary biometrics to use ABCs or other facilitative technologies and/or processes. In addition to providing alternatives to States, the capability of adding biometrics post-issuance provides more choice for document holders, who may opt to RTPs or other facilitation schemes after their documents have been issued.

### IATA AND ICAO

A number of groups within IATA and ICAO, are studying how to improve the current situation. The ICAO Technical Advisory Group on the Traveller Identification Programme's (TAG/TRIP) New Technologies Working Group (NTWG), is addressing this issue with a work item on enhancing use of the ePassport. Importantly, the NTWG is holding its triennial *Request for Information* (RFI) process ([www.icao.int/security/FAL/TRIP/pages/rfi.aspx](http://www.icao.int/security/FAL/TRIP/pages/rfi.aspx)), through which Governments receive insight into emerging technologies that may warrant examination. The current RFI will conclude in early 2017 and is studying, amongst other technologies, the following categories: Mobile/Virtual ID, smartphone and online application processes, LDS2 and mobile technology, creative ways to send certificates to the PKD, and image manipulation detection systems.

The IATA PEMG is working to revisit the E2E passenger journey, including the promotion and development of self-service options that rely on mobile technology and the capture of both biographic and biometric data. To support these efforts, the PEMG has four sub-groups working on: 1) Biometrics; 2) Common Use; 3) Fast Travel; and 4) Passenger Facilitation.

The IATA/CAWG is an expert informal forum of airlines and Government officials that work collaboratively to develop

and/or recommend solutions, and establish best practices for border management, that contribute to the facilitation of legitimate travellers whilst ensuring border security is maintained. The IATA/CAWG is currently focused on API data quality and Registered Traveller Programmes (RTP). The IATA/CAWG has consistently developed best practice and guidance material for existing Standards and Recommended Practices (SARPs) and developed proposals for new SARPs in ICAO's Annex 9.

Also, within IATA, the developing *One Identity* initiative is exploring the concept of a single travel token, most likely based on biometrics, which can be used both for industry processes and government requirements.

### CONCLUSION

Clearly, identity verification and the use of ePassports as the globally interoperable medium for presenting and validating one's identity, is central to all of the facilitation tools available, especially in regards to facilitating international travel. The ePassport is the source for Government issued, standardized, secured and verifiable data that, if properly utilized, can allow passengers to be processed using more automated tools, creating efficiencies across the entire travel continuum. However, if the ePassport is not utilized more robustly – it could very well be overtaken by other mediums and technologies in the future.

As a result of UN Security Council Resolution 2178, it is likely that there will be an increased exchange of passenger data between airlines and Governments that will significantly shape the facilitation framework of the future. IATA supports a growing trend towards interactive API exchanges combined with ETS travel validation, augmented by other facilitation tools such as ABC and RTP. This more fully integrated border management concept could be further complemented through implementation of Passenger Name Record (PNR) data exchanges if and when the global impasse over data privacy is settled in an equitable fashion. ■

## Passports, visa stickers, eID cards

### PRODUCTION AND PERSONALISATION



# INTERNATIONAL STANDARDS FOR CIVIL REGISTRATION AND VITAL STATISTICS



## SRDJAN MRKIĆ

He is the Chief of Demographic Statistics in the United Nations Statistics Division at the UN Headquarters. In this capacity, he leads the technical work on the programmes for developing international statistical standards for population and housing censuses, civil registration and vital statistics, and, previously in the field of social statistics. A lawyer and statistician, Mrkić has multi-decade experience managing statistical programmes at the national and international levels, all in the field of demographic and social statistics.

✈ In the many ongoing discussions regarding the integrity of individual identity documents, a considerable and quite understandable emphasis is placed on the security features that link biometrics with identity. International standards for establishing identity are seldom part of this discourse. Though these standards, which established the procedures for issuing birth and death certificates and registering these events within the civil registration system were inaugurated in the 1950's, they remain in place and are regularly updated today.

## WHAT ARE THE STANDARDS?

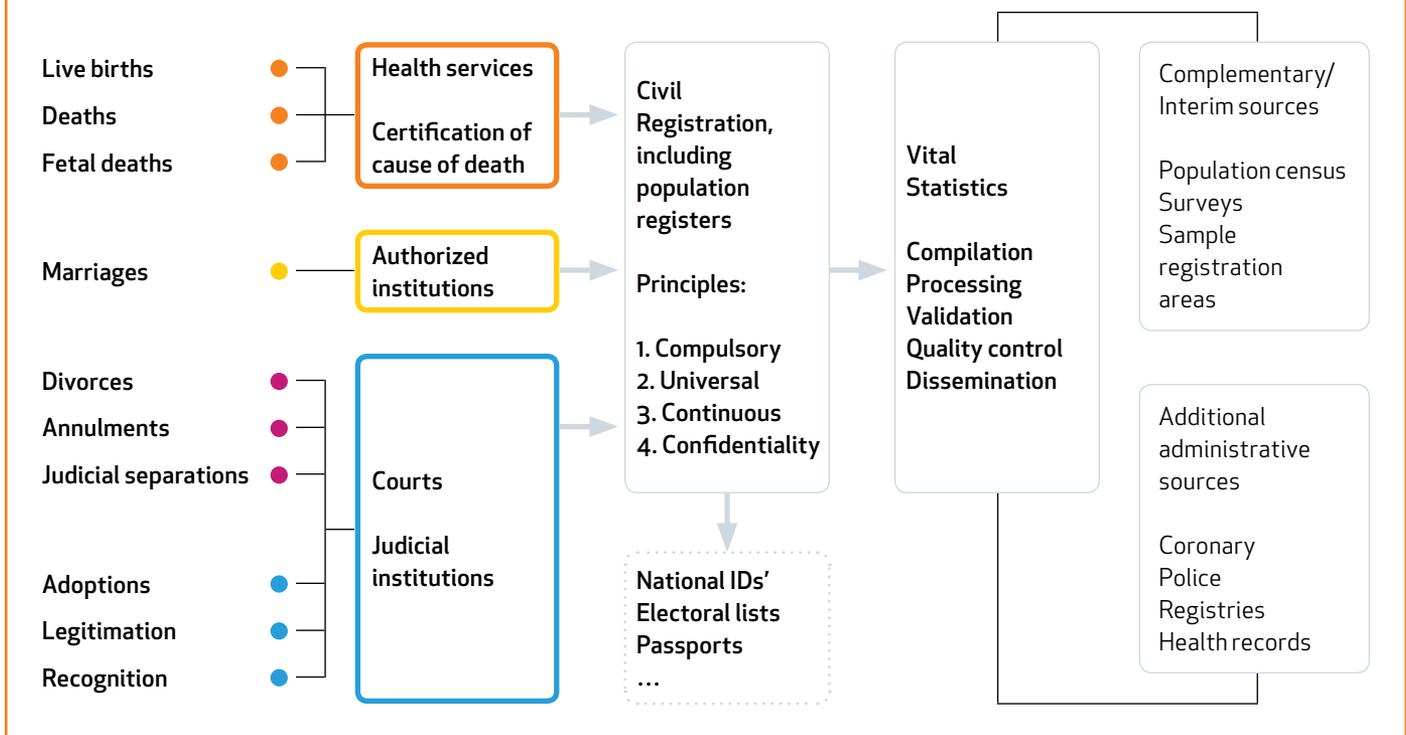
The 2014 version of the United Nations *Principles and Recommendations for a Vital Statistics System, Revision 3*, which was first issued in 2014 by the UN in 1953, elaborates in detail the process of: registering vital events; issuing legal tenders to certify the occurrence of these events; and translating these administrative data in regular and reliable vital statistics.

As is the case with all international standards, the methodologies were developed to ensure their implementation in every State around the world. Based on best practices and tested by a combination of different mechanisms – expert group meetings, professional and scientific gatherings – the primary purpose of implementing international standards at the national level is to increase the capacity of each State to deliver on their responsibilities in the most efficient and wholesome manner.

For civil registration and vital statistics, the set of international standards focuses on developing and maintaining a system that ensures that all vital events (births, deaths, foetal deaths, marriage, divorces – to name a few) are properly registered, and that the official certificates issued and characteristics of events and persons involved, are collected and translated into regular, accurate and reliable vital statistics. The components, flows and the relationships of such a system are displayed in **Figure 1**.

In using births as an example, every birth in a State needs to be reported by informants designated by the law and recorded in the civil registration records. A birth certificate is issued to establish the legal identity of the newborn and all relevant information on the event (including the names of the newborn, mother and father) is collected and transmitted to statistical authorities for collation, processing and dissemination. While the system components in a particular State can include additional institutions – and in many States the registration component includes population registers and identity management agencies – the essential standard of registering each vital event, certifying its occurrence with legal tender (certificate), collecting pertinent information and translating it into vital statistics, needs to be implemented and maintained.

Figure 1. Civil registration and vital statistics system



### WHY DO THESE STANDARDS MATTER?

Civil registration, the process of attesting the incidence of a vital event and legally certifying its occurrence, has an unparalleled impact on the exercise of basic human rights endorsed and promulgated by the United Nations. *The Convention on the Rights of the Child*, to which all 193 members of the United Nations are party to (albeit United States has yet to ratify it), in its Article 7, reads:

*"1. The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.*

*2. States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under the relevant international instruments in this field, in particular where the child would otherwise be stateless."*

A State without a fully functioning civil registration system is, therefore, in breach of the Convention, depriving the newborn of the basic human right to identity, to being registered and to have a name. Far from being the only human right, the exercise of which is directly linked to the existence and functioning of civil registration, this right of the child to be registered and to have a name, is just one on the long list.

In September 2015, the Heads of States gathered for the United Nations Sustainable Development Summit where the 2030 Sustainable Development Agenda, its seventeen goals and one hundred sixty nine targets, were launched. Each of these targets is accompanied by one or more indicators that will be used to monitor the achievement of the Sustainable Development Goals. Indicator 17.19.2 reads:

*"Proportion of countries that (a) have conducted at least one population and housing census in the last 10 years; and (b) have achieved 100 per cent birth registration and 80 per cent death registration."*

In a clear and straightforward manner, this message related to the need for establishing a fully functioning civil registration based on international standards. There is a lower standard for the registration of deaths in many States where cultural traditions, religious customs and weather conditions, among other factors, prevent an effective registration of deaths, particularly when there are no considerations regarding inheritance, pension remuneration and so forth.

### WHY ARE VITAL STATISTICS PART OF THE PACKAGE?

Vital statistics refer to the collection of information on vital events that occur in a State in a well-specified period of time. It provides regular and reliable statistics on the number of births,

the newborn, the characteristics of the mother and father, on deaths and the characteristics of deceased and the causes of deaths, on marriages and divorces. These detailed statistics are critical in terms of quantifying demographic phenomena that influence the most valuable asset of any State – its human capital. Vital statistics provide answers to many questions, such as: how many are we? What is the average age of the mother at birth? How many births can we expect next year? What causes the most deaths in a State? What is the impact of marriage on a nation's fertility? How many marriages and divorces were there in previous years?

The most accurate source of vital statistics is civil registration, since only through civil registration can the many data items needed for the production of comprehensive vital statistics be collected. Parts of the international standards refer to the need for collecting these data items.

As an example, the current set of international standards for civil registration and vital statistics lists the following characteristics of the event and the participants in the case of live birth: date and place of occurrence, date and place of registration, type of birth (single, twin ...), attendant at birth; sex and weight of the newborn; date of birth and marital status of mother, her educational attainment, place of usual residence and duration of residence, her place/State of birth, number of children previously born alive, number of stillbirths – if any, date of last previous live birth, date of marriage; as for the father, data items refer to the date of birth, marital status, educational attainment and place of usual residence. In sum, a total of twenty-two data items are considered the necessary minimum to produce internationally recommended vital statistics.

Who is responsible for collating these data items? The civil registrar is the critical link. In the process of registering a live

birth and issuing the birth certificate, they need to collect the requested information from the health institution and the parents to channel it to statistical authorities for generating vital statistics.

### RELATIONSHIP TO IDENTITY MANAGEMENT

The contemporary explosion in activities related to identity management is easily documented; almost everywhere there are new agencies mandated with issuing biometric identity documents to everyone in the State. Technology allows for efficiently conducting enumeration drives and maintaining databases; fingerprints and photographs, not to mention personal identification numbers, can be easily processed and maintained in contemporary storage devices.

It is critical to incorporate international standards for civil registration and vital statistics in the development phases of identity assignment and management at the national level. Though the civil registration agency can be absorbed by the new structure, the civil registration function – registering vital events and issuing legal tenders of their occurrence, from birth to death certificate and all changes in the civil status of a person in between – needs to remain firmly entrenched in the foundations and functioning of population identity management agencies. The same goes for vital statistics; international standards for collecting information and for producing comprehensive small area statistics on vital events have to be implemented to the letter and appropriate mechanisms developed and put in place.

Finally, international standards elaborate in detail the importance of protecting the privacy and confidentiality of individuals' information. These guidelines can be well put to use in the installation of protocols and procedures regarding identity management at a national level. ■

## Check eIDs in the blink of an eye.

Not everyone crossing your border are who they pretend to be. That's why secunet developed the eID PKI Suite: It checks the integrity of eID documents and the traveller's identities in the blink of an eye. Choose between individual software modules for easy integration into your existing setup, and the complete turn-key solution. Just as you need it.

**IT security made in Germany.**

[www.secunet.com/en/eidpki](http://www.secunet.com/en/eidpki)



**secunet**

IT-Sicherheitspartner der Bundesrepublik Deutschland

**HID**

# LOCAL NATIONAL GLOBAL SOLUTIONS FOR A SECURE SOCIETY.

Government agencies around the world place absolute trust in HID Global to protect their data, facilities and citizen populations. From secure print and access management solutions to advanced credentials, biometrics, and innovations in mobility, HID provides the most flexible, secure, custom solutions on the planet.

You'll call it protection at every level. We call it, "*your security connected.*"

**YOUR SECURITY. CONNECTED** | Visit us at [hidglobal.com/solutions/government-mobile-id](https://hidglobal.com/solutions/government-mobile-id)

© 2016 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, and the Chisel Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

# THE OECS SINGLE DOMESTIC SPACE FOR TRAVEL: UNDERPINNING THE OECS ECONOMIC UNION



## DR. LORRAINE NICHOLAS

She is an OECS Commission Tourism Specialist with extensive research and technical experience in the tourism field. Facilitation of ease of intra-travel is arguably the most critical aspect of the Tourism work programme of the OECS Commission and one of her most recent achievements was the development of an Air Service Agreement that seeks to liberalize air transportation in the Eastern Caribbean region. She also developed an Action Plan for Ease of Travel within the region in 2013 that grants full clearance for visitors to the region at the first port of entry, without the need for subsequent checks during the same trip. Dr. Nicholas represents the OECS on the Caribbean Tourism Organization's Aviation Task Force which addresses air transportation issues for the wider Caribbean region.

 This article provides a synopsis of the progress made in the operationalization of the Organisation of Eastern Caribbean States (OECS) Single Domestic Space. An account of the origins of the concept of the OECS Single Domestic Space is delineated, followed by a discussion on the principles of the Single Domestic Space. The outcome of discussions held with key stakeholders on the activities required to operationalize the Single Domestic Space is also outlined, followed by a note on the way forward.

## BACKGROUND

The Organisation of Eastern Caribbean States (OECS) was established 18 June 1981. Ten countries in the Eastern Caribbean constitute the OECS, namely: Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St. Kitts and Nevis, Saint Lucia and St. Vincent and the Grenadines; with Anguilla, the British Virgin Islands and Martinique as Associate Members.

The Revised Treaty of Basseterre was ratified in January 2011 and established the OECS Economic Union as a single economic and financial space where goods, people and capital move freely among Member States who are parties to the Economic Union. The Revised Treaty also mandates participating countries to harmonize monetary and fiscal policies and to adopt a common approach to trade, health, education and environment, as well as to develop key sectors of the economy such as agriculture, tourism, and transportation.

These Treaty obligations constitute the platform for the establishment of a single domestic space that allows for the free and seamless movement of people and goods in the OECS Economic Union Area (EUA).

At the 52<sup>nd</sup> Meeting of the Authority held in Grenada on 24 January 2011, OECS Heads of Government agreed, among other things, that a valid state-issued photo identification card containing the bearer's nationality can be used as a travel document for all OECS citizens who could be granted an indefinite stay in Member States.

The Heads of Government also agreed that OECS citizens would not require a temporary driver's permit to drive in participating Member States. These arrangements are now in effect in all Member States participating in the Economic Union.

It is envisaged that the OECS will go further in this regard by undertaking initiatives that will lead to the creation of a single domestic space for travel that would involve the removal of immigration and customs checks and the removal of the requirement of embarkation/disembarkation (E/D) cards for OECS citizens travelling in the Economic Union Area.

Given the significance of tourism as the lead sector in the OECS, the OECS Single Domestic Space will also allow for the full clearance of third country nationals (visitors to the OECS) at their first port of entry into the Economic Union Area so that these persons can then move freely throughout the Economic Union Area after having satisfied immigration and customs requirements at their initial port of entry.

The concept of a Single Domestic Space for travel within the Caribbean region is not entirely new. During Cricket World Cup in 2007, a temporary Single Domestic Space was successfully created, comprising ten Caribbean islands (six of which were OECS territories) for this event.

Travellers were only required to submit completed entry and departure forms at the first port of entry. Onward travel throughout the Single Domestic Space did not require subsequent customs and immigration clearance. Once passengers arrived at the Immigration Department Desk at the first port of entry, they were provided with a blue CARICOM wristband that identified them as being entitled to free movement throughout the Single Domestic Space.

### PRINCIPLES OF THE OECS SINGLE DOMESTIC SPACE

The basic principles of the Single Domestic Space are:

1. Movement of people:
  - travellers arriving from within the EUA are to be treated as if they have been cleared for entry and have satisfied all requirements for entry;
  - travellers arriving from outside the space should satisfy all entry requirements at the first point of entry into the EUA; and
  - travellers departing the EUA should satisfy all requirements for exit at the last port of departure.
2. Movement of goods:
  - common treatment of passenger and crew baggage, particularly in relation to duty free allowances on goods purchased within the domestic space, quantities of excisable goods and household and personal effects.

### STAKEHOLDER CONSULTATION

The OECS Commission held a Symposium on Single Domestic Space comprised of top officials of the OECS from 30 May



to 2 June 2016, in Antigua and Barbuda to develop a framework to establish a Single Domestic Space in the OECS.

The Symposium brought together Commissioners of Police, Chief Immigration Officers, Comptrollers of Customs, Air and Sea Port Managers and other high-ranking officials to share ideas and chart the way forward for the operationalization of the Single Domestic Space.

All Member States of the OECS were represented at the meeting. Also in attendance were representatives from organizations including:

1. The International Organization for Migration (IOM)
2. Eastern Caribbean Civil Aviation Authority (ECCAA)
3. Regional Security System (RSS)
4. The Caribbean Community's (CARICOM) Implementation Agency for Crime and Security (IMPACS), Joint Regional Communications Center (JRCC)
5. CARICOM Office for Trade Negotiation (OTN)
6. Caribbean Bank Note (CBN)
7. Rockwell Collins – Global Networks
8. Caribbean Development Bank (CDB)
9. The World Bank (WB)

The key objectives of the symposium were to:

1. facilitate the exchange of ideas and information on facilities, systems and experiences relevant to the establishment of the OECS Single Domestic Space;
2. benchmark and make proposals for adoption of best practices for the development and application of an integrated framework for the operationalization of a Single Domestic Space within the context of the OECS Economic Union; and
3. develop a comprehensive strategy on the development of a Single Domestic Space with recommendations for practical application for the OECS EUA.

The main issues discussed were:

1. systems required for harmonized border management, including the management structure for border agencies, and security procedures and systems;
2. procedures and systems for full clearance of immigration and customs at the initial port of entry into the EUA, including the separation of domestic and international travellers at ports of entry;
3. mechanism for information sharing, intelligence gathering and sharing among border agencies within Member States and among Member States;
4. requirements and implications for application of a common visa regime;
5. mechanism for distinguishing between movement of personal effects and the movement of commercial goods within the EUA; and
6. procedures for treatment of goods including passenger baggage, excisable goods and personal and household effects owned by individuals relocating to another Member State.

### PROPOSED SOLUTIONS

A key element of the Symposium was the formation of four working groups, comprised of representatives from each of the border management agencies (customs, immigration, security and port authority) to enable in-depth discussion by each agency on the main issues and possible solutions to create the SDS.

The session also allowed members of the agencies to get to know counterparts from other Member States to facilitate better collaboration within Member State agencies following the symposium. Groups were asked to identify the essential issues, challenges and opportunities associated with facilitating the creation of the Single Domestic Space.

The following solutions emerged from the respective groups:

#### Customs

1. harmonization of customs legislation;
2. common procedures for clearance of import and export goods;
3. harmonization of all taxes, fees and charges;
4. the implementation of the Customs Union should lead to the overall objective of economic development and not disadvantage any participating members of EUA;
5. standardization of duty free allowances across the islands;
6. uniform list of prohibited and restricted goods;
7. standard customs clearance system;
8. share information, best practices and build regional competences;
9. implement a national and regional risk management unit; and
10. develop a common customs passenger declaration form.

#### Immigration

1. harmonization of guidelines for regional border issues;
2. reactivation of synergistic working groups;

3. inventory of current systems and processes;
4. enhancement of mechanism for border management which should comprise/facilitate:
  - watch-listing: regional and national and connectivity/interactivity with INTERPOL and other international agencies for intelligence gathering;
  - inter-agency cooperation: regionally and nationally;
  - interoperability of border management systems; and
  - interaction with international border management agencies.
5. enactment of revised model Advanced Passenger Information System (APIS) legislation and consider the use of Passenger Name Recognition (PNR) systems;
6. continuous training in standard operation procedures;
7. alignment of processes with information technology;
8. expand and upgrade information communication technology systems in Member States;
9. abolish the use of E/D cards in the EUA; and
10. move to implement e-Passports across Member States which, among other things, will capture biometric data.

#### Port Authority

##### Airports

1. reconfigure infrastructure at airports to separate domestic from international travellers;
2. implement an APIS to facilitate faster processing of passengers, identify risks and track passengers;
3. airlines collect E/D cards for passengers departing the EUA thereby eliminating the need for emigration checks upon departure;
4. upgrade current IT systems for the purpose of processing passenger information and tracking persons coming into the space;
5. procure luggage screening equipment; and
6. implement ECCA approved systems to facilitate one-stop security screening which eliminates multiple screening of in-transit passengers.

##### Seaports

1. improve and upgrade infrastructure;
2. procure scanners for faster processing of passenger baggage;
3. enhance security by utilizing K-9s for screening passenger baggage, eliminating the need for manual checks and speeding up processing time;
4. harmonize legislation for levying of fees and charges;
5. design new ports to accommodate inter-island as opposed to intra-island travel;
6. improve security systems at the port – install closed-circuit television (CCTV), port security officers and container scanners; and
7. upgrade systems for processing in-transit cargo.

#### Security

1. develop Human Resource policy and strategy to strengthen institutions;

2. create or enhance mechanisms for data management and intelligence gathering; and
3. source and allocate adequate resources to build capacity in the following areas:
  - Infrastructure
  - Human Resources
  - Equipment
  - Supplies.

A synthesis of the discussions reveals that the underlying changes required to operationalize the OECS Single Domestic Space for travel include: legislation harmonization; information sharing; harmonized systems that are interoperable; and common operating procedures. In addition to these proposed solutions, some general recommendations were made including the establishment of a combined border management agency that does not create distinctions between the roles of immigration, customs and security.

#### THE WAY FORWARD

Clearly, the pursuit of the creation of a Single Domestic Space involving multiple islands is a complex undertaking which involves many players, necessitates critical changes and requires significant resources. As the OECS moves ahead to establish this Domestic Space, the following activities are currently being pursued by all OECS Member States:

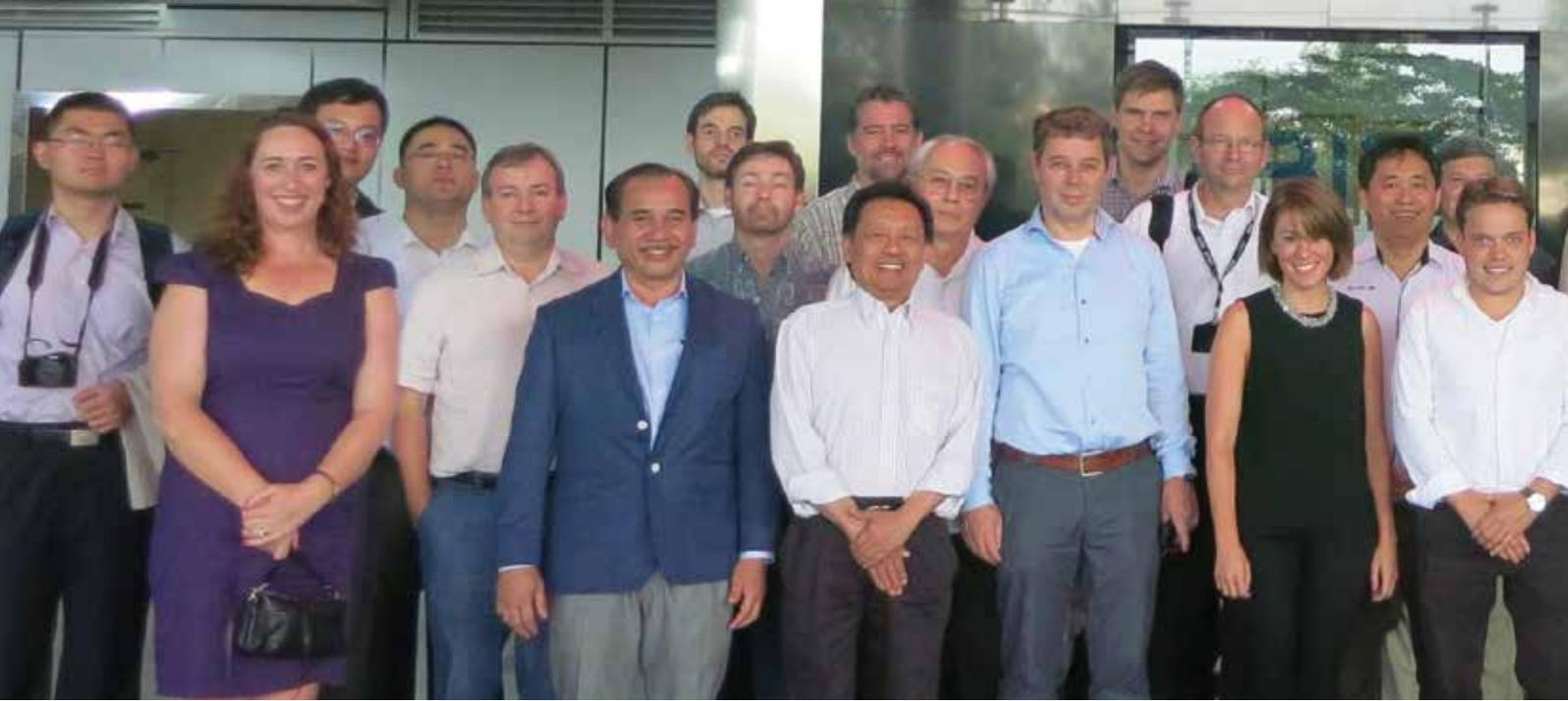
1. document all concerns and challenges, develop actions to mitigate them and circulate the findings to all OECS States;
2. undertake a comprehensive review of all current border management systems and how these systems can be used more effectively by agencies;

3. convene a separate meeting with border management personnel to agree on information-sharing modalities and mechanisms involving:
  - completion of requirements for the facilitation of the one-stop security initiative;
  - harmonization of ED cards among OECS States;
  - agreement concerning the treatment of passengers arriving on domestic flights (that are originating and proceeding directly into another OECS State); and
  - authorization to the OECS Commission to engage in discussion and possibly, negotiation with the providers of border management systems in most States to provide an IT solution ensuring information-sharing and connectivity between current border management systems.
4. monthly newsletter updates to all interested parties and stakeholders to be posted on the OECS website and possibly an OECS blog to highlight progress and key issues;
5. country-by-country training program for all border agency officers, on standard operating procedures in compliance with the principles of the Revised Treaty of Basseterre and the operationalization of the Free Movement of People, and the creation of a step-by-step guide book for all border agents on the process and treatment of OECS citizens – The Free Movement of People Guide; and
6. development of a comprehensive strategy to facilitate the Single Domestic Space for sign off by OECS Heads of Government and agreement on the policy areas requiring decisions/approvals for submission to the Council of Ministers and/or the OECS Heads of Government for their ratification.

Once this is completed, the process of operationalizing the OECS Single Domestic Space will commence. ■



# Document Verification Solutions



New Technologies Working Group (NTWG)

# ICAO NEW TECHNOLOGIES WORKING GROUP 2016/2017 REQUEST FOR INFORMATION OPPORTUNITIES FOR TECHNOLOGIES AND SYSTEMS AVAILABLE



## LOUISE COLE

She is the Manager, Passport Operations for Identity & Passport Services for the Department of Internal Affairs in New Zealand. Louise has worked for Internal Affairs since 2006, and has been the New Zealand representative on NTWG since 2014.

## ✈ INTRODUCTION

THE ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP) and its New Technologies Working Group (NTWG) is holding a **Request for Information (RFI)** on new and improving technologies relevant for use with machine readable passports, visas and card-based travel documents. The RFI is opened to all parties interested in providing information on future capabilities.

The RFI is issued every three years to inform and update current knowledge on the specifications, development and implementation of new tools, systems and technologies.

## BACKGROUND

The New Technologies Working Group (NTWG), which supports the TAG/TRIP, is responsible for research, analysis and reporting on new technologies available today, or in the near future, to use in machine readable travel documents (MRTD), including the development of MRTD specifications contained in the Seventh Edition of ICAO Document 9303 – Machine Readable Travel Documents. The NTWG also has a broad interest in technologies that can be applied in traveler identification to effectively facilitate passengers and uniquely identify individuals.



# RFI

## Request for Information

### AREAS OF INTEREST

Submissions are welcome in areas that include applicant eligibility assessments, document security and production, linking documents to holders/bearers, providing reliable authentication of genuine documents and the secure and reliable transit of travelers through airports, seaports and other international border control points.

The 2016/2017 RFI is seeking submissions in the following specific areas of interest:

#### ■ Mobile / Virtual Identity

Smartphone-based and virtual identity systems with capability to establish, present, verify and validate identification through the use and exchange of non-privacy data, as an example, without disclosing any personally

identifiable information during the process of establishing, presenting, verifying and validating identities.

#### ■ Image Manipulation Detection Systems

Image manipulation detection systems that can detect when an image (photograph, fingerprint or iris, for example), either digital or hard copy, original or digitized, has been altered, amended or tampered with, in order to prevent attacks such as morphing or beautification.

#### ■ Liveness Factor / Detection

Liveness detection systems with the ability to integrate into online and mobile passport application systems, and which are able to determine that the subject is the actual live person submitting the photograph or biometric image, and not a model or photograph.

#### ■ **Smartphone and Online Application Processes (excluding security tolls and photos)**

Technologies and strategies to help prevent service denial attacks and blunt force attacks to overcome fraud controls built into online systems. Measures to provide assurance on the integrity and genuineness of individual applications.

#### ■ **Creative Ways to Send Certificates to the Public Key Directory (PKD)**

Creative ways to send, upload/download ePassport certifying credentials to the PKD.

#### ■ **Photo Quality Assessment Systems**

Assessment systems that can be utilized to judge whether a facial photo, submitted by travel document applicants, for online and hard copy, is compliant with the photo specifications provided in Doc 9303 and the appropriate ISO standard 19794-5.

#### ■ **Physical Security Features**

Physical security features that protect travel documents from counterfeiting, photo-substitution, alteration of text of the data page, and replacement of inlays. Features that make it easy to recognize visually and/or be authenticated at automatic border control by automated inspection systems are welcomed.

#### ■ **Machine Readable Security Features / Authentication**

Systems and/or software that can optically and electronically read travel documents and be used to confirm their integrity and authenticity at passport application with kiosk systems or automatic border control. Information on design rules and examples for documents suited for machine authentication. Reader systems and authentication software and reference databases.

#### ■ **Leveraging ePassports**

Use of the passport beyond purely as a travel document. Uses such as an identification document, whose validity can be verified through the use of the PKI process.

#### ■ **Storage Media and Contactless Chips**

New technology or improvements relating to storage media and contactless chips.

#### ■ **Logical Data Structure 2 (LDS2) and Mobile Technology**

Applications relating to the storage and secure operation of LDS2 using mobile phone technology. Applications that allow mobile phones to securely communicate with integrated circuit chip inspection systems, send and receive information stored in LDS2 to inspection systems and/or display data stored in LDS2 using a phone as a medium.

#### ■ **Multimodal Biometrics**

Latest developments in biometric capture systems, specifically cost effective systems that enable the capture of high quality facial and iris biometrics in a single pass.

#### ■ **Facial Recognition Algorithms**

Algorithms that can be used to verify facial images at travel document application or border control points.

#### ■ **Remote verification of ePassports**

Already NFC enabled smartphones are being used to read data on passport chips. This has potential to enable remote verification of passports. This could be strengthened by enabling such devices to also undertake PKI authentication of passport chips.

#### ■ **Biographic Search**

Information on the latest developments in database lookup algorithms that support the pre-issuance stage of MRTDs. Related techniques may involve name-matching, address equivalence and other test fields and descriptors including distance between biographic text.

### SUBMISSIONS

An international selection panel will review submissions against a variety of qualitative and quantitative factors.

These factors will generally include cost, innovation and compatibility with current and future document issuance and border control processes. Dependent technologies, reliability, accuracy and speed will also be considered by the selection panel.

Following the evaluation process successful vendors will be invited to make oral presentations to Government representative members of the NTWG, and representatives of ICAO Contracting States. The presentations are planned to take place from 18 to 21 April 2017 in Amsterdam, the Netherlands.

The information gathered during the RFI process is then summarized and shared amongst ICAO Member States and may also be considered when international travel document standards are developed.

Responses to the Request for Information will close on 15 November 2016.

For further information and instructions on how to make a submission can be downloaded at

**[www.icao.int](http://www.icao.int)** ■

# CLOSING THE SECURITY GAP

## EXTENS® SmartStamp: the machine readable travel stamp

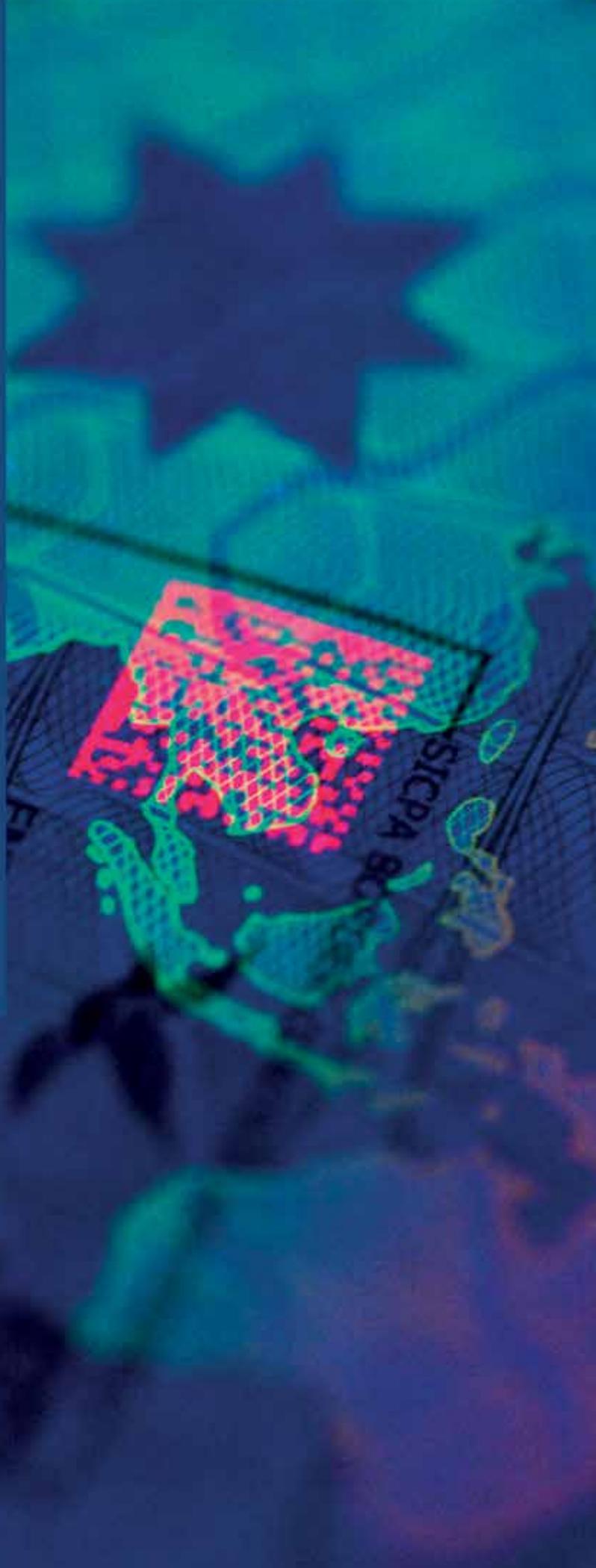
Governments and immigration agencies are increasingly concerned about who enters and exits their borders, but the tools to do so today are limited. To close this security gap, SICPA developed a solution that connects the tangible to the virtual.

EXTENS® SmartStamp is a unique, secure and customisable entry/exit stamp that can contain traceable data - both static and dynamic - about travellers and their trips.

Come visit us at our booth #1 to find out more about our new border control solution, at the upcoming ICAO TRIP 2016, in Montreal, Canada.



Enabling trust



# THE ORIGIN OF *ORIGINS*



## CHARLES DE COUËSSIN

*After starting his career at the Paris Louvre Museum as a curator in charge of scientific analysis of art objects, he became an expert on paintings before moving to the oil and then aviation industries. In 1998 he became Development Director at SITA, a main provider of aviation communication and IT infrastructures. He pioneered the first EC funded programme based on biometrics and smart cards after 9/11, together with IATA and industry stakeholders. Since then, he founded ID Partners, a consulting practice based in Paris that is involved in various aviation security and border management initiatives on funded by the European Commission. Charles has been an advisor to the French government for both identity and passenger data (PNR) programmes.*

✈ The underlying idea of the European Commission funded ORIGINS Project is to improve border controls by investigating how breeder documents are delivered and how they are used for the issuance of passports. It represents a consortium of market-leading industrial companies, relevant subject matter experts (SMEs), renowned public research institutes and universities, passport and breeder document manufacturers, end-users represented by public administrations, and legal, ethical and sociological issues experts. Partners come from various Member States, external border countries (Estonia, Latvia, Poland), and associated countries (Norway, Turkey).

## RATIONALE

Breeder documents (notably birth certificates) are the basic designation of an individual's relationship to their community (where that individual was born and lives). Since the introduction of electronic passports (e-passports) and the use of security features in their chips (such as biometrics), the security of these documents has greatly improved. However, they are based on breeder documents (such as birth certificates) that do not offer the same level of security and are much easier to counterfeit.

In most European countries, and in the rest of the world, breeder documents are unsecure documents, yet they are the basis of identity verification. Therefore, the weakest link of the identity (ID) chain and travel documents issuance, and in particular of ePassport issuance, continues to reside in the entitlement process, in which **the evidence of an applicant's identity** is evaluated.

Such evidence is often supported solely by breeder documents, which remain mainly paper-based without any form of security in their manufacturing or issuance processes. Most of these breeder documents are much easier to forge than ePassports, and by using forged breeder documents (via identity theft or fake ID), people can obtain genuine travel documents. To make matters worse, there is, as yet, no standard format or standard issuance process for breeder documents throughout Europe or within many Member States.

A FRONTEX study on the Operational and Technical Security of ePassports confirmed that this "breeder documents" issue was crucial to the legitimacy of documents, which could be issued based on unreliable ones. It is therefore of the utmost importance to ensure the reliability of the ePassport issuance process to offer efficient European Union (EU)/Schengen border control. The process must be founded on reliable breeder documents.

ePassports are not the sole cause for concern related to breeder documents: stolen, counterfeit or altered birth certificates are often used to create new identities, paving the way to a variety of frauds, smuggling of migrants, drugs or weapons, trafficking in persons, terrorist mobility, etc.

Approaches to counteracting the weaknesses of breeder documents have been implemented in some States. Centralized databases are often used to record the credentials of individuals in order to avoid using breeder documents during the issuance procedure. However, these solutions remain an insufficient answer to making breeder documents secure and trustworthy. In consequence, both ID cards and ePassports can be considered to be unreliable.



Breeder documents must be issued based on reliable data and processed securely from a system standpoint. A complete, secure chain which can be securely accessed by issuance officers is required starting from birth registers and encompassing life events (such as marriage, divorce, etc.) until death. This lack of standardization and harmonization of data records becomes a crucial issue, especially when citizens relocate to other countries and undergo family or social events. This situation will only increase as student exchanges, business mobility and relocation opportunities become more frequent.

The lack of interoperability and secure access to national registries, together with the provision of unregulated breeder documents issued by other States, might further increase vulnerability and suspicion. The existence of a standard for breeder documents would simplify the verification process and the secure issuance of a passport anywhere when needed. The procedure and entitlement criteria for passport issuance is regulated at the national level as it is intimately linked to sensitive issues like national sovereignty and national citizenship.

Although the weaknesses of breeder document security have been well known for many years, there is not yet wide acceptance of a suitable solution at European levels to overcome the issue. However, in December 2010 the EU Council recommended that Member States consider mechanisms on “preventing and combating identity-related crimes and on identity management, including the establishment and development of permanent structured cooperation between the Member States of the European Union” for which breeder documents and birth certificates are an essential element.

#### **OBJECTIVES OF THE ORIGINS PROJECT**

As a first phase of the project, the partners have carefully investigated the current state of breeder documents issuing practices in Member States and associated countries.

The main objectives of ORIGINS can be summarized as follows:

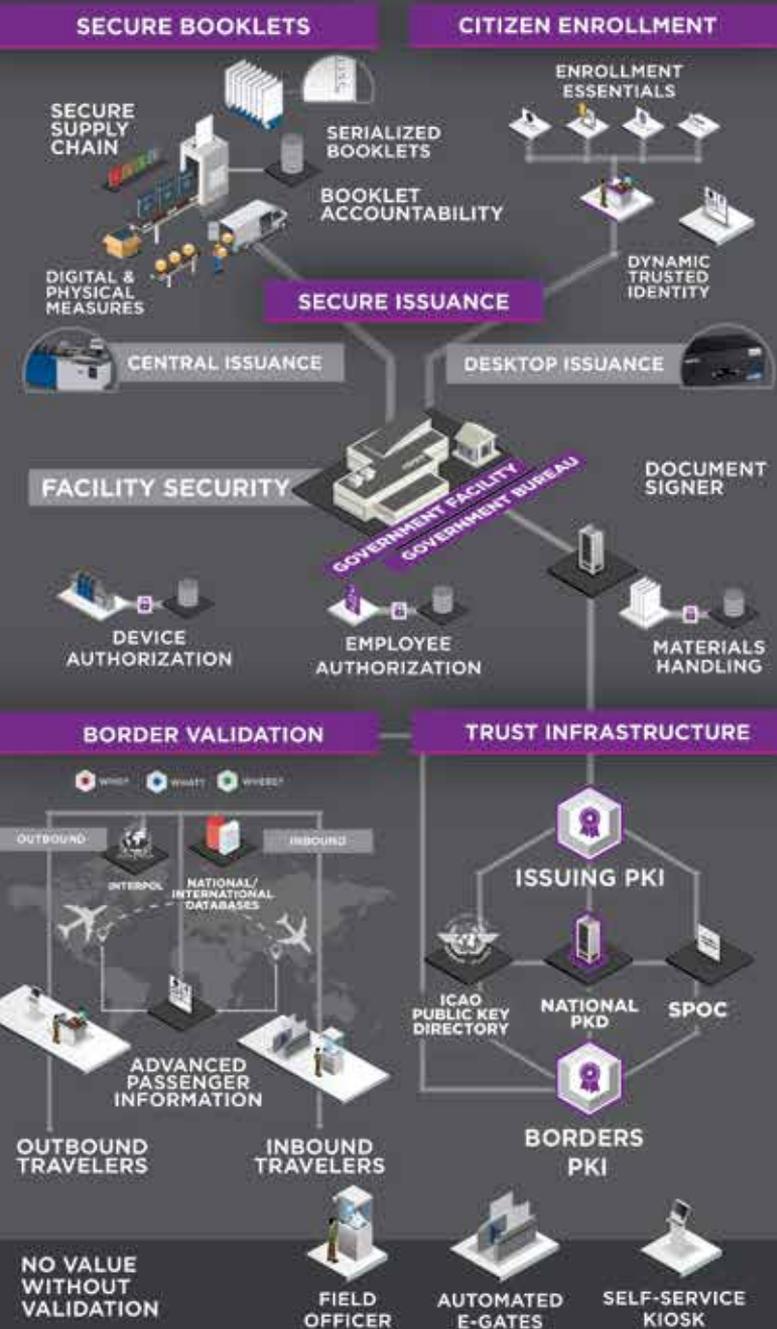
- identify best practices of each State in the area of breeder documents, and provide a guide for minimum level security in Europe;
- develop a tool-kit with multi-level security from which Member States can derive technology suggestions for their own breeder documents implementation;
- supply technical know-how and assist the breeder document community to set up specific training for checking documents used in the ePassport application process;
- initiate a standardization project on breeder documents as a new work item for CEN, the European Committee for Standardization (CEN TC224), based on the proposed technical and procedural solutions;
- establish a link to the ICAO New Technologies Working Group’s (NTWG) initiative on breeder documents;
- facilitate the access to training/availability of training materials (and possibly tools) for the verification of breeder documents by ePassport issuance officers;
- study the ethical, societal and legal aspects related to breeder documents in general and of the proposed recommendations in particular;
- disseminate the results to the issuance community and other relevant communities (such as the border control community), as well as standardization groups; and
- promote the need for requirements for breeder documents at a European level toward Member States, so that they can put regulations in place.

The implications of this should be considered in the context of the existing situation: more than half-a-billion breeder documents have been issued in Europe, there is an on-going roll-out of millions of ePassports (valid for up to 10 years), and any innovative solution must be introduced progressively, ensuring backwards compatibility (i.e. compatible with existing standards, processes and infrastructure for the millions of ePassports already issued) in order to safeguard investments made.

# MODERN BORDER SECURITY

## HOW COUNTRIES OF ALL SIZES CAN BETTER PROTECT THEIR CITIZENS, BORDERS & BUDGETS

Every country faces critical challenges at their borders. The technologies required to address these challenges exist today. Entrust Datacard is helping forward-thinking governments with leading technologies to create highly effective trust infrastructures. The result? Greater security, improved efficiency and lower cost.



SEE THE TRUST INFRASTRUCTURE INFOGRAPHIC IN FULL DETAIL AT [WWW.ENTRUSTDATACARD.COM/BORDERS](http://WWW.ENTRUSTDATACARD.COM/BORDERS)

The major impact of ORIGINS will be to restore trust and confidence in ePassports and breeder documents by recommending solutions that deal with the identified security limitations, while protecting the privacy of ePassport holders. This is important to enable the further deployment of both ePassports and other ID documents. As a matter of fact, other documents issued by Member States rely on breeder documents including: ID cards, residence permits, applications for naturalization, applications for a marriage/divorce, and registrations in the commercial registers.

### PIONEERING ACTIVITIES

Based on the project's findings, ORIGINS will provide recommendations to leverage the security of the life cycle of critical documents. Emphasis will be placed on relationships with issuance officers (application, renewal and loss and robbery claims) in order to provide secure primary-line processes. Other parameters, such as the support of supplementary documents to breeder documents, will be considered. Advanced research will be conducted into state-of-the-art security mechanisms, cryptography and security features to be added to ID documents.

Although security features may be implemented based on a standard and secure format, there will always remain the need to ensure the reconciliation between applicants and their credentials during the issuance process. As for proof of identity, the integration of biometric technologies will be investigated (in particular, biometric-related issues such as aging effects since childhood and template protection). The inclusion of biometrics from the breeder document holder's parents will also be studied with a view to building a secure link to guarantee the identity of the individual since birth.

Concerning the provision of future breeder documents, the prevailing aim is to build upon existing/ongoing research (for instance, integrating compressed biometric data with birth certificates in the form of a bar code). A strong focus on existing or in-development security features will also be performed (bubble tag, data-matrix, laminated technologies, secure paper) in order to determine which are the most appropriate methods of securing future breeder documents.

### DISSEMINATION ACTIVITIES

The consortium has set up an ambitious communication strategy to inform the Commission and the broader breeder documents, ePassport and policy communities on the outputs of the project on an ongoing basis. In order to exchange with broader communities (ePassports, issuance bodies, policy, governments or border control), the consortium is currently organizing a standardization workshop to present the preliminary results and preliminary recommendations on breeder documents security to external stakeholders.

It is expected that ORIGINS Project results will continue to live beyond the end of the project, in particular via think-tank groups developed during the project, standardization groups and the implementation of recommendations. ■

# THE ROADMAP FOR IMPLEMENTING NEW SPECIFICATIONS



## TOM KINNEGING

He is the senior advisor on ICAO and eIDAS regulations at Morpho. He is also the convenor of ISO/IEC JTC1 SC17 Working Group 3, the group, in close cooperation with ICAO, that is responsible for the development and maintenance of the standards for Travel Documents, ICAO Doc 9303 and ISO/IEC 7501.

In this function he is an active contributor to the work of the Technical Advisory Group, the New Technologies Working Group and the Implementation and Capacity Building Working Group of ICAO and has been the lead editor of various technical papers, such as Technical Reports, ICAO Doc 9303 and its Supplement.

## ✈ INTRODUCTION

Travel documents are continuously evolving. Though the effectiveness of their advancements are directly tied to the application of existing or new security features and/or specifications, it is critical that all pertinent stakeholders involved in the production, use and inspection of these documents are aware of, and/or are configuring their systems to fully leverage any security and facilitation advantages that are offered, with new or enhanced international specifications.

Experiences in the past show that, although ICAO's Technical Advisory Group (TAG) on the Traveller Identification Programme (TRIP) – formerly TAG on Machine Readable Travel Documents (MRTDs) – endorsed new specifications in the form of Technical Reports (TR), sharing these Technical Reports on the ICAO website was not always enough to trigger stakeholders to undertake the necessary actions required to implement them. The challenge with having new material is that its existence doesn't reach the entire audience and its importance, and the reasons for revising the specifications, are not clearly communicated.

The introduction of new travel document technologies is a gradual learning process that requires adaptation from the organizations that issue these documents, as well as those that use them and supporting systems to effectively manage travelers at points of entry and departure. Ensuring that all affected systems and processes are effectively modernized is needed if States are to fully benefit from improved document functionality. More specifically, new reading systems, new storage media, and new measures that are required to protect privacy and ensure data integrity and interoperability must all be addressed.

More guidance is needed for the implementers of both inspection systems and MRTDs on the implementation strategy that is to be followed.

With this in mind, a Roadmap for the implementation of new specifications has been developed to raise awareness on key advancements of travel document specifications, and to ultimately support the introduction of new specifications. It should be noted that the roadmap itself does not impose additional specifications; it is simply the guidance which provides information about the implementation of new specifications.

The Roadmap will be published each time new specifications are adopted, and will be made available through a range of channels, such as the ICAO website ([www.icao.int/security/FAL/TRIP/Pages/Publications](http://www.icao.int/security/FAL/TRIP/Pages/Publications)), the ICAO TRIP Platform, symposia and seminars, and through this ICAO TRIP Magazine.

This Roadmap provides information on implementation issues related to:

- (Backwards compatibility) consequences for MRTDs and systems;
- Additional pre-requisites to be met before implementation (such as the availability of test specifications);
- The path to be followed by States and implementers;
- Time tables (planning diagrams) for updating inspection systems; the overlap period with respect to issuing new features in MRTDs; the time period in which both 'old' and 'new' MRTDs will be in circulation; and the timing of when 'old' specifications become deprecated.

**ROADMAP FOR IMPLEMENTATION OF NEW SPECIFICATIONS - RELEASE 1**

The first release of the Roadmap provides guidance on the implementation of the following Technical Reports and updates, which do not necessarily contain new specifications right now, but have been published before and were not given the attention that is needed.

1. **Technical Report "Supplemental Access Control (SAC)"**
2. **Logical data Structure V1.8**
3. **Updated certificate profiles**

**1. TECHNICAL REPORT "SUPPLEMENTAL ACCESS CONTROL"**

Two subsequent versions of the Technical Report "Supplemental Access Control (SAC)" have been published. The Technical Report specifies the use of Password Authenticated Connection Establishment (PACE) in addition to Basic Access Control (BAC) i.e. (SAC=BAC+PACE).

**Technical Report V1.01 – 2010**

ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents", V1.01, November 2010 was endorsed by the TAG in its 19<sup>th</sup> meeting in December 2009 (emphasizing the final version to incorporate the result of a patent discussion). It specifies the PACE protocol containing two variants of mappings, the generic mapping and the integrated mapping.

**Technical Report V1.1 – 2014**

ICAO Technical Report "Supplemental Access Control for Machine Readable Travel Documents", V1.1, April 2014 was endorsed by the TAG in its 22<sup>nd</sup> meeting in May 2014. This is an update of the 2010 version in the sense that an optional additional mapping for the PACE protocol, the Chip Authentication mapping, has been added.

The V1.1 version of the Technical Report has been incorporated in the Seventh edition of Doc 9303 – *Machine Readable Travel Documents*.

**Backwards compatibility**

The PACE protocol for chip access and communications encryption is different from the BAC protocol, which is in use in eMRTDs since 2004. The technical report specifies the use of PACE in addition to BAC instead of the use of only PACE, because inspection systems may not all support PACE yet. PACE is a recommended addition.

To allow for inspection systems to implement support for the PACE protocol a conversion period has been defined by the ICAO New Technologies Working Group (NTWG) (see *Implementation strategy*).

**Implementation pre-requisites**

The addition of PACE to the specification in the Technical Report "Supplemental Access Control" has implications for the test framework in the RF and Protocol Tests Part 3 (Tests for Application Protocol and Data Structure). The test specifications have been extended to accommodate the new protocols in the updated ICAO Technical Report "RF protocol and application test standard for eMRTD - part 3", V2.07, October 2014.

**Implementation strategy**

According to the outcomes of the 19<sup>th</sup> meeting of the TAG, PACE should be implemented in eMRTDs "within a period of 5 years", which was approximately by 1 January 2015.

BAC being present on the eMRTD ensures that inspection systems that do not support PACE (yet) will still be able to access the eMRTD's chip with access control. To access eMRTDs supporting only PACE, inspection systems will need to support PACE. For inspecting authorities and inspection system vendors to prepare their systems to support PACE a date has been established before which MRTDs supporting only PACE are not considered to be ICAO compliant. The chosen date should provide enough time for inspection system owners and vendors to implement the necessary modifications to their systems.

**Time table for implementation of PACE.**

	2010-01	2015-01	2018-01	2020-01	2025-01	2028-01	2030-01
Being issued	BAC-only		end date tbd				
	BAC + PACE		depends on BAC depreciation date				
	PACE-only						
In circulation	BAC-only		end date tbd				
	BAC + PACE		depends on BAC depreciation date				
	PACE-only						
IS update							



In its meeting on 19-21 February 2013 the NTWG concluded that as of the date 01 January 2018 eMRTDs supporting only PACE will be considered to be ICAO compliant.

A date for BAC to become deprecated has not been established yet. It would make sense to declare BAC deprecated once all inspection systems support PACE, which is planned to be in January 2018 according to the aforementioned NTWG's conclusion.

## 2. LOGICAL DATA STRUCTURE (LDS) V1.8

In its 20<sup>th</sup> meeting (September 2011) the TAG endorsed ICAO Technical Report "LDS and PKI Maintenance", V1.0, May 2011. The Technical Report provides a revised specification for the versioning information in the LDS to be implemented in the LDS, revision V1.8.

The new specification is incorporated in the Seventh edition of Doc 9303.

### Backwards compatibility

The change has an impact on inspection systems. These systems will need to be able to parse the document security object (SOD) V1 structure, which is an updated version of SOD V0 defined in the Sixth edition of Doc 9303. When the EF.COM is not present,

version information (both the LDS version as well as the SOD version) can only be retrieved from the SOD. Therefore in LDS V1.8 the change has been implemented in the SOD whilst the EF.COM remains present.

### Implementation pre-requisites

The test specifications have been extended to accommodate the LDS V1.8 specifications in the updated ICAO Technical Report "RF protocol and application test standard for eMRTD - part 3", V2.07, October 2014.

### Implementation strategy

With this change, all information presented in the EF.COM, has been duplicated in the SOD. This means that the EF.COM will be removed from the specifications from the next LDS version after V1.8. Issuing States should implement this change in their MRTDs as soon as possible. A period of five years from the endorsement date after which all issuing States will have implemented LDS V1.8, is assumed.

Inspection systems that rely on the EF.COM need to be modified to use the SOD as soon as possible, since the next version of the LDS after V1.8, the EF.COM, will be removed from the specifications and systems from then on rely on the SOD for obtaining version information.

Time table for the implementation of LDS version 1.8.

	2010-01		2015-01	2018-01	2020-01		2025-01	2028-01	2030-01	
Being issued	LDS V1.7 <span style="float: right;">depends on V1.7 deprecation date →</span>									
	LDS V1.8									
In circulation	LDS V1.7 <span style="float: right;">depends on V1.7 deprecation date →</span>									
	LDS V1.8									

### 3. UPDATED CERTIFICATE PROFILES

In its 22<sup>nd</sup> meeting (May 2014) the TAG endorsed ICAO Technical Report "LDS and PKI Maintenance", V2.0, April 2014. The certificate and certificate revocation list (CRL) profiles in this edition of the Technical Report integrate the inherited detailed technical requirements from RFC 5280 directly. This approach should provide an increased support to implementers as all the requirements are presented together.

This version of the Technical Report has been incorporated in the Seventh edition of Doc 9303.

#### Backwards compatibility

The profiles use the following terminology for presence requirements of each of the components/extensions:

- m** = mandatory, the field **MUST** be present
- x** = do not use, the field **MUST NOT** be populated
- o** = optional, the field **MAY** be present

The profile uses the following terminology for criticality requirements of extensions that may/must be included in certificates:

- c** = critical, the extension is marked critical, receiving applications **MUST** be able to process this extension.
- nc** = non-critical, receiving applications that do not understand this extension may ignore it. The indication non-critical is an addition to the previous certificate profiles specifications.

These certificate profiles impose new requirements to the certificate issuers. From an interoperability point of view relying parties should be capable of accepting certificates that conform to the previous profile, as well as the profiles specified in this Technical Report.

**Implementation pre-requisites** – not applicable

#### Implementation strategy

Issuers are recommended to start issuing certificates conforming this new profile starting at their next Country Signing Certification Authority (CSCA) roll-over. It is assumed that for each CSCA the next roll-over will occur within five years from the publication date of the Technical Report. ■

Time table for the implementation of the updated certificate profiles.

	2010-01		2015-01		2018-01	2020-01		2025-01		2028-01	2030-01	
Being issued	CSCA_1 *											
				CSCA_2 **								
In circulation	CSCA_1 *											
				CSCA_2 **								

- \* Certificates and CRLs according to profiles set out in TR - LDS & PKI Maintenance V1.0
- \*\* Certificates and CRLs according to profiles set out in TR - LDS & PKI Maintenance V2.0

**SEMLEX GROUP**  
BIOMETRIC IDENTIFICATION

Semlex provides solutions to secure identification and authentication using biometric information.

Semlex finances and operates systems according to governmental needs.

www.semlex.com  
europe@semlex.com

Document production and personalization

Biometric border control

# THE EVOLUTION OF THE JAPANESE PASSPORT



**ABOUT AKIRA ENDO**

He is the Director of the Passport Division, Consular Affairs Bureau in the Ministry of Foreign Affairs of Japan. He is responsible for issuing passport and overseas travel and has worked in several diplomatic establishments abroad, including the Permanent Mission of Japan to the United Nations.

✈ Showcasing more than 1,500 booths from Japan and 140 States around the world, Tokyo's *Tourism EXPO Japan 2016*, which was held from 22 to 26 September 2016, welcomed a crowd of 190,000 visitors. One of the big highlights at the exposition was "The 150<sup>th</sup> anniversary of Japanese passport issuance" booth, which was hosted by the Ministry of Foreign Affairs of Japan (Image 1).

At the time the original first 'passports' were introduced as a travel document in Europe required to pass the checkpoints of walled cities, Japan was in the Edo Era (1603-1868) and had adopted an

isolationist policy under the rule of the Shoguns (hereditary military commanders). In 1866 Japan decided to open its borders and allowed overseas travel to the general public. The first batch of Japanese passports (Image 2) was issued to 18 members of an acrobatic troupe to attend the Paris International Exposition. One of them is now kept in the Japan Diplomatic Archives – and was exhibited, along with a variety of other Japanese passport models at the Tokyo Tourism Expo.



Image 2 : First Japanese passport

The 150-year legacy of Japanese passports reflects the evolution of travel documents worldwide. In 1917, Japan began to issue passports with photos attached, and in 1926, the book-type passport was introduced. Machine-readable passports were introduced in 1992, and in 2006, ePassports launched, reflecting the rapid development of Information Technology. In recent years, in response to the global need for tackling passport forgery, Japan has been working to consolidate advanced technologies to ensure the legitimacy of its travel documents.

Japan will host the Olympic and Paralympic Games in 2020 and is planning to issue its next model of passport in 2019. The model will be modernized with some distinctive Japanese technologies that protect it against forgery, and it will also introduce typical Japanese illustrations on the visa pages.

The theme that was chosen from the contenders is from Hokusai's world-famous woodblock print series "Thirty-Six Views of Mt. Fuji" (Image 3), which depicts Mt. Fuji as it is seen from various locations in Japan.



Image 3 : Illustration on visa page of the next Japanese passport

The bearer of this passport will be able to enjoy a different view of Mt. Fuji on each page. On the heels of 150 years of achievement, the Japanese passport is taking steps to make its mark on a new page of history. ■

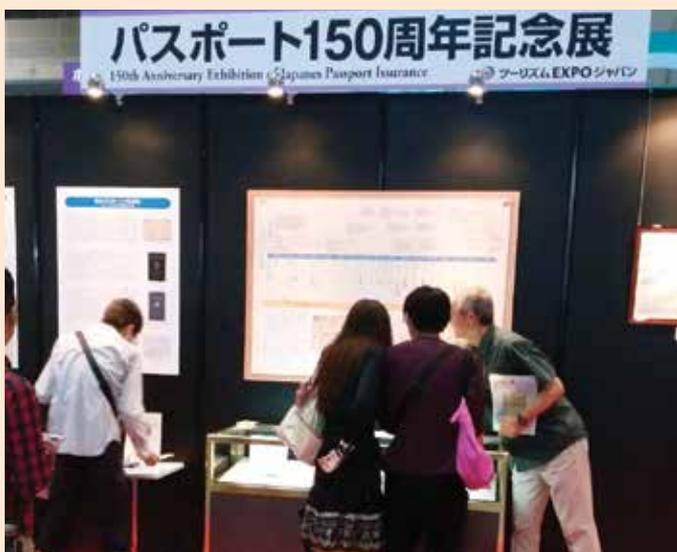


Image 1 : Booth of the 150<sup>th</sup> anniversary of Japanese passport issuance



Every year, ICAO organizes two ICAO TRIP Regional Seminars focused on strengthening aviation security through improved traveller identification. Relying on the generous support of Host State authorities, Regional Seminars have taken place in:

Brazil (2012), Burkina Faso (2013), Islamic Republic of Iran (2016), Kenya (2015), Mozambique (2010), Nigeria (2010), Qatar (2011), Singapore (2011), Sint Maarten - Dutch Antilles (2013), Spain (2014), Uruguay (2010), Uzbekistan (2014) and Zimbabwe (2012).

An upcoming Regional Seminar will be held in St. John's, Antigua and Barbuda from 31 January to 2 February 2017.

# IN SEARCH OF HOST STATES

**ICAO TRIP REGIONAL SEMINARS  
IN 2017 AND BEYOND**

## BENEFITS OF HOSTING

ICAO TRIP Regional Seminars address the five elements of the ICAO Traveller Identification Programme (ICAO TRIP) Strategy: machine readable travel document (MRTD) standards; specifications and best practices; secure travel document issuance; and the robust evidence of identity processes. Seminars also look at information technologies such as: Advance Passenger Information (API) highly relevant to the execution of the UN Security Council Resolutions 2178 (2014) and 2309 (2016) agreement on combatting foreign terrorist fighters, with a special focus on effective border management control, and emphasize the importance of issuing ICAO-compliant machine readable travel documents and participation in the ICAO Public Key Directory (PKD).

Besides the recognition they get in supporting ICAO's Strategic Objectives, Seminars have a strong regional focus and address challenges specific regions face. They provide an opportunity for States, and in particular, the Host State Authorities, to become better informed about ICAO TRIP technical specifications and to discuss their technology concerns, requirements and assistance needs with the ICAO Secretariat, ICAO TRIP experts and the donor community, allowing them to explore options for further capacity building activities.

## BENEFITS OF AN ICAO TRIP EXHIBITION

Each ICAO TRIP Regional Seminar is complemented by an exhibition which allows the industry to display a broad range of products and services related to MRTDs, biometric identification, travel document security applications and border management systems. Exhibitions provide an opportunity for Member States to familiarize themselves with the latest available technologies and solutions and discuss any special requirements or challenges they may have directly with on-site industry representatives.

## CONTACT

For details about becoming a Host State of an ICAO TRIP Regional Seminar, please contact the ICAO Facilitation Section at [FAL@icao.int](mailto:FAL@icao.int).

For more information on exhibition opportunities, please contact ICAO Marketing and Sales at [icao-trip-events@icao.int](mailto:icao-trip-events@icao.int)

## ICAO TRIP EVENTS

For more information on ICAO TRIP events worldwide, visit the ICAO website at <http://www.icao.int/Security/FAL/TRIP/Pages/Events.aspx>

# THE TRAINAIR PLUS METHODOLOGY: VALIDATION PROCESS FOR A STANDARDIZED TRAINING PACKAGE

## “Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1”



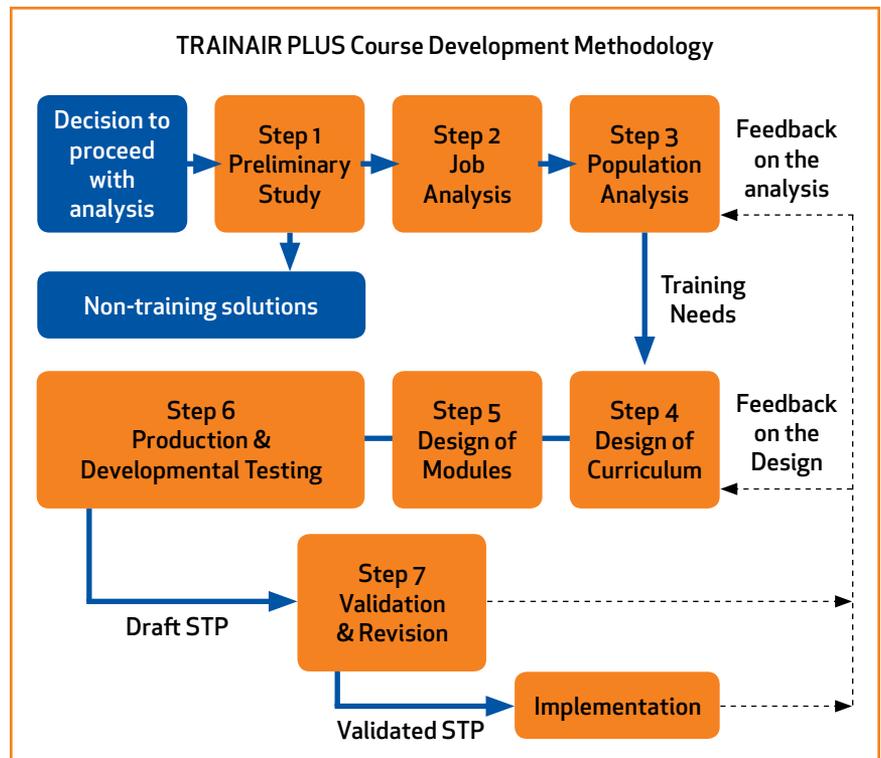
**JACQUES BELINGA ONANA**  
He is currently the Senior Air Traffic Control Instructor and Chief Teaching Methods at EAMAC. Furthermore, he is an ICAO TRAINAIR PLUS Training Developers Course (TDC) Instructor and ICAO TRAINAIR PLUS Standardized Training Package (STP) Validator. He is also a recipient of the 2015 TRAINAIR Plus Programme ICAO John CHAPMAN award.



**KARINE BOULET GAUDREAU**  
She has been working as the consultant in the ICAO Secretariat in Montréal responsible for implementing Canada-funded projects in the Sahel and the Caribbean Regions under the ICAO Traveller Identification Programme (TRIP) Strategy since July 2014. She previously worked for the Canadian government in various positions with Global Affairs Canada, mainly focusing on security and political affairs in West Africa and the Sahel.

✈ In July 2016, the International Civil Aviation Organization (ICAO) launched a new ICAO Training Package (ITP) entitled *Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1*. The initiative was undertaken through the Canada-funded project “Strengthening Travel Document Security and Identification Management in the Sahel and neighboring States”.

The development of a training package that complies with the TRAINAIR PLUS methodology referenced in ICAO’s *Training Development Guide, Competency-based Training Methodology* (Doc 9941) involves a seven-step process. Between January 2015 and July 2016, the development team composed of the Course Development Unit (CDU) from the École Africaine de la Météorologie et de l’Aviation Civile (EAMAC) based in Niger, a team of senior Subject Matter Experts (SME), jointly led by the Global Aviation Training (GAT) Office and the Facilitation Section, completed this process.



The development phase began during the ICAO Traveller Identification Programme (TRIP) Implementation Regional Seminar that took place in Niamey, Niger in January 2015. An analysis of the training needs to be addressed by this ITP was performed, in consultation with authorities in charge of border security in the Sahel. It was then established that the training package would address the consolidation of the competencies required by front-line border control officers from immigration and other airport border control authorities to examine travel documents effectively, allowing them to expedite the movement of legitimate travellers while identifying high-risk individuals.

The months that followed were dedicated to designing the training through intensive collaborative work of the development team, in order to create a product that would assist border control officers in playing their critical role of performing the initial screening of all passengers crossing borders, and in identifying individuals that may be travelling for illegitimate purposes.

The last step of the development process involves the validation of the course. Validation delivery is the first implementation of a newly developed ITP to an experimental group (EP) of at least 10 trainees who are selected from the primary target population.

#### VALIDATION OF THE ITP IN CAMEROON

The validation delivery was conducted with the valuable support of the École Régionale de Sécurité Incendie (ERSI) located in Douala, Cameroon, from 7 to 11 March 2016. The EP, selected by the general Delegation for National Security of Cameroon, was composed of 10 trainees: eight officers in charge of travel document control and two supervisors working for one of the two main international airports in Cameroon, at Douala and Yaoundé.

None of the trainees were experts in the subject matter, although they were performing the tasks in their daily work, and as such, the group formed the genuine primary target population required for the validation delivery, in compliance with TRAINAIR PLUS methodology.

Four ranking officials also attended the course, as the secondary target population. The four included a diplomat from the Cameroon Ministry of External Relations, a Commissioner from the International Airport of Conakry, Guinea, the Head of the French Regional Training in travel document examination in Ouagadougou, Burkina Faso, and the INTERPOL Specialized Regional Officer based in Yaoundé, Cameroon.

The course was taught jointly by Mr. François-Pierre Déry, formerly of the Canadian Border Service Agency (CBSA), as senior ICAO Instructor, and Mr. Tidiani Coulibaly, Airport Commissioner from the International Airport of Bamako, Mali. Also present during the validation training delivery were Bonnie McEachern, TRAINAIR PLUS methodology expert, Karine Boulet Gaudreault, ICAO TRIP Officer, and Jacques Belinga Onana, TRAINAIR PLUS Expert Validator.

The ITP *Control of the Authenticity and Validity of Travel Documents at Airport Borders – Level 1* is made up of three modules with the following learning objectives:

- identify the basic elements of a travel document and the different types of fraud;
- examine a travel document manually and visually to detect whether it is fraudulent or not; and
- examine a travel document using an electronic document reader to detect whether it is fraudulent or not.

Each module consists of a mix of slides with visuals of the teaching points and practical exercises performed with travel document samples, security paper samples, UV lights, magnifiers, fraudulent passports, identity card samples, as well with machine for reading machine readable travel documents. Critical to the methodology, each module concluded with a Mastery Test where trainees were evaluated on their comprehension of the competencies learned and practiced in each module.



Practical exercises during the training

#### CRITERIA OF VALIDITY OF AN ITP

Based on the Mastery Tests results, the benchmark of validity used in the TRAINAIR PLUS Programme is 80/80. A module is considered valid when at least 80% of the test group achieves at least 80% of the end-of-module objective. The whole ITP is considered valid when the criteria of validity are met for at least 80% of the modules.

The results of the Mastery Tests were analysed by the TRAINAIR PLUS Expert Validator and 100% of the test group achieved at least 80% of the end-of-module objective for each of the three modules. Therefore, 100% of the modules were valid. The ITP on Travel Document Examination met the validation criteria which allowed the validator to declare the ITP fully validated and ready to join the international exchange of training courses through the TRAINAIR PLUS network.



The first fourteen trainees who successfully completed the ICAO training on Travel Document Examination

### FEEDBACK AND REVISION

The last day of the training was dedicated to listening to trainees express their opinions, reactions and queries on the course and the way it was delivered. These comments, along with information collected in a questionnaire, allowed the Expert Validator to diagnose and identify areas needing modification or adjustment.

Based on the observations of the trainees, instructors and Expert Validator, the SME, with the assistance of the course development team, produced the final version of the course in May 2016. The course, which was approved by ICAO in both English and French, is available for implementation worldwide (see: [www.icao.int/Training/Pages/TDexam.aspx](http://www.icao.int/Training/Pages/TDexam.aspx)).

The validation delivery also served to qualify the first two instructors to deliver this new training. After being selected for their expertise, François-Pierre Déry (Canada) and Tidiani Coulibaly (Mali) successfully completed the TRAINAIR PLUS

Training Instructors Course. Given their performance in meeting the TRAINAIR PLUS criteria for instructors during the validation delivery, they became the first ICAO Qualified Instructors for delivering this training. ■

**ICAO's Facilitation Section and Global Aviation Training Office are taking this opportunity to convey their sincere thanks to the CDU and the Expert Validator from EAMAC, the team at ERSI who truly made the validation course possible and the Ministry of External Relations of Cameroon, and for underling the tremendous contribution of subject matter experts, from multiple nationalities (Burkina Faso, Canada, France, Mali, Morocco and United Kingdom), International Organizations (INTERPOL, United Nations Office on Drugs and Crime (UNODC), International Organization for Migration (IOM) and members from ICAO's Implementation and Capacity Building Working Group (especially members from Germany, the Netherlands, Switzerland and the United States). Lastly, we would like to appreciate the contribution of States and regional organizations that provided ICAO with samples of their travel documents that are nowadays used during training delivery; this is significantly enhancing the quality of the training and the hands-on experience of the trainees.**



Tidiani Coulibaly and François-Pierre Déry

NEW



ICAO

# UNITING AVIATION.COM ONLINE MAGAZINE



Interested in expanding your audience?  
Submit SECFAL content to be highlighted on our new website



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



# ICAO'S NEW TRIP PLATFORM RELIABLE INFORMATION: THE BASIS FOR POLICY



## RENEE ONG-DE-JONG

After joining the National office for Identity Data, a special agency from the Ministry of the Interior and Kingdom relations in the Netherlands, as a lawyer from 2003 till 2012, she then became a Research & Development Advisor on travel documents, responsible for the physical part of the travel documents. Ong-de-Jong participates in the International Capacity Building Working Group from ICAO and leads the sub-working group infoTRIP.



## INTRODUCTION

Without dependable information, governments cannot effectively develop solid policies. Participants at ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD/22) that was held in Montreal in May 2014, broadly pronounced their support for Working Paper (WP/19) which contained the Implementation and Capacity Building Working Group's (ICBWG) proposal to set up a secure online ICAO Portal – or Group - environment. Within the Group – now known as the **infoTRIP Group**, authorized governments and international organizations would be able to store, use, and maintain their information in a secure setting that would allow for information sharing.

After receiving the approval of TAG, the ICBWG set up a sub-working group to develop the **infoTRIP Group**. This article describes the work of the ICBWG sub-group.

## COMPOSITION OF THE SUB-GROUP

Following TAG/MRTD/22, the ICBWG formed the sub-group with representatives from Canada, the Netherlands, Portugal, the United Kingdom, the United States of America, the International Organization for Standardization (ISO) and ICAO. The sub-group closely studied the history of the portal concept and the assignment, as outlined in TAG/MRTD/22 WP/19, during its first meeting, which was held in The Hague in April 2015.

## HISTORY

In 2004, the Netherlands began researching the European Union (EU) States that were working on the development of a biometric passport. Their findings determined that the exchange of information between States was only taking place on an incidental basis and that there was a need for a permanent online facility where information could be retained. At the time, information was being exchanged through an online portal called the International Forum for Travel Documents (IF4TD).

The IF4TD could only be accessed by authorized officials of governments and international organizations and document information was entered in the portal by individual participants. Two things became clear: that the portal was meeting a demand, and that States outside the EU also wanted to join. The Netherlands collaborated with other States to expand the IF4TD, but it became apparent that ICAO should assume responsibility for the operation of the portal, given the global role of the Organization. After consultations, ICAO took over the responsibility for the portal from the Netherlands and asked the ICBWG to revitalize the contents of the Portal while making use of the new ICAO TRIP Platform that ICAO was developing.

## CURRENT SITUATION

With the implementation of the ICAO TRIP Strategy in 2013 and following other developments at ICAO, the Sub-Group analysed the content in the IF4TD portal and compared results with the objectives of the ICAO Trip Strategy. The analysis quickly showed that the content of the IF4TD portal had a strong focus on travel documents from the perspective of an issuing institution, while the TRIP Strategy looks at all aspects of traveller identification management. The finding led the Sub-Group to reconsider the assignment as it was formulated in WP/19 and as a result, users of the new infoTRIP Group will be able to store and retrieve information in accordance with the subjects contained in the ICAO TRIP Strategy (Figure 1).



Figure 1: ICAO TRIP Strategy



Figure 2: InfoTRIP logo

To begin, the Sub-Group determined a name for the new, secure portal, which would be accessed by authorized officials from governments and international organizations: **infoTRIP Group**. A logo was designed (credit to Alma van Vliet) to make the infoTRIP Group recognizable (Figure 2).

## CONTENT

The content of the infoTRIP Group is broader than the original IF4TD portal, incorporating the following areas corresponding to the ICAO TRIP strategy:

- **General information on the infoTRIP Group;**
- **Evidence of Identity;**
- **MRTDs;**
- **Document Issuance and Control;**
- **Inspection Systems and Tools; and**
- **Interoperable Applications**

While the IF4TD Portal only contained information on MRTDs and Document Issuance, the infoTRIP Group will contain additional data that better meets the information requirements of governments. Because the areas covered in the infoTRIP Group, like the ICAO TRIP Strategy are diverse it is possible that they fall under the responsibility of different organizations or departments within a particular country.

## ICBWG SUPPORT

At the ICBWG Working Group meetings, which were held in Samoa in May 2015 and Ottawa in October 2015, the Sub-Group provided feedback on its activities. The proposals of the sub-group for the name 'infoTRIP' and the adjustments to the portal content (to be in-line with the ICAO TRIP Strategy) were approved by the ICBWG.

Additionally, the proposal to set up an Editorial Board was also accepted, with the Members of the sub-group sitting on the Board. The Editorial Board will define access rules for the infoTRIP Group while also monitoring the quality of the information provided by members of the infoTRIP Group. Where necessary, the Board will encourage parties to enter or update their information on the infoTRIP Group. The Editorial Board will work closely with the ICAO Secretariat in Montréal who have responsibility for managing and administering the ICAO TRIP Platform on which the new infoTRIP Group is located.

At the First Meeting of the Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP/1) which was held from 30 March to 1 April 2016 in Montréal, TAG/TRIP greeted the work of the Sub-Group enthusiastically and endorsed the continued work on development and implementation on the infoTRIP Group.

## DEVELOPMENT AND IMPLEMENTATION

For technical issues related to the infoTRIP Group work during development and implementation phases, the Sub-Group is supported by ICT experts at ICAO Headquarters in Montreal, who also carry-out installation and technical maintenance on the system as required.

## infoTRIP GROUP INPUT

A point of contact (POC) will be based in each State or organization. The POC will be the focal point of contact for ICAO and will be responsible for recruiting experts within their State or organization who will input, and maintain, data in the infoTRIP Group on the ICAO TRIP Platform. Information must be accurate and reliable and contact people must be assigned for each TRIP area. In the event that somebody retrieves data and requires further information, they should be able to contact the State nominated organization/expert listed in the ICAO TRIP Platform, to obtain practical and direct information.

Although the sub-group has taken steps to be as clear as possible about the subjects on the infoTRIP Group, the person entering the information may still be unclear. In such cases, they should contact the ICAO Secretariat to avoid input errors.

## USE AND MAINTENANCE

### Use

Only those who are authorized as the SPOC have access to the Portal and the data stored on it. A State is allowed to look at the data from another State or organization when their own State or organization has added over 50% of the requested information in the Portal. This incentive was created because a Portal without information is useless. Whether one has a simple question that needs to be answered or a complete overview is needed, infoTRIP Group functionality can generate several defined reports, reports that can be compiled by individual users or requested and compiled by the Sub-Group.

### Maintenance

Various topics that are at issue in the ICAO TRIP Strategy are relatively dynamic and as such, topics will change frequently

with new solutions implemented. It goes without saying that renewals and adjustments will have to be updated in the infoTRIP Group. This maintenance is the State or organization's responsibility. Maintenance must be taken seriously because out-of-date information might cause confusion and should be avoided.

### PLANNING

The sub-group is working closely with the ICAO Secretariat to make the final changes to the construction of the infoTRIP Group within the ICAO TRIP Platform. The sub-group members have successfully begun to add the necessary information from their own States with success in the infoTRIP Group.

Following this, governments and international organizations will be invited to appoint their own national focal points. Once authorization has been provided, focal points can begin entering information in the Portal and using it to ensure up-to-date, reliable information from, and for, governments is available.

The goal is to present the definitive version of the Portal during the ICBWG which is to be held in December 2016 and for the new infoTRIP Group to 'go-live' in early 2017. ■



## Perfection in every detail

**Gemalto's new Sealys Premium eCovers** for electronic passports deliver superior flexibility in bookbinding operations, as well as greater durability and better visual impact on booklet closing.

With improved processability on all manufacturing equipment, booklets can be produced to the highest possible standards.

So now you can count on Gemalto's inlays and electronic covers to provide enhanced performance in a seamless migration to electronic passports.

➔ [GEMALTO.COM/GOVT](http://GEMALTO.COM/GOVT)



# GUIDANCE FOR CIRCULATING SPECIMEN TRAVEL DOCUMENTS

## INTRODUCTION

Based on ICAO recommendations (ICAO Doc 9303 – *Machine Readable Travel Documents, Seventh Edition, 2015*), all States launching a new design of a machine readable travel document should inform all other States of the details (*Doc 9303, Part 2 – Specifications for the Security of the Design, Manufacture and Issuance of MRTDs; and Part 5 – Specifications for TD1 Size, Machine Readable Official Travel Documents (MROTDs)*).

When States are sharing new MRTD specifications with other States, they should include information on evident security features and provide personalized specimens for use as a reference. The distribution of the specimens should be made to established contact points who are responsible for verifying the authenticity of such documents.



Many States are not aware of the options available for sharing specimen documents with the wider travel document and border control communities. The Implementation and Capacity Building Work Group (ICBWG), a subgroup of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP), has produced the following guidance for circulating specimen travel documents along with sample letters that should accompany the specimens pack.

Sample letters (available in all six ICAO official languages) and other relevant documents and guidance material, can be found on ICAO's website under the Security and Facilitation Section, Publications, Guidance Material at [www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx](http://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx)

Additional Parts of Doc 9303 should be taken into account when a State is launching a new design of machine readable travel document: *Part 1 – Introduction* and *Part 3 – Specifications common to all MRTDs*.

To facilitate international travel, Member States issuing passports must distribute specimens to other States. This should be done as widely as possible and is extremely important when an issuing State introduces a new passport or updates an existing design with new features.

By sharing their passport specimens, a border authority would have a strong base for conducting a visual or forensic comparison and could more easily identify a falsified passport. There is also a benefit for travellers in that the State would have be familiar with their travel document. This guidance

establishes the process that needs to be followed to achieve the minimum standard of communicating the features of a new passport and how this might be achieved, as well as an example of a best practice.

#### AIMS

The intent in sharing this process is to ensure that all receiving States are aware that an issuing State has introduced a new or updated passport; has sight of its design and security features; and has at least one specimen.

Receiving States can decide where to retain the sample specimen(s) according to their own internal policies, however, where no policies exist it is recommended that this be the border control authority. This paper also suggests ways in which the distribution might be achieved.

#### PROCESS

Passport specimens are generally distributed via Diplomatic exchange. Methods for achieving this will vary from State-to-State, Doc 9303 (Part 3 and Part 5) includes the list of countries specimens should be sent to. While this may be used as a check list, it should not be considered an exhaustive list because in many cases, dependencies, regions and non-State entities may also benefit from having specimens.

For some Member States this can be achieved by writing to the Embassy or High Commission of each country that is represented in that State. Addresses can be found in a local version of the List of Diplomatic Missions or on the internet on [www.embassyinformation.com](http://www.embassyinformation.com)

Specimens should also be sent to the organizations that offer a secure reference database of images of passports and their security features. These image databases are made available to bona fide bodies with a genuine need to authenticate MRTDs (border control authorities, other government departments, carriers, banks, etc). Furthermore it is advisable to share specimens with manufacturers of passport readers to ensure that their systems can read the MRZ and chip (for new ePassports), and to ensure they can develop the templates used by readers for optical verification of physical security features (i.e. placement of holograms and optically variable ink, etc). This also helps to ensure that readers are fully compliant to international standards, which in turn benefits the States that might buy the readers.

From an issuing State and traveller perspective, sharing specimens as early as possible will reduce the likelihood of travellers being unnecessarily referred to secondary inspection.

Since more organizations are commercial businesses, they are not listed in this paper, but they can be identified via web searches. Though it will vary from State-to-State, for many countries distribution will be the responsibility of the Department of Foreign Affairs, since that department is most likely to have representation in other Member States.

Other routes through which distribution might be achieved is through regional bodies such as the European Union, CARICOM,

OAS, ASEAN, etc., or through representatives of the issuing State assigned to ICAO in Montreal. Ideally the specimens will be received by the Government Departments responsible for border control, but as stated previously, this may not be the case in every country.

### SPECIMENS PACK

It benefits receiving States, if the issuing State provides details of the security features of their new or updated passport with the specimens. This need not be an onerous task, a simple one page leaflet introducing the key features would be sufficient in some cases. Some states may wish to produce a detailed brochure containing images of many of the security features with pouches with the actual specimen inserted.

With the global introduction of eMRTDs, the exchange of the certificates required to reliably authenticate travel documents became a new element that must be considered when information on travel documents are exchanged. Country Signing Certificates (CSCA), Certificate Revocation Lists (CRLs) and Document Signer Certificates (DSC) must be made available to control authorities. The ICAO Public Key Directory (ICAO PKD) is a cost effective, reliable and efficient system to get access to Certificates, including Master Lists issued by PKD Participants containing validated CSCAs. The Certificate exchange and the participation in the ICAO PKD is the modern day addition to the traditional specimen exchange.



### MINIMUM STANDARD

As a minimum, issuing States should send one example, personalized with 'specimen data' of their new ordinary passport, together with a letter detailing the introduction date of the new passport. Where the new passport is an e-passport, the chip should be personalized and the data should match that reproduced on the biodata page. The chip data should be signed by the Issuing State's CSCA.

The accompanying letter should identify the variants of this passport design (Diplomatic, Service, Official, Emergency, etc.) that are to be issued and their date of introduction. Examples of this letter can be found on the ICAO website (link previously provided).

Issuing States should provide information about their personalization processes; identify whether all passports are issued centrally or via a distributed solution; and include reference to overseas issuance. This should be accompanied by at least one specimen from each process if they differ – for example laser toner personalization centrally and inkjet in regional offices.

Where the new documents are eMRTDs, the issuing State should take the opportunity to send a CD with its CSCA-certificate and any DS-certificates already issued.

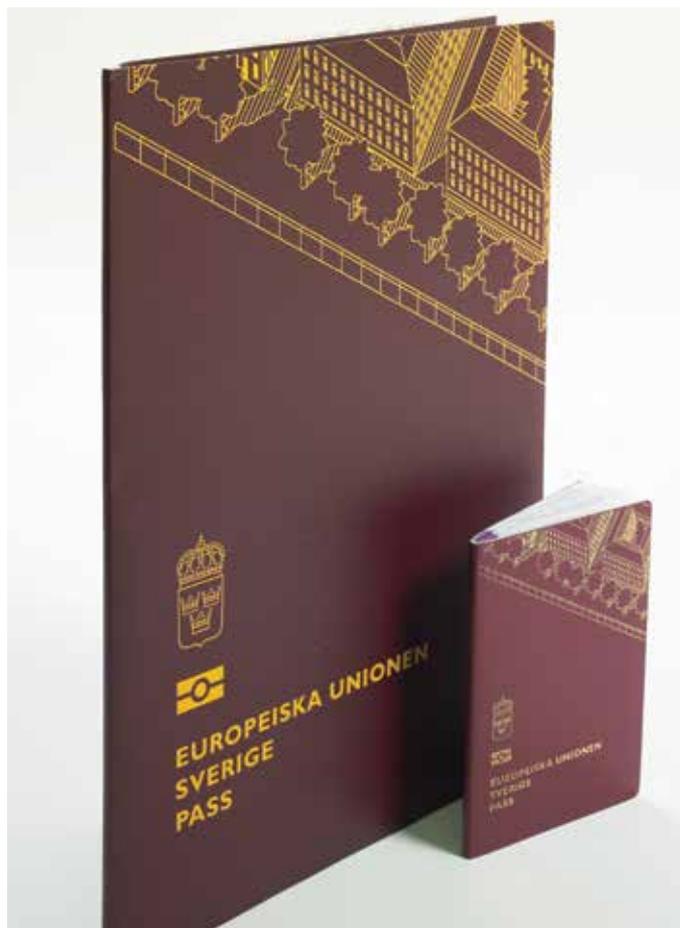
### BEST PRACTICE

Production and distribution of specimens can be expensive for many States, but it is a vital part of introducing a new or updated passport design.

A brochure detailing the key security features of the passport with images and description should be distributed with an example of each passport variant. The brochure or the



“it is vital that specimens are representative”



accompanying letter should also indicate the e-mail address or the government website, if available, where additional information (like CSCA certificate's fingerprint) can be retrieved. Ideally several sets of these specimens should be sent to each receiving state and further sets should be made available on request.

The number of sets required will vary from State-to-State depending upon the number of international crossing points. It is vital that specimens are representative of the actual issuance procedures that are used by the issuing State. If different processes are used for passports that are produced centrally (those that are produced in a distributed issuance process and those that are produced in a Consular office overseas), this should be made clear and specimens from each process should be distributed. ■

# EXHIBITORS AND SPONSORS

**3M** Science.  
Applied to Life.™

**Optical recognition.  
Applied to verifying they  
are who they say they are.**

Visit the 3M booth to learn more about  
3M Security Identification Solutions and  
Border Management Systems.  
[3M.com/IdentityManagement](http://3M.com/IdentityManagement)

**Booth #  
45/46**



3M and 3M Science, Applied to Life, are trademarks of 3M. Used under license in Canada.  
© 2015, 3M. All rights reserved. 1508-03153-E

**Access IS**

**Ludovic Coumétou**  
Head of Sales  
Identity & Security

18 Suttons Business Park  
Reading, Berkshire  
RG6 1AZ, UK  
[access-is.com](http://access-is.com)

m: +44 774 877 0632  
t: +44 118 966 3333  
e: [ludovic.coumetou@access-is.com](mailto:ludovic.coumetou@access-is.com)



P<GBRICHARDSON<  
88826 GB

**Aisino** 航天信息股份有限公司  
Aisino Corporation

Stock Code:600271

**Zhiqiang Liu**  
Aerospace Golden Card Co.  
Shenzhen Office  
Director

Add: 5F, Aisino, No.7018, Beihuan Rd.,  
Futian District, Shenzhen 518049,  
Guangdong, China  
Tel: (86)755 8256 1401  
Mobile: (86)158 1550 0158  
E-mail: [liuzhiqiang@aisino.com](mailto:liuzhiqiang@aisino.com)  
<http://www.aisino.com>

Passports, visa stickers, eID cards  
PRODUCTION AND PERSONALISATION

1102 Budapest, Halom utca 5. Hungary  
Phone: +36 1 431 1200  
[info@any.hu](http://info@any.hu) | [www.any.hu](http://www.any.hu)

**ANY** BIZTONSÁGI NYOMDA  
SECURITY PRINTING COMPANY  
FOUR STAR PRINTING COMPANY



**VERIDOS**

Labinot Carreti  
Senior Vice President  
Global Sales

IDENTITY SOLUTIONS  
by Giesecke & Devrient  
and Bundesdruckerei

**Veridos GmbH**  
Truderinger Str. 15, 81677 Munich, Germany  
Phone: +49 89 41197-330  
Fax: +49 89 41197-87172  
Mobile: +49 173 6378554  
E-mail: [labinot.carreti@veridos.com](mailto:labinot.carreti@veridos.com)

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

**DWIGHT MACMANUS**  
Applications Director  
Identification Systems Division Marketing

18 Auriga Drive  
Ottawa, Ontario, Canada K2E 7T9

Tel: 1 (613) 722-6807 Ext. 4450  
Fax: 1 (613) 722-8494  
E-mail: [dmacmanu@cbnco.com](mailto:dmacmanu@cbnco.com)  
Website: [www.cbnco.com](http://www.cbnco.com)

**cbn**  
CANADIAN  
BANK NOTE  
COMPANY, LIMITED



DeLaRue

De La Rue North America Holdings Inc  
Miami  
Florida  
USA

**Darren Lal**  
Business Development Director  
Identity Solutions

Telephone +1 786 493 1294  
darren.lal@us.delarue.com  
www.delarue.com

EVERY DAY, OUR **SECURE ID SOLUTIONS**  
ARE DELIVERING



- 100,000 ePassports
- 200,000 Smart Cards
- 300,000 Secure ID Cards
- 20,000,000 ePayment Transactions



**Emperor Technology**  
Tel: +86-755-83416677  
www.emperortech.com

Fax: +86-755-83416349  
marketing@emperortech.com

foster+freeman

**Document Examination Solutions**

usoffice@fosterfreeman.com  
Tel: 888 445 5048

fosterfreeman.com



Securing the identity  
of millions of travelers  
worldwide

➔ GEMALTO.COM/GOVT/TRAVEL



GET.Into the future

**GET Group Holdings Ltd.**  
Dubai Airport Freezone, K19  
P.O.Box: 95703 Dubai, UAE  
T: +971 4 299 0886  
F: +971 4 299 0687  
infopid@getgroup.com



**Céline Gouveia**  
International Sales Director - Government Programs

104, avenue du Président Kennedy - 75016 Paris - France  
T +33 (0)1 40 58 30 26  
M +33 (0)6 15 71 03 43  
celine.gouveia@imprimerienationale.fr

**LOCAL NATIONAL GLOBAL**  
**SOLUTIONS FOR A SECURE SOCIETY**  
YOUR SECURITY. CONNECTED  
Visit us at [hidglobal.com/border-protection](http://hidglobal.com/border-protection)



**HOLLISTON™** MOST DURABLE CLOTH  
COVERS in the WORLD

*Setting the Security Standard for Over a Century*

William Waldron  
VP Security sales

001-423-256-6009 Direct  
001-423-367-7979 Mobile  
bwaldron@holiston.com  
www.holliston.com



**Bart Crols**  
Managing Director

+31 6 11 32 06 94  
bart.crols@iai.nl



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



Free Trial  
documentchecker.com



**Solutions for checking ID documents**  
Over 6,000 organisations around the world rely on our solutions  
Every day  
[www.keesingtechnologies.com](http://www.keesingtechnologies.com)

## Tomáš Antolík

Business Development Manager

+421 2 2071 4056 +421 911 392 562

tomas.antolik5

tomas.antolik@innovatrics.com

Pri vinohradoch 82, 831 06 Bratislava, Slovakia

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

**innovatrics**  
YOUR BIOMETRIC PARTNER

## Michele Myers

Business Development Manager

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

Toll Free (866) 617-4675

Direct (484) 696-1372

Cell (484) 680-4253

Fax (610) 873-9105

Email [michele.myers@inspectron.com](mailto:michele.myers@inspectron.com)

## Inspectron

ENSURING DOCUMENT INTEGRITY

### Corporate Office

Inspectron

187 Billerica Road

Chelmsford, MA 01824 [USA]

### Administration Support

(978) 256-6444

## SECURE PASSPORT SOLUTIONS

Tél. +41 21 345 7000

Fax. +41 21 345 7010

[info@kba-notasys.com](mailto:info@kba-notasys.com)

### KBA-NotaSys SA

Avenue du Grey 55, CH-1018 Lausanne

PO Box 347, CH-1000 Lausanne 22

Switzerland



Identity Management &  
Authorization Solutions

**MT. AIREY GROUP, INC.**

4300 Tartan Oak Ct.

Fairfax, VA 22032

**Paul Townsend, CISSP**

Director of Cybersecurity

(O) +1.240.285.9596

(M) +1.301.908.0293

(F) +1.240.255.4883

[ptownsend@mountaireygroup.com](mailto:ptownsend@mountaireygroup.com)

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



YOUR TURNKEY SOLUTION PROVIDER  
TO REALIZE GOVERNMENT ID PROJECTS

### Mühlbauer Inc.

Ms. Heike Davis, Vice President

226 Pickett's Line

Newport News, VA 23603-1366, USA

Phone: +1 757 947 2823

Mobile: +1 757 876 6070

Fax: +1 757 947 2930

Mail: [heike.davis@muhlbauer.com](mailto:heike.davis@muhlbauer.com)

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



Your Complete Hardware and Software  
Solution for Secure Government ID

Please visit the NBS Booth (#24) to learn  
more about our Government ID Solutions.

NBS Technologies Inc.  
703 Evans Avenue, Suite 402  
Toronto, ON M9C 5E9  
(416) 621-1911  
[info@nbstech.com](mailto:info@nbstech.com)



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



### Stefan Barbu

Head of Secure ID Americas

NXP Semiconductors

Mob: +1 408 893 7509

1455 Pennsylvania Avenue NW, Suite 400, Washington DC, 20004

[stefan.barbu@nxp.com](mailto:stefan.barbu@nxp.com), [www.nxp.com](http://www.nxp.com)

Our world is now a world of permanent, uninterrupted connections. In one way or another objects, machines and people are now connected to a digital networks for work, leisure, travel, or shopping. Oberthur Technologies' (OT) mission is to provide responses to all these situations by guarantee a stress-free experience each time you connect, authenticate or pay.

Contact us:  
<http://www.oberthur.com/contact-us/>

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



## LASINK

A new generation solution for totally safe portrait personalization and extremely resilient documents against aging and fraudsters attacks



Come and meet us at our  
booth #47

## SAFE, RELIABLE, MODERN DOCUMENTS AND BANKNOTES

[www.pwpw.pl](http://www.pwpw.pl)  
[sale@pwpw.pl](mailto:sale@pwpw.pl)  
+48 22 235 2000

PWPW  
1 Sanguszki, 00-22 Warsaw  
Poland



forensic science systems

### REGULA Ltd.

Phone: +375 17 286 28 25 Fax: +375 17 213 68 97

1-314 Volokha Street, Minsk, 220036, Belarus

[mail@regula.by](mailto:mail@regula.by)

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

IDENTITY & SECURITY

**SAFER, EASIER TRAVEL**

@SafranIDSec  
info@morpho.com  
www.safran-identity-security.com




**Oliver Jahnke**

Sales Director EMEAA  
Homeland Security Division

secunet Security Networks AG  
Osterbekstr. 90 b, 22083 Hamburg  
Germany

+49 201 5454-3716  
+49 201 5454-1326  
+49 151 23060256  
oliver.jahnke@secunet.com  
www.secunet.com



**SEMLEX**  
GROUP

Biometric security for identity  
and travel documents

SEMLEX EUROPE S.A.  
Avenue Brugmann, 384  
1180 Brussels, Belgium

europa@semlex.com  
www.semlex.com

T. +32 2 346 80 19  
F. +32 2 346 80 29



**Dr Catherine Fankhauser**  
Sales Director ISS - Identity Security Solutions  
Identity & Document Security Solutions

Security Inks Solutions

Direct +41 21 627 59 56  
Mobile +41 78 817 34 96  
catherine.fankhauser@sicpa.com

SICPA SA  
Av. de Florissant 41, 1008 Prilly, Switzerland  
PO Box, CH - 1000 Lausanne 16  
Tel. +41 21 627 55 55 Fax +41 21 627 57 27  
www.sicpa.com

**Nils Ågren**  
VP, Business & Product Development

+46 (0) 733 11 2097  
nils.agren@speed-identity.com

**SPEED IDENTITY**

**SURYS** From science to confidence

contact@surys.com  
T +33 1 64 76 31 00

Parc d'activités Gustave Eiffel - 22 avenue de l'Europe  
Bussy-St-Georges - 77607 Marne-la-Vallée Cedex 3 - France  
www.surys.com  
www.blog.surys.com



SMART SEARCH & MATCH

**Tarvinder S. Sembhi**  
VP Sales Identity Market

Office +1 888 922 9224  
Mobile +1 856 261 8639  
tsembhi@wcc-group.com

TRUSTED IDENTITIES | SECURE TRANSACTIONS

Connecting Citizens & Governments  
1187 Park Place, Shakopee, MN  
888-690-2424  
info@entrustdatacard.com  
entrustdatacard.com



CELEBRATING **10 YEARS** In Digital Identity Documents and Smart Cards Software Solutions



secure identity and payments

E: info@x-infotech.com T: +371 67930171  
W: www.x-infotech.com F: +371 67930172



simone foini  
sales & marketing director

e-mail: simone.foini@centrograficodg.it  
mobile: +39 335 5780412

via einstein, 76  
20010 marcallo (mi) italy  
tel. +39 02 9761301 - fax +39 02 9761953  
sales department:  
tel. +39 02 97950932 - fax +39 02 9760080  
e-mail: info@centrograficodg.it  
www.centrograficodg.it

# MUEHLBAUER TECURITY®

COMPREHENSIVE GOVERNMENT SOLUTIONS



- 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**





**The officer's  
best friend  
goes mobile.**

The **KINEGRAM®** DIGITAL SEAL integrates the secure physical credential with mobile ID processes. Learn more on [kinegram.com/digitalseal](http://kinegram.com/digitalseal)

For banknotes: LEONHARD KURZ Stiftung & Co. KG  
Schwabacher Straße 482 | D-90763 Fuerth | Germany | [banknote.security@kurz.de](mailto:banknote.security@kurz.de)

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

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



**KINEGRAM®**