NEWS AND FEATURES ON THE ICAO TRAVELLER IDENTIFICATION PROGRAMME - VOL. 13 - NO. 1

ICAO TRIP

MAKING BORDERS MORE SECURE

IN THIS ISSUE

- CAN BIOMETRIC SYSTEMS BE CHEAP AND SIMPLE?
- DIGITAL TRAVEL CREDENTIALS: LOOKING BEYOND THE BOOK
- IMPROVING FRONTLINE DOCUMENT CHECKS
- GLOBAL BORDERS WITH A KNOWN TRAVELLER CONCEPT

ICAO

SECURITY & FACILITATION

TRIP2019

ICAO TRIP

Regional Seminar Cotonou

Benin, 12 to 14 February 2019

ICAO Traveller Identification Programme (TRIP) Regional Seminar will take place from 12 to 14 February 2019 in Cotonou, Benin.

The Seminar, hosted by the Government of Benin, 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. The event will provide an opportunity for enhancing international and regional cooperation and collaboration that addresses the threats faced by international civil aviation. This will be accomplished by promoting the global framework established by Annex 9 – Facilitation to the Convention on International Civil Aviation. Accordingly, a special focus of the Seminar will highlight border integrity and border control management challenges, such as Advanced Passenger Information (API) system implementation.

This ICAO TRIP Regional Seminar provides a unique opportunity to exchange information and enhance expertise and would be of benefit to passport issuing offices, aviation security authorities, civil registries, border control and law enforcement authorities, as well as to airline companies, airport authorities, and other interested parties.

ICAO SECURITY & FACILITATION

Information for online registration is available on the Seminar website at:
www.icao.int/Meetings/TRIP-Benin-2019

Participants are invited to register online before 11 January 2019.

CONTENTS

ICAO TRIP MAGAZINE
VOLUME 13, NUMBER 1, 2018

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

Coordinators:
Anthony Frederick
Garleen McGann
Tel: +1 (514) 954-8219 ext. 6991
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
Graphic Designer: June Kim
Tel: +1 (514) 954-8219 ext. 7168
E-mail: jukim@icao.int

ADVERTISING

Advertising Representative: Caroline Casabon
Tel: +1 (514) 954-8219, ext. 6466
Fax: +1 (514) 954 6769
E-mail: ccasabon@icao.int

SUBMISSIONS

The ICAO 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

Printed by ICAO

ICAO

www.icao.int

TECHNICAL ADVISORY GROUP ON THE TRAVELLER IDENTIFICATION PROGRAMME (TAG/TRIP)

Member States

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

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 Coordinating 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 Co-operation in 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 Economic Forum (WEF)

World Tourism Organization (UNWTO)

SECURING BORDER INTEGRITY

Dr. Narjess Abdennebi
Chef, Facilitation Section
Air Transport Bureau
International Civil Aviation Organization

ICAO's Traveller Identification Programme (ICAO TRIP) Strategy has been a key pillar in ICAO's Security and Facilitation Strategic Objective since it was first endorsed by the 38th Session of the ICAO Assembly in 2013. Three years later, during the 39th Session of the ICAO Assembly, ICAO TRIP Strategy priorities were further endorsed when the Assembly identified the need for national coordination and international cooperation to ensure the security and integrity of traveller identification and border control programmes. Under the ICAO TRIP Strategy programme, ICAO continues to focus on ensuring traveller identification follows a holistic and coordinated approach, from document issuance to border control systems.

The ICAO TRIP Strategy-related legal framework was enhanced through Amendment 26 to Annex 9 – *Facilitation* to the Convention on International Civil Aviation. Sixty-four Standards and Recommended Practices (SARPs) relate to the ICAO TRIP Strategy in the 15th edition of Annex 9, as compared to forty-eight in the previous edition. The new SARPs became applicable in February 2018. Notably, a Standard obliging Member States to establish an Advance Passenger Information (API) System, pursuant to United Nations (UN) Security Council resolution 2178 (2014). With the increasing use of API for border security and counter terrorism, ICAO has intensified its efforts to provide assistance to States in implementing API and interactive API (iAPI) systems and related Annex 9 SARPs. This supports the wider UN action plan to achieve important milestones on border control management improvements.

Through the project "*Strengthening Border Control Management in the Caribbean Region*", which was funded by Canada, ICAO developed the ICAO TRIP *Guide on Border Control Management (BCM)*. The Guide serves as a reference for States so that they can optimize the use of inspection systems and tools and interoperable applications that are available, to enhance their national BCM. This guide is available for download: *https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx*

Rapid changes in technology present opportunities for leveraging new technologies that enhance both travel facilitation and security at border control points. In this context, ICAO's New Technology Working Group is assessing inter alia, the feasibility and benefits of using digital representation of the ePassport in travel through a Digital Travel Credential (DTC). DTCs are meant to temporarily, or even permanently, substitute a conventional passport with a digital representation of the traveller's identity.

Biometrics technologies have considerable potential to further facilitation and security objectives, but effectively using them in the implementation of the ICAO TRIP Strategy around the world has its challenges. After empirical evidence, based on ICAO's Implementation and Capacity Building Working Group (ICBWG) consultations with State agencies, pointed to some misconceptions on the strengths and weaknesses of biometric applications, the ICBWG began working on the development of high-level guidance material related to the scope of the ICAO TRIP Strategy.

As this publication went to print, we were in final preparations for the 14th ICAO Symposium and Exhibition on the Traveller Identification Programme that will take place at ICAO Headquarters from 23 to 25 October 2018. The Symposium provides opportunities for enhancing international cooperation and collaboration to address the threats faced by international civil aviation. The theme of this year's event will highlight *How to Use Traveller ID for Streamlined Border Controls*, and will include an interactive session on API systems. We hope we will see you there!

We always welcome feedback and suggestions for articles and themes for future issues of the ICAO TRIP Magazine. Send your contributions and comments to *ICAOTRIPmagazine@icao.int.*

DIGITAL TRAVEL CREDENTIALS: LOOKING BEYOND THE BOOK

Travellers' behaviours and expectations are changing. In our ever-increasing world of digital transactions, it is hard to imagine a future where we will still need to present a traditional, physical passport in order to cross a border. Increasing international traffic volumes are placing pressure on airport passenger facilitation, and the need for secure and trusted traveller identification remains ever present in the face of global turmoil. How can border authorities and the airline industry adapt to meet the changing needs, and manage traveller facilitation without compromising security, all while maintaining interoperability?

Taking these challenges into consideration, ICAO's New Technologies Working Group (NTWG) established a specialized sub group to begin work on standardizing a digital travel credential (DTC). In developing these technical specifications and policies, the ePassport is used as the benchmark given that it offers a secure, portable, verifiable and unclonable token.

OPPORTUNITY FOR CHANGE IN THE TRAVEL CONTINUUM

An estimated 139 States have issued more than one billion ePassports to date. The growing number of ePassports improve the travel network by enhancing facilitation for travellers. They also improve security for border management. One particular advantage of the ePassport that has the potential to revolutionize the way travellers are processed, is the digitization of the traveller's biographic and biometric data that is stored in an integrated circuit (IC or chip) embedded in the book.

This chip data has already generated many benefits. Not only does it verify of the passport bearer's identity through facial recognition, it has provided authorities with the tools to authenticate the travel document. While these processes have made significant contributions to the security and facilitation of traveller movements, the ePassport has yet to be fully leveraged to provide all of the possible benefits to change the way travellers clear checkpoints during departure and arrival.

The DTC envisioned by the NTWG uses the technology available in the ePassport to create a credential that can bring these additional benefits, while maintaining a balance between security and facilitation.

LEVERAGING THE KEY ATTRIBUTES

For a DTC to be effective and practical it needs to maintain the key attributes already contained in the ePassport, namely:

- verifying entities must be able to authenticate the credentials supplied;
- inclusion of a means to protect against cloning;
- capable to accept and store pertinent holder and/or travel data;
- protection of the privacy of the user; and
- verification processes must be at least as secure as for ePassports.

A DTC essentially serves the same functions as an ePassport in reliably confirming the identity of the traveller. Additional benefits to those in the travel continuum include:

- An improvement to passenger flows by allowing travellers to provide their data in advance and engage in more self-service;
- The ability for airports and airlines to link additional data, such as a boarding pass, to the DTC; and
- Advance provision of passenger data to aviation stakeholders to support biometric matching through controlled checkpoints, to facilitate biometric boarding and assist in improving pre-arrival security and/or risk assessment.

In order for these benefits to be realized, wide acceptability of globally-interoperable features, and an issuers ability to control the credential, are paramount.

THE CHALLENGE OF BALANCE

Creating a secure and reliable form of electronic identification that can be used to enhance facilitation is perhaps the simpler part of this work. Not only are there a number of established and emerging e-Identity schemes around the world, but airports and airlines have an increasing number of stand-alone traveller facilitation schemes. These solutions all leverage off a range of differing technologies and use a variety of form factors. What is important for travel is that there is a balance in security, facilitation, and interoperability.

While considering this, the sub group examined and considered a range of technologies, or 'form factors', such as smart devices, closed servers, remote servers, and distributed ledgers. The form factors were evaluated against these four basic criteria to ensure the credential could be:

1. Produced from a Travel Document Issuing Authority.
2. Capable of being provided unaltered to verifying entities in advance of the traveller's journey or arrival.
3. Globally interoperable to ensure that it could be used in different environments.
4. Adopted by travellers. This requires creating trust that:
   - › The DTC is as, or more secure, than an ePassport, and
   - › Biographic and biometric data will be handled in a manner ensuring the protection of the traveller's personal data and privacy.

Each form factor considered had a number of positives, but each also presented limitations that would result in a solution less secure than an ePassport. While these different form factors would mostly work well for facilitation, few would be globally interoperable, and all would present security concerns that would be unacceptable for most, if not all, border authorities.

However all is not lost! By combining one or more of the form factors with the existing technology already available in the ePassport, there is an opportunity to create a hybrid credential that would meet all the basic criteria and key attributes, and bring the additional benefits without losing the balance between security, facilitation, and interoperability.

THE PREFERRED SOLUTION – A HYBRID DTC

A hybrid credential is a combination of a virtual token (credential) that is linked to one or more physical tokens (authenticators). The credential could be stored in a remote system, such as a database or webserver, and the authenticator could be an ePassport, smart card, or mobile phone. This combines the virtual and the physical in a way that merges the advantages of both approaches, while minimizing the disadvantages.

When defining options for the issuance of these tokens, the sub-group determined that the virtual credentials would have

to include many of the same security elements of the current ePassport, including authentication, when required by inspection authorities.

Authentication currently takes place when the chip in the ePassport is electronically validated by the border authority – a simple electronic check that ensures the ePassport is authentic. This check verifies the digital signature in the chip and that the digital certificate was used by a bonafide authority when the data in the chip was sealed. It confirms that the biographic and biometric data endorsed in the document when it was issued has not been altered. The authority can then confidently rely on the information in the chip to compare against the information printed in the physical passport book, and if need be, against the traveller themselves.

So how can a hybrid credential match this level of confidence?

By linking the virtual travel credential to one or more physical tokens, it enables the verifying entity, such as a border agent, to perform additional active authentication of the credential when required for increased security. The physical token can be used to retrieve the data from the remote system by authenticating the holder of the virtual credential to that system.

This model is preferred by the ICAO NTWG because the credential is already securely linked to the Issuing Authority. The physical token allows the verifier to select the correct virtual credential which was potentially provided in advance. It also provides the verifying entity the flexibility to decide whether the virtual credential is sufficient, or the physical token, the authenticator, is additionally required. Or, put simply, whether the traveller can pass through controlled checkpoints without having to physically present their passport.

One of the advantages in the DTC is that it provides several options for creation and form, without losing the benefits of interoperability. The DTC itself could be derived from an existing ePassport by the holder of that ePassport. Or the issuing authority could create the DTC and has the option to store the virtual component on a remote system or securely on a smart device.

When booking or checking in, travellers could send their virtual component in advance to the border authority, in an electronic system for travel authorization (ESTA) process or using API/PNR etc. When they arrive at the airport, they could use their token, whether it is a physical token such as their phone, or purely virtual token, such as their facial biometric, to pass through the different check points in the airport journey.

If not sent in advance, then the virtual component must be able to be read in a standardized method using passive authentication.

ON TRACK FOR 2020

Development of technical specifications, proof of concept and testing methodologies for the Hybrid DTC are underway. The Working Group continues to work towards resolving policy issues, such as issuance, revocation and inclusion of additional travel data. Their aim is to have the DTC technical specifications presented for endorsement by the ICAO TAG/TRIP in 2020. T

LOUISE COLE
Manager Information Partnerships,
Department of Internal Affairs,
New Zealand Department of
Internal Affairs (DIA)

WILLIAMS
NICOLE ANNE
10/10/85
UTO
FEMALE
DC186585
UTO
01/05/20

INTERPOL AND FRONTEX COLLABORATE TO IMPROVE FRONTLINE DOCUMENT CHECKS

THE CHALLENGE

Around the world, the number of travel documents issued by different States grows every day. New types of travel documents are continuously issued as States react to the pressures to make these documents even more secure, incorporating the latest developments of the document security industry. But even as new security features are being developed and used, there are new trends and modus operandi of document fraud that are evolving quickly.

Verifying travel documents is one of the main challenges for border guards and police officers and it is pivotal during first-line border control inspections. This underlines the importance of frontline document and database checks at international borders.

It is worth noting that frontline border control activities are conducted in extremely complex environments. Police officers and border guards are required to operate under tight time constraints (rapid passenger control) and to be familiar with a growing number of new types of travel and identity documents.

Criminals are aware of these constraints and exploit weaknesses in the system to cross borders with the purpose of committing further illegal activities.

THE VISION

Frontex, the European Border and Coast Guard Agency, and INTERPOL are committed to fighting document fraud. The mission of both organizations includes supporting police and border guards in effective border control.

The FIELDS (Frontex INTERPOL Electronic Library Document System) project aims to support border guards and police officers in authenticating travel and identity documents by giving them access to visual information on the key detection points of inspected documents, in the framework of their national systems.

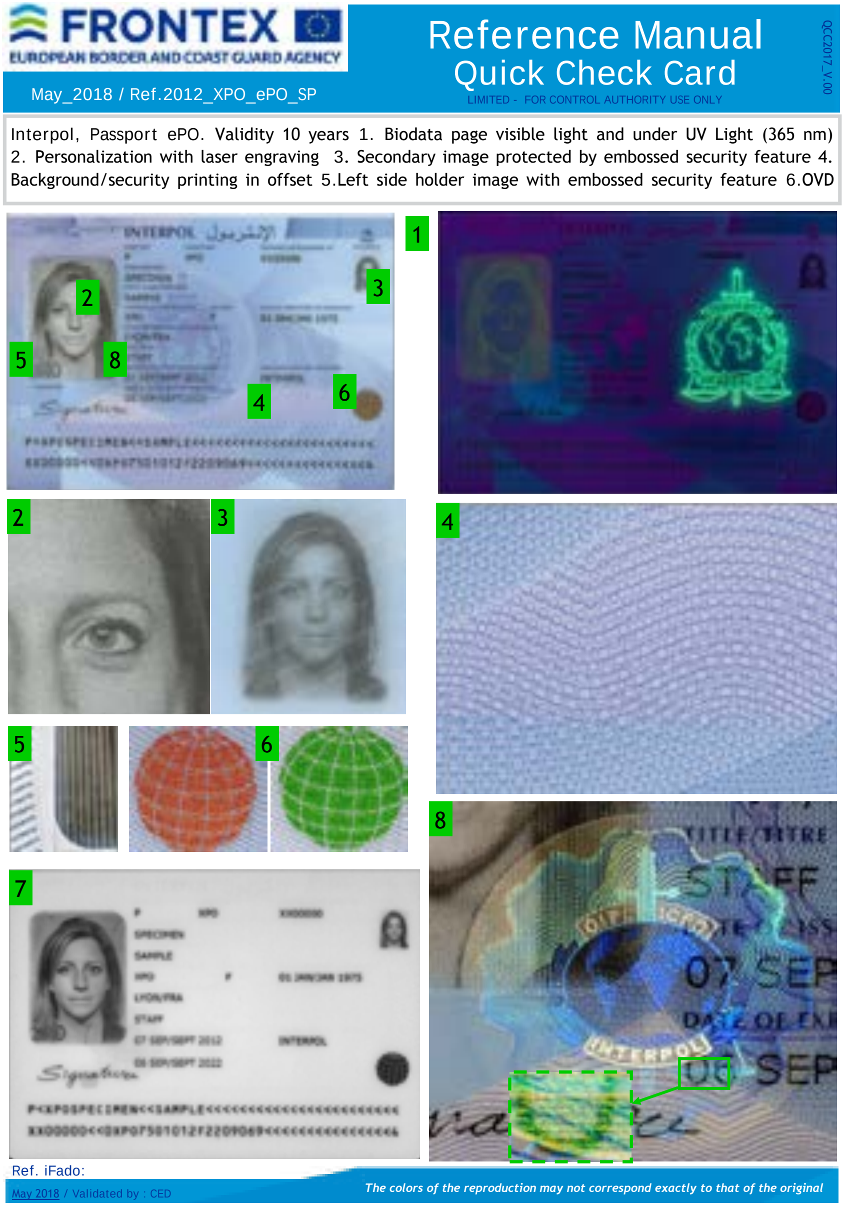
Officers conducting first-line border checks have only seconds to verify the authenticity of a document and assess whether it is genuine or potentially fake. Knowing which key markers to check on a travel or identity document can ultimately help improve border and international security.

The project is intended to complement existing national examination processes and systems, including those equipped with automated document scanning technologies.

AN EFFICIENT TOOL FOR BORDER GUARDS AND POLICE OFFICERS

Expanding upon their respective Dial-Doc (Digital INTERPOL Alert Library – Documents) and Quick Check Cards initiatives, INTERPOL and Frontex are partnering to further enhance the ability of police and border officers to authenticate travel and identity documents at national borders.

Frontex recently developed a new product called Quick Check Cards (QCCs). The aim of this tool is to assist first-line border guards to quickly identify key document features that indicate potential fraud. It helps ensure that suspect documents are spotted and referred to secondary processing for closer examination, while rightful holders of authentic documents are not exposed to unnecessarily thorough inspections.



FRONTEX EUROPEAN BORDER AND COAST GUARD AGENCY

Reference Manual Quick Check Card

LIMITED - FOR CONTROL AUTHORITY USE ONLY

May_2018 / Ref.2012_XPO_ePO_SP

QCC2017_V.00

Interpol, Passport ePO. Validity 10 years 1. Biodata page visible light and under UV Light (365 nm) 2. Personalization with laser engraving 3. Secondary image protected by embossed security feature 4. Background/security printing in offset 5.Left side holder image with embossed security feature 6.OVD

Ref. iFado:

May 2018 / Validated by : CED

The colors of the reproduction may not correspond exactly to that of the original

The QCCs are a decision-aid for law enforcement officers during travel document authenticity verification 'at first encounter', concisely presenting the most relevant information on the inspected document. The tool specifically focuses on key detection points that are selected on the basis of the specific security features of the inspected document, as well as the known, recent and most relevant forgery trends.

Frontex has also recently established its Expert Group on Document Control (EXP-DOC). The working group is composed of nominated technical specialists and operational document experts from Schengen Member States. To ensure the highest quality of the product, Frontex relies on the working group when developing and creating QCCs. This unique initiative takes the knowledge of several highly professional document experts from numerous Member States, to build one, simple-to-use product that is designed for frontline officers.

INTERPOL's Dial-Doc is a tool containing 'alerts' and information on recently detected counterfeit documents. It is designed to assist border guards and other law enforcement officers during second-line document checks in the identification of document fraud.

Project FIELDS will bring together and enhance the existing Dial-Doc platform to make the Frontex Quick Check Cards available to frontline border control officers via INTERPOL's I-24/7 secure global police communications system.

National authorities will be able to benefit from this new system using their existing infrastructure and connectivity to INTERPOL.

PROJECT IMPLEMENTATION

INTERPOL and Frontex are currently working to determine the requirements and the technical and functional specifications of the proposed system. An interagency steering committee is leading the project to ensure it is technically feasible and will add value to the participating States and their citizens by contributing to border and international security.

Technical and operational experts from a small pilot group of States are assisting in the development of the project, to make sure the system can be integrated with national IT infrastructures and will meet the daily needs of officers on the ground. The 18-month planning and analysis phase is expected to conclude in early 2019, after which the technical upgrades to the Dial-Doc system will be implemented based on the approved design within one year.

HOW WILL THE NEW SYSTEM WORK?

Based on the specific identifier of the inspected document, a request will automatically be sent to INTERPOL to ascertain if a QCC corresponding to the inspected document, is available in the Dial-Doc database.

Border guards and police officers using mobile equipment will also be able to connect to Dial-Doc directly from their national applications, and to consult QCCs when checking the authenticity of inspected travel and/or ID documents during frontline policing. The envisaged Dial-Doc system will be made available to any national law enforcement authority upon a national decision.

BENEFITS FOR PUBLIC SECURITY

Having effective control of travel and identity documents is an important cornerstone of border security and successful migration management. It is also an inevitable tool in the fight against terrorism and organized crime, significantly contributing to global security.

The real-time availability of the Frontex Quick Check Cards at frontline border checks will increase effectiveness in verifying the authenticity of travel and identity documents at border checks, contributing to the security of EU and partner countries.

INTERPOL, through its global I-24/7 network, already provides real-time information on the validity of travel documents through its Stolen and Lost Travel Documents (SLTD) database that contains records on lost, revoked, invalid, and stolen blank documents. Once the envisaged system is implemented, the enhanced Dial-Doc will become an additional tool to enhance document border control, covering other elements of document fraud, such as counterfeits and forgeries not currently recorded in SLTD.

Member States will be able to take advantage of the opportunities for streamlining first-line border control systems through the integration of the new INTERPOL-Frontex solution within

> *"...effective control of travel and identity documents is an important cornerstone of border security and successful migration management. It is also an inevitable tool in the fight against terrorism and organized crime..."*

existing national border management and police systems. The use of ad-hoc technologies will ensure maximum flexibility and customization.

The envisaged system may be made available to any law enforcement officer in any INTERPOL Member State, but access and implementation will remain under the sovereignty of the individual States after the project has been finalized. At the same time, in line with national information sharing policies, a thorough restriction system will be implemented to allow each State using the system to decide with whom it will share any information uploaded to the system.

Finally, through this project, INTERPOL and Frontex together aim to leverage and expand international cooperation between border control and law enforcement authorities to raise awareness of and tackle the global challenges posed by document fraud.

FABRIZIO di CARLO
Specialized Officer, Forensic and Police Data Management, sub-Directorate, INTERPOL

SZABOLES HORVATH
Team leader, Centre of Excellence for Combating Document Fraud, Frontex

BIOMETRIC SYSTEMS: CAN THEY BE CHEAP AND SIMPLE?

INTRODUCTION

Thinking about installing or improving a biometric system for traveller identification? You may feel pressured to buy something that's expensive, complex and large in scope.

Based on Australia's experience with issuing passports, you may not need a system like that. We're sharing what we've learned in recent years about putting together simple, effective biometric controls that don't break the national treasury.

Every identity authority's circumstances are different. Nobody would want, or would be able to replicate our solution in full. But the principles behind our approach, and many specific elements, may give you something to think about. Though we deal with facial biometrics, the concepts apply equally to iris and fingerprints.

OUR STARTING POINT

Every year, Australia's Department of Foreign Affairs and Trade processes two million travel document applications. Slightly more than half come from the 14 million Australians who need to renew the passport they already have. We archive the biometric facial image from every application. Our image repository has 27 million biometric images, a figure that grows by more than 8,000 every business day.

We were one of the first passport authorities, and one of the first government agencies anywhere, to integrate biometrics into our identity management. That was in 2004. Back then, it wasn't possible to purchase whole biometric systems, so we developed our own system in-house.

We built our biometric system into our passport processing software (called Delta), and coupled it to Delta's workflow engine. It functioned very well. But because it was so deeply embedded in Delta, it was not adaptable.

When we recently developed completely new processing software (Atlas), we were unable to simply take Delta's biometric system and transplant it.

We needed a new biometric system. And we needed it to not just process new passports, but to also verify existing passports for other agencies. This way we could participate in the nationwide biometric identity-matching arrangements that Australia's federal, state and territory governments launched in 2017.

WHAT WE DIDN'T DO

Hype about biometrics, and the fear of missing out on the benefits, can tempt senior managers into seeing biometric systems as a solution to all kinds of identity risks. This opens the door for vendors to oversell the capability of their biometric products, or to bundle them with business rules engines, identity repositories, middleware layers and other add-ons.

Bundling can leave organizations with opaque 'black box' systems they do not fully understand, that foster excessive dependence on the vendor, and that are more likely than simple systems to fail. While black boxes are good for vendors, they add complexity, cost and maintenance overheads that organizations don't generally need. Often, black boxes don't optimize the business value of the personal information the organizations have collected.

HOW WE AVOIDED THIS

We made decisions about our new biometric system with a hard-headed understanding of what we would not need it to do.

- It would not need to include an identity repository. Sitting behind our processing software, we already had a robust non-biometric database that linked identity elements (names, addresses and so on) to application form numbers and the passport numbers of completed travel documents. This ensured that every client only had a single identity record.
- Our new biometric system would not need a business rules engine. Through Delta and Atlas, we already had, like most passport issuers around the world, an IT workflow that followed defined business rules for handling applications logically.
- Our Atlas software was going to have a thin-client interface that presented

biographic and biometric information to passport processing officers on a single screen. Our new biometric system would need to service this interface but not integrate with it.

We boiled down what we would need to three core functions.

- **1:n (Identification)** – comparing a supplied image to multiple images in our records to detect identity fraud and identify unknown persons for identity-matching purposes. Identification answers the questions, 'do we know this applicant under another identity' and 'do we know this person at all'?
- **1:1 (Verification)** – comparing a single image in our records to the supplied image of someone who purports to be that person. Verification confirms that a renewal client is using the same identity as in previous applications or that a person interacting with government in other contexts is who they claim to be.
- **QA (Image Quality Assurance)** – determining whether a facial image is good enough to be used for Identification or Verification.

We did not build a single big application to perform these three functions. Instead, for simplicity and flexibility, we developed a set of three separate services.

HOW IT WORKS

The Image Quality Assurance (QA) service accepts a single facial image and returns a list of quality attributes. Which internal system calls the service isn't important, it could be our Delta or Atlas passport processing software, an identity-matching software or a future software not yet conceived. The service will return the same list regardless. The workflow engine in the software that calls the service decides whether the attributes in the list signify an image quality high enough to attempt a match using the other two services.

The Verification service takes two facial images as an input and returns a match score, a figure between 0 and 1 indicates the likelihood of a match between the two images. The workflow engine in the software that calls the service, decides whether the score constitutes a match, and what to do with it next.

The Identification service takes a single facial image and returns a list of the top 200 possible matches. The list includes only the identity record number and match score, for each result. The workflow engine in the software that calls the service decides what to do with the information.

This approach has a number of benefits.

- The services proved relatively simple and quick to build.
- Keeping them discrete from other software means we can make them highly available at a lower cost than what would otherwise be the case.

- The services can be called by any of our business processes, not just passport application processing software.
- Each service can be upgraded or replaced separately, with no impact on the other two services, and with no effect on business processes as long as the new service returns outputs within the same range.
- The outputs are simple and known, so developing new business processes that use them, is straight forward.
- New approaches to facial comparison, such as using multiple matching engines, can easily be implemented behind the service interface.

BIGGER IS NOT ALWAYS BETTER

With the new system came a new line of thinking about the identification service. Until recently, our policy had been to enrol every facial image in our archive into the database of our biometric system. This posed two challenges.

- 1:n Identification engines are expensive, and licencing is based on the number of templates enrolled.
- Extensive research has shown that as the size of the database increases, the matching effectiveness decreases.

We have therefore decided to rationalize the number of templates we enrol. Because facial images of young children and outdated images of adults are of little value for identification, in the future we will only enrol the images of children above a certain age, and the most recent image of other clients.

These policies will reduce the size of the database from 27 million to around 13 million. This will bring a significant saving in licence and maintenance fees, and a corresponding increase in matching effectiveness. Images not enrolled in the database will be retained in the archive, from where we will be able to access them manually if we need to.

THE BOTTOM LINE

The project took 12 months to complete at a cost of just AUD 2 million (USD1.477 million). This kind of inexpensive outcome is not typical, but then neither was our approach.

In deciding on a biometric system, the most important factor is a clear-eyed understanding of what you do and don't need. Every biometric system uses commercial components, such as algorithms and service interfaces. The key is to buy only what you require, to make the technology work for you rather than the other way around, and to deal with vendors from a position where you, not they, are setting the agenda. T

STEPHEN GEE
Australia's TAG-TRIP Member and
Assistant Secretary in
Department of Foreign Affairs and Trade
of Australia

GLOBAL BORDERS WITH A KNOWN TRAVELLER CONCEPT

In January 2018 the World Economic Forum introduced its Known Traveller Digital Identity (KTDI) concept, an initiative co-designed by public and private sector partners that seeks to anticipate the challenges, and take advantage of the immense opportunities that emerging technologies will present, in the cross-border movement of people. The KTDI concept seeks to address the changing behaviours and expectations of travellers, the growing global traveller volumes, and the rise in geopolitical insecurity. As a traveller-centric system, the KTDI concept would provide authorities and security officials with early, reliable and verified information prior to individuals arriving at the border. In doing so, the KTDI concept would better enable risk-based traveller differentiation and facilitation, providing authorities with added time and resources to detect and address risks and threats.

The World Economic Forum (the "Forum") is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas. The Forum is organized into fourteen System Initiatives, each of which is designed to stimulate a more effective public-private response to a complex global issue, in order to improve the state of the world. Systems leadership works by cultivating a shared vision for change, empowering widespread innovation and action, and enabling mutual accountability.

The Forum's System Initiative on the Future of Mobility connects stakeholders within and across industries and regions to effectively combine expertise and resources to deliver positive change in the safe, clean and inclusive movement of goods and people. The Forum is fortunate that ICAO's Secretary General, Dr. Fang Liu, serves as a member of the Board of Stewards on this System Initiative, which has enabled increasing collaboration between the two organizations.

LEARNING FROM TRUSTED -TRAVELLER PROGRAMMES

Research undertaken in 2016 and 2017 by the Forum in collaboration with the International Criminal Police Organization (INTERPOL), and interviews with leaders of the most advanced trusted-traveller and registered-traveller programmes, revealed the impediments to scaling such programmes geographically, and reaching more travellers. These impediments limit the potential to pre-screen and pre-clear larger numbers of low-risk travellers.

Among the challenges identified were the expensive and human resource-intensive nature of trusted-traveller programme implementation, the lack of trust between participating countries – which results in the duplication of vetting processes – and the low rates of adoption due to the cost and onerous nature of the application process. As such, governments have a limited ability to reduce bottlenecks in screening and border management. Where registered traveller programmes, rather than trusted-traveller programmes, have been adopted to improve uptake and implementation, initial vetting remains dependent on legacy systems whereby risk-levels are based on the country of origin.

Undertaking risk assessment based purely on biographic data, such as nationality, can be ineffective since high-risk travellers from countries deemed 'safe' may be overlooked. Furthermore, this approach could risk being discriminatory, in that trustworthy travellers may be subjected to excessive screening if they come from countries deemed 'high-risk'.

THE KNOWN TRAVELLER DIGITAL IDENTITY CONCEPT

At its core, the KTDI concept promotes a risk-based, data-driven approach to traveller screening and border security. The concept is founded on the principle that individual travellers have control over the use of their own identities and their components. It empowers travellers to become active partners in the security process by choosing to share their data with security and border screening officials, as well as private sector entities, in advance of travel. Through the advance sharing of identity information, the KTDI concept equips government and private sector entities with traveller information that would improve decision-making and risk assessment related to authorizing travel and border crossing.

USER-CENTRICITY

The KTDI concept puts the individual traveller in control of the specific identity information (such as biometric, biographic and travel history data) provided to governmental and private-sector players along the journey, for the purpose of risk-assessment, verification and access. The traveller can select which information is shared and for how long, in accordance with the requirements of the authority or private entity from which he/she is seeking access to services. His/her identity is authenticated through biometric verification, and profile information is protected by distributed ledger technology and cryptography. By self-selecting the sharing of their digital identities, not only will travellers be integral in the security process, but they will experience the reward of more personalized and seamless journeys.

ADVANCED PASSENGER SCREENING

When travellers push proof of their identity information to governmental authorities throughout their journey, they will build trust in their digital profile, which will, over time, create facilitation opportunities. The access by authorities to verified personal biometric, biographic and travel history data enables entities to undertake advanced risk assessment of the traveller based on verified identity information and provide seamless access through biometric recognition technology, which will also further ease traveller facilitation. For travellers who are deemed low risk, this could result in a more efficient and seamless pre-boarding screening process.

For receiving organizations and entities, the validated identity proof of the KTDI concept offers the advantage of knowing in advance those they will be interacting with. By having this information provided in advance, organization-specific processes can be executed more efficiently and effectively. Also, both public and private entities will be able to offer more custom-made services with more direct benefits for the traveller.

PROOF OF IDENTITY AND ATTESTATIONS

To build a verified “Known Traveller” status, the traveller needs attestations. Authenticated claims as declared by a trusted entity, attestations, would be added to a traveller’s KTDI wallet each time a trusted entity (e.g. a government border official) verifies an identity claim. Currently the opportunity to collect these attestations in a distributed ledger-enabled KTDI wallet is being explored.

Eventually, the distributed ledger-enabled KTDI wallet will have the ability to include verified attestations such as proof of citizenship in country X, proof of an educational degree from college Y and proof of vaccination for viral disease Z. In the future, country A might authorize

a traveller to enter country A based on attestations, which do not contain any personal information, by country B (e.g. visa, entry and exit attestations).

Attestations are verified ‘proofs’ of granular identity components, provided by governments or other entities. Together these attestations generate the basis of the traveller’s reputation and ultimately can influence the determination of future security decisions related to immigration, border clearing, customs and pre-departure screening. The more attestations a traveller receives, the more confidence authorities may have in the traveller’s status as “known”, and the more data points authorities have upon which to make risk assessments.

An attestation is recorded in the form of a digital stamp in a traveller’s KTDI wallet and can be shared as part of identity validation history with other entities. The attestations linked to an issuing/attesting authority’s record would remain stored in a secure government solution. Access to the authority’s record of the attestation would only be granted by the issuing/attesting authority upon request of another trusted entity.

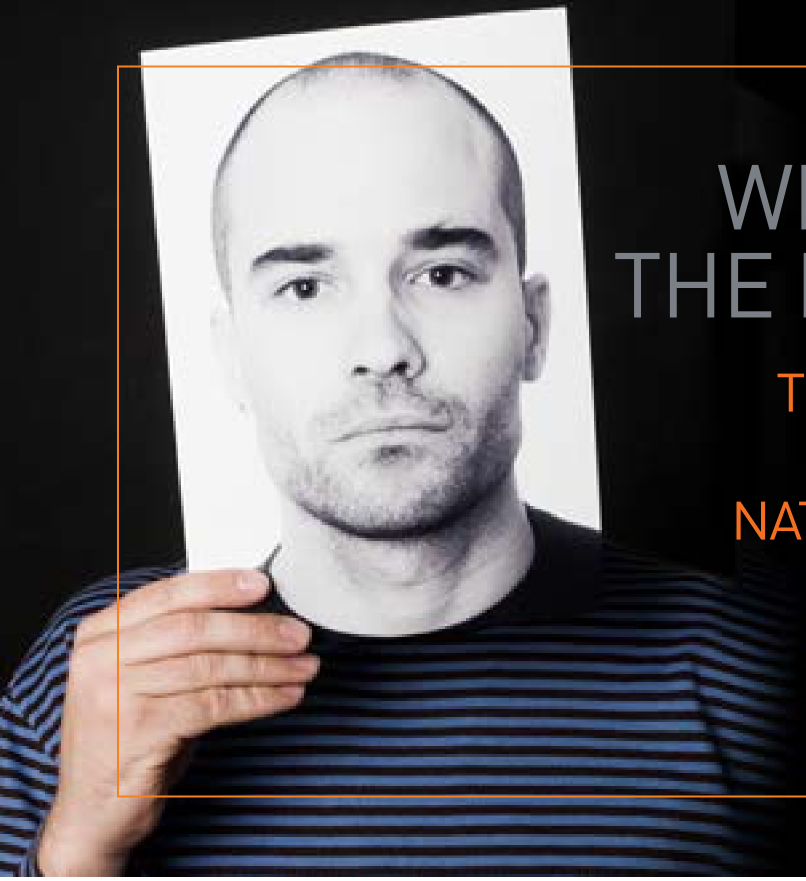
In the application for an attestation, the identity of the traveller is authenticated through biometric facial verification and any personal identity information remains protected by distributed ledger technology and cryptography. As travellers consolidate attestations into their Known Traveller wallet, they increasingly strengthen their claim to compliance, trust and legitimacy as a “known traveller”.

NEXT STEPS

Today’s aviation security and border crossing reality is not the reality that we will come to know in the next decade. The Forum supports the ongoing efforts of ICAO and its Member States that are dedicated to achieving the TRIP strategy, particularly work that relates to the exploration of digital travel credentials, the promotion of interactive API systems, and the collaboration with international organizations like INTERPOL and the International Organization for Migration (IOM). The Forum will continue to interact with all valued partners to explore what the changing technology, security and traveller behaviour landscapes may mean for the evolution of these activities, and the integrated responses to them.

For a more detailed overview of this work, please refer to 2018 report, The Known Traveller, by visiting *http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.*

LAUREN UPPINK CALDERWOOD
Head of Aviation, Travel and Tourism
Industries, World Economic Forum



WHO'S AFRAID OF THE BIG BAD WOLF?

THE ROLE OF THE OSCE IN IMPLEMENTING UNITED NATIONS SECURITY COUNCIL RESOLUTION 2396 (2017)

If you've ever heard the fairy tale of Little Red Riding Hood, you know that the Big Bad Wolf races ahead of the young girl who is going to visit her grandmother, and gets into bed disguised as the grandmother, after he has eaten her. Though Little Red Riding Hood notices her grandmother looks strange, she fails to discover the ruse, so she is also eaten by the Big Bad Wolf.

Hiding our identities is easier than we think. While the Big Bad Wolf's simple disguise fooled Little Red Riding Hood, with advanced forgery techniques and the lack of intelligence sharing among States, disguising one's identity today is more elaborate. Terrorists take advantage and travel unnoticed so we are often unable to detect their movements. The implications to society can be devastating, as we have seen in attacks over recent years.

Foreign terrorist fighters (FTFs) in their countries of origin, or those travelling to other regions, pose a serious threat to States, given the risk that they may carry out attacks at home, or engage in recruitment efforts.

With the adoption of Resolution 2396 in December last year, the United Nations (UN) Security Council identified a series of measures that will help States deal with the challenge of returning and relocating FTFs. Resolution 2396 has four key border security elements: (i) improving screening procedures at the border; (ii) cross-checking passenger data against watch lists and databases; (iii), collecting biometrics; and (iv), enhancing information exchange.

The aim of this article is twofold. After looking at these four elements separately, we'll consider the ways the OSCE is supporting the implementation of Resolution 2396 in each of these four areas.

BORDER SCREENING

In January 2017, 14 people were convicted by a Belgian court of producing fraudulent identity documents. Some of these documents had been sold to individuals who were involved in the November 2015 Paris attacks and in the 2016 Brussels bombings. When considering that the group managed to forge more than 2,000 passports and IDs, it is terrifying to imagine what other terrorist incidents could have taken place had these documents fallen into the wrong hands.

It is imperative that States set up effective measures at their borders to assess whether travelers are using fraudulent identities and travel documents. This is particularly relevant at the border crossings of OSCE participating States where they do not have passport readers or even electricity! In these areas, border security is completely reliant on the border guard's ability to analyze the traveller and the travel document to recognize a fake.

Resolution 2396 obliges States to strengthen border security through more thorough checks of forged documents and enhanced identification management. At the OSCE, we are supporting States by training front-line officers on the detection of imposters and fraudulent documents. We also have a dedicated Mobile Training Team that delivers on-site training to border officials to be able to better identify and interview potential FTFs at border controls.

PASSENGER DATA

On 24 May 2014, four people were killed in Brussels by a man armed with a Kalashnikov rifle. Despite being on several terrorist watch-lists, the man was able to fly back to Europe to carry out the attack because his data was not checked against the watch-lists before he travelled.

With the adoption of Resolution 2396, all States are required to collect passenger data in advance and cross-check this information against watch-lists and databases. This obligation includes two different types of data: Advance Passenger Information (API) and Passenger Name Record (PNR).

API and PNR are not quite the same. API data is the biographic data contained in a passenger's travel document that is submitted to the airlines during check-in. PNR data is the information provided when booking a flight, including contact details and payment information. While API is useful for matching against watch-lists and risk profiles, PNR can help to identify suspicious travel patterns and hidden connections between known threats and their unknown associates by examining specific data elements, like credit card numbers.

The OSCE has been offering support to States for establishing API and PNR systems. We have been working directly with national authorities to prepare tailored action plans for implementation. We further help them to implement these plans by providing legislative advice as well as technical and operational support.

BIOMETRICS

In November 2017, US authorities arrested a Saudi citizen residing in Oklahoma who trained with Al Qaeda in late 2000. The FBI was able to identify the man when they matched his fingerprints against those taken from an application form for the terrorist group's training camp when it was seized in Afghanistan.

Biometrics can be a valuable tool for verifying that individuals are who they say they are. Terrorist and organized criminals will try to mask their identities in a number of ways, whether by using fraudulent passports or taking on new identities, but it is a lot harder to fake their fingerprints.

Because fingerprints and facial scans can be used to validate the identity of travellers and their travel documents, Resolution 2396 mandates that all States begin collecting biometric information. Given how massive this undertaking is, it will take many years for all States to be able to securely and safely collect and store biometric data.

The OSCE is ready to provide capacity-building assistance in this regard. We are assisting States to improve the security of their ePassports by helping them join the ICAO Public Key Directory (PKD), a repository which allows them to verify the biometric and biographic data in the chip of the passport.

We have also been partnering with INTERPOL to promote States' access to their databases, including those of fingerprints, DNA profiles, and of suspected FTFs. Additionally, we are communicating with independent bodies to identify potential gaps in the use of biometrics for counterterrorism purposes. An OSCE-wide seminar on best practices in the collection of biometric data will be organized jointly with the Biometrics Institute in the first half of 2019.

INFORMATION SHARING

In the aftermath of the November 2015 Paris attacks, we learned that information on the backgrounds of some of those involved was available months before the attack, but that it was not shared between European intelligence services. Dealing effectively with transnational threats requires continuous co-operation and intelligence sharing between law enforcement authorities. This is why Resolution 2396 stresses the need for increasing information exchanges both within, and among, States.

With regards to internal information sharing, the OSCE supports States in adopting integrated border management strategies and establishing Police-Customs Co-operation Centres. Likewise, in our work on passenger data, we help States to establish a single window or passenger information unit where national agencies can share information with one another.

Inter-State information sharing usually takes place through the use of international or regional databases, such as those of INTERPOL or Europol. The challenge is that not all border control points have access to these databases, and not all States are populating the databases with the relevant data. The OSCE and INTERPOL have recently adopted a Joint Action Plan with a view to closing these information exchange gaps.

CONCLUSION

This article focussed on the significance of UN Security Council resolution 2396 in four key areas: border screening, passenger data, biometrics, and information exchange. While important steps have already been taken, there is still a lot to be done.

Looking back at the tale of Little Red Riding Hood, my favourite ending has a group of young girls, who help her escape from the Big Bad Wolf, washing bed sheets by the river. While Little Red Riding Hood manages to cross the river by walking over the sheets, the girls let go of them when the wolf tries to do the same, leaving him to be carried away by the waters.

This ending shows the importance of working together. Resolution 2396 calls for States and International Organizations to collaborate in preventing the movement of terrorists and that is what the OSCE is striving to achieve. T

ADRIÁN CARBAJO
Adviser on Passenger Data Exchange,
OSCE Border Security and
Management Unit

BIOMETRIC IDENTIFICATION OF CHILDREN FOR IMMIGRATION CONTROL

The European Commission is the executive arm of the European Union (EU) that implements the Union's political and strategic direction. As the science and knowledge service of the European Commission, the mission of the Joint Research Centre (JRC) is to support European Union policies with independent evidence throughout the policy cycle.

European Commission

In line with other regions around the world, the EU began integrating biometrics in a number of identity documents as a means for increasing border security for immigration control. New generation passports are equipped with electronically readable fingerprints and face images, the EU Visa Information System uses face and fingerprint verification for checking the validity of visas.

The proposed new EURODAC system (fingerprint database of asylum seekers) involves the enrolment of children from the age of six years. In this context, the JRC carried out research to determine whether or not automated fingerprint recognition works as well for children as it does for adults. In fact, it does – provided fingerprints can be acquired with sufficient quality.

THE CHALLENGE

The proper use of a technology requires precise knowledge of its limits and constraints. With automated fingerprint recognition technology, well-known limits related to *processing performance* (i.e. how fast it can be done), to accuracy (i.e. how reliable the result of a recognition is) and to handling (i.e. the level of expertise necessary for its use), exist. However, there is also a limit with respect to ageing.

One thing biometric identifiers, including fingerprints, have in common is that they are based on physiological properties that may change over time. In particular, with fingerprints, it is assumed that the characteristic pattern obtained from each finger is unique and remains unchanged for a lifetime, but at minimum, the size of the pattern grows during adolescence.

FINGERPRINT DATA OF PORTUGUESE CHILDREN:

- Some *1600 children*, scanned twice within 2–4.5 years, using *500-dp*i fingerprint scanners
- left and right index finger
- age coverage: *0–11 years*
- *three “black box” algorithms,* issuing a matching percentage

Does the pattern evolvement significantly hamper the automated fingerprint verification of children? While human fingerprint experts do not encounter a problem when they review fingerprints obtained at different ages of the same person, automated systems were not originally designed to cover such cases. Before the JRC began its study (requested by the European Parliament in 2008), there was no evidence that automatic fingerprint recognition systems would be able to correctly match samples of the same (juvenile) user acquired with several years’ difference. On the contrary, developers of these systems already highlighted the existence of potential problems with the recognition of child fingerprints.

JRC APPROACH

Though access to child fingerprint data became integral to the study, very few, and in most cases inappropriate, resources existed. In particular, there was no data available where the data subjects were followed over a sufficiently long period of time to address the feasibility question.

Fortunately, the Portuguese authorities offered by courtesy, anonymized fingerprint data of children obtained in the context of issuing passports (see Figure 1). One public domain and two commercial algorithms for automated fingerprint recognition systems were used to study their behavior under the particular age constraints.

The feasibility question of the study was broken down according to three lines of investigation:

1. Perform recognition experiments with current and prototype matching algorithms, targeted to analyse dependencies with respect to age groups and time differences between the acquired fingerprints.
2. Analyse the growth effect by estimating the feature displacement in two corresponding fingerprints, and create a model to describe the feature displacement.
3. Quantify issues related to the image acquisition through experiments with traditional and alternative acquisition devices (fingerprint scanners).

MAIN FINDINGS

Surprisingly, it was found that the **growth of the fingerprint pattern** had much less influence on recognition accuracy than predicted. All tested algorithms showed the same recognition rate regardless of the time between the fingerprints (of up to 4½ years).

Another important uncertainty concerned the **image resolution**. Is the usual image resolution of 500 dpi (of state-of-the-art fingerprint scanners – see image) sufficient to identify the relevant fingerprint features of young children? The answer is yes, despite the fact that the distance between ridges (fingerprint lines) of children can be up to one third of those of adults. Within the available time window of up to 4½ years between the acquired fingerprints, there was no principle barrier observed for proper automated recognition by existing matching algorithms – provided the images were of sufficient quality.

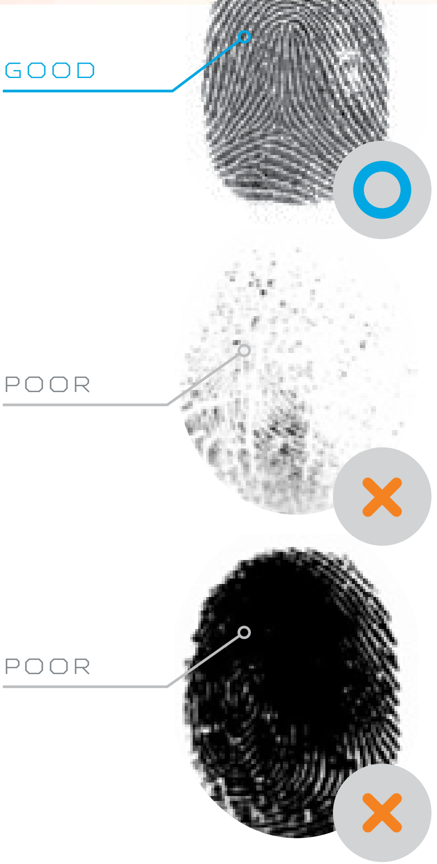


Figure 1

In fact, **image quality** remains the only limiting factor. Though this is a well-known constraint for adults (Figure 2), with the smaller structure sizes of child fingerprints, the constraints get worse, and the probability for these constraints increases. Therefore, proper enrolment is the key factor for successful recognition. In short: smaller dimension + poor quality = reduction in recognition.

> *"Surprisingly, it was found that the growth of the fingerprint pattern had much less influence on recognition accuracy than predicted."*

In summary, the study confirmed that under proper acquisition conditions, *fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy.*

RECOMMENDATIONS

A minimum level of training of operators and (child) clients is necessary for acquiring high quality images. This concerns mainly the proper monitoring of the condition of the particular finger skin part that needs to be enrolled. Poor quality usually occurs when the skin is either too dry or too humid. It is recommended to conduct relevant best practice studies to find optimal operation conditions.

Matching algorithms can be further improved by taking into account the age of the child and the time between individual fingerprint enrolments. The study confirmed the validity of an isotropic growth model that can help to predict the change of fingerprint patterns over time.

Relevant quality metrics for fingerprints need revision with children. As quality metrics for fingerprint images assume feature dimensions for adults, adaption to child fingerprints will be required. Otherwise, the reported quality scores might mislead the acquisition process.

Finally, more emphasis should be put on the selection of acquisition devices. The image quality constraints mentioned mainly occur when using the state-of-the-art optical fingerprint systems that are currently, widely used in border and immigration controls. Alternative technologies, such as touchless devices or multispectral devices, showed in a number of experiments, better resilience with respect to the quality degrading issues of the optical fingerprint sensors.

In any case, larger field trials on the enrolment of children need to be conducted in order to quantify a practical age limit, given the best available technology. These trials should further investigate and quantify the impact of certain enrolment devices and procedures.

The full JRC report can be downloaded from: *http://publications.jrc.ec.europa.eu/repository/bitstream/JRC85145/fingerprint%20recognition%20for%20children%20final%20report%20%28pdf%29.pdf* or *https://tinyurl.com/yauto7q5*

GUNTER SCHUMACHER
Program Manager, Joint Research Centre of the European Commission

JAN LÖSCHNER
Scientific Officer, Joint Research Centre of the European Commission

COMPLETING THE TRIP CONTINUUM BODY OF TECHNICAL GUIDANCE MATERIAL:

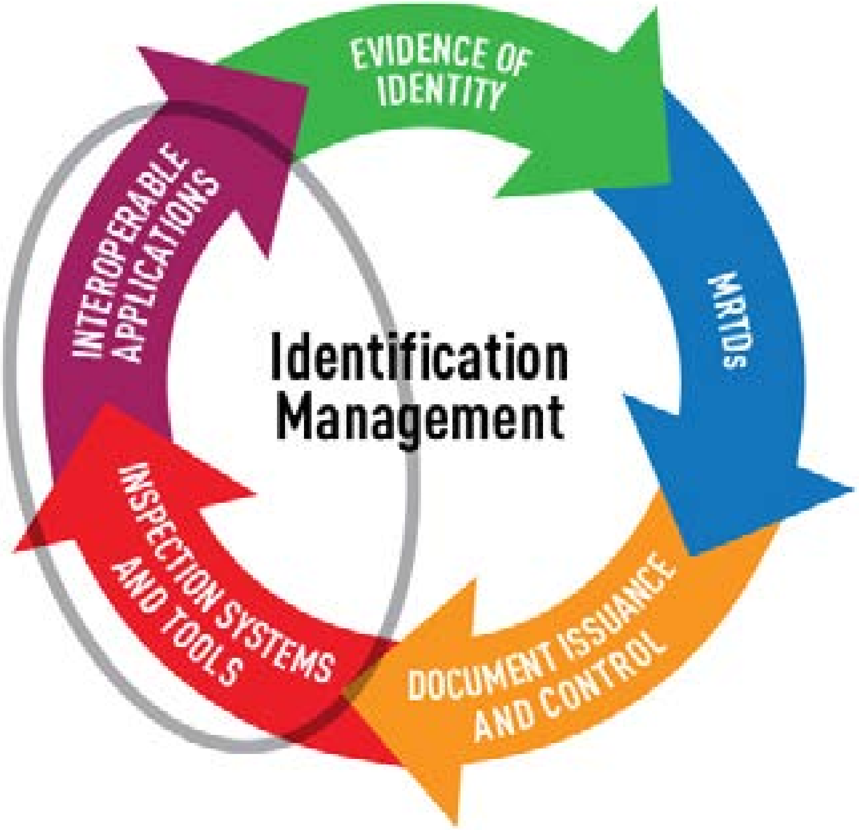
BORDER CONTROL MANAGEMENT

Funded by the Government of Canada | Canada

SUMMARY
ICAO's Facilitation Section has been delivering direct technical assistance to States since 2014. This engagement seeks to enhance the implementation of the five elements of the ICAO Traveller Identification Programme (TRIP) Strategy by States, in partnership with a broad range of stakeholders, including the ICAO Technical Advisory Group (TAG) and international and regional organizations. The most recent such initiative, focussing on border control management, was implemented in the Caribbean region.

The project *Strengthening Travel Document Security and Identification Management in the Sahel Region* was the Facilitation Section's first project that delivered direct assistance to States. This pilot project, completed in 2016, set the stage for a second project, *Strengthening Border Control Management in the Caribbean Region* ("Caribbean Project"), undertaken between 2016 and 2018. Both projects were funded by the Government of Canada.

The Caribbean Project provided an opportunity for further advancing work related to Border Control Management (BCM) because it focussed on two TRIP elements: *Inspection Systems and Tools and Interoperable Applications.*


EVIDENCE OF IDENTITY
MRTDs
DOCUMENT ISSUANCE AND CONTROL
INSPECTION SYSTEMS AND TOOLS
INTEROPERABLE APPLICATIONS
Identification Management

The project complemented the on-going efforts of the Facilitation Section to extend the dialogue beyond the traditional interlocutors of the Machine Readable Travel Document (MRTD) Programme, to the full array of parties concerned with the TRIP Strategy, expanding the focus from the travel document issuance community to all stakeholders concerned with authentication of MRTDs at borders.

The ICAO TRIP Guide on BCM ("the Guide") was the key outcome of the Caribbean Project. The Guide is intended as reference for Member States to optimize the use of technologies available that enhance their national BCM. Being a product of the TRIP Strategy, the Guide focuses on the border controls applied to travellers. The regulatory framework of the Guide is found more prominently in the Standards and Recommended Practices (SARPs) of Annex 9 – *Facilitation* and in the technical specifications of Doc 9303, Machine Readable Travel Documents.

By providing a framework of 13 technical topics that describe and categorize *Inspection Systems and Tools* and *Interoperable Applications*, the Guide completes the body of technical guidance material available to States covering the full continuum of traveller identification.

With their traveller border control arrangements, States seek to maximize

Inspection Systems and Tools	Interoperable Applications
A. Visas and Electronic Travel Systems	H. Advance Passenger Information and Interactive Advance Passenger Information
B. Document Readers	I. Passenger Name Record
C. Biographic Identity Verification	J. Public Key Infrastructure and the ICAO Public Key Directory
D. Biometric Identity Verification	K. eMRTD Biometric Identity Verification
E. National Watchlists	L. INTERPOL's Stolen and Lost Travel Documents Database
F. Entry and Departure Databases	M. International Watchlists
G. Automated Border Controls	

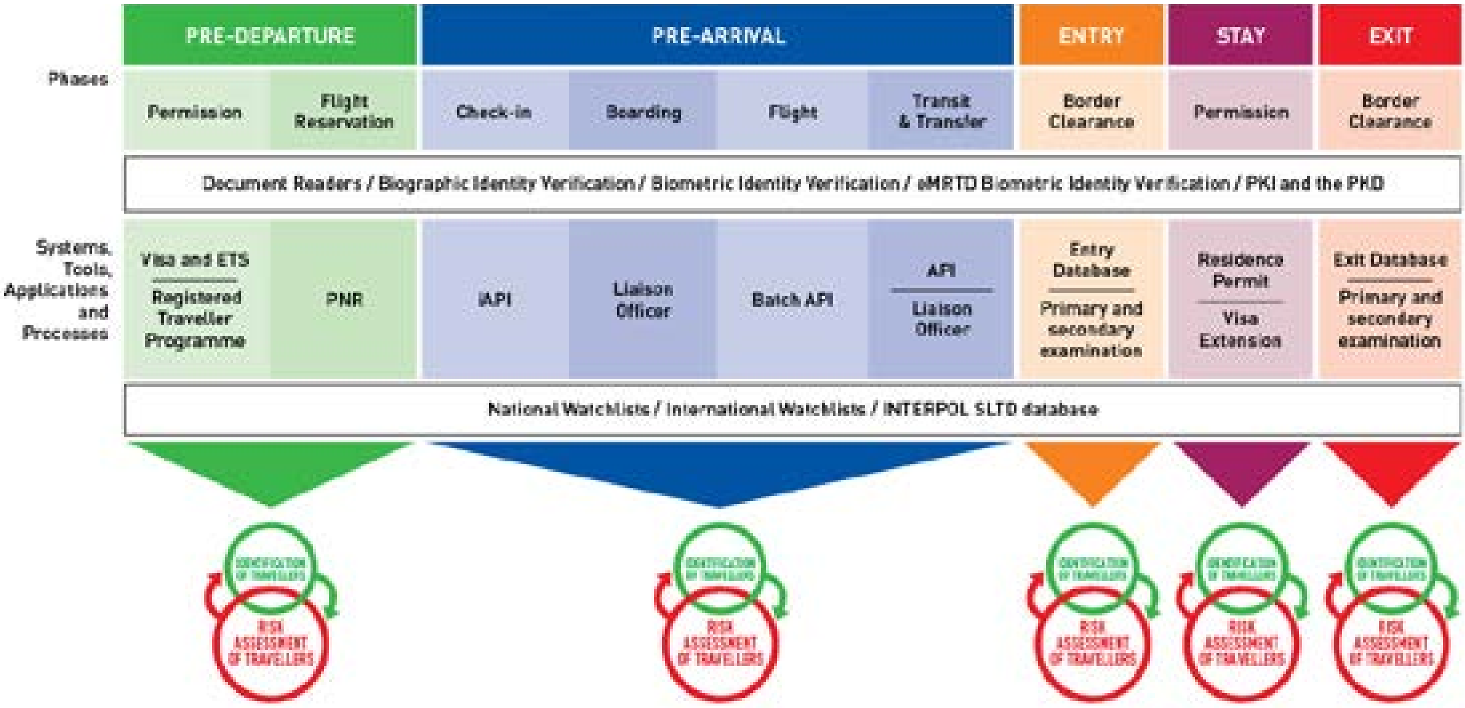
TRIP technical guidance material is available for download at: *https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx*

the economic, social and political benefits of travel while at the same time identifying and mitigating risks and threats. The central concept of the Guide is that BCM is most effective when the iterative process is repeated when new information becomes available at each phase of the journey: pre-departure, pre-arrival, entry, stay and exit.

While technology is central to the TRIP Strategy, the Guide addresses other aspects that are critical to the management of border controls, including the environment in which border controls are applied, strategic and legal frameworks, BCM agencies and stakeholders, the examination of travellers, the inspection of travel documents, and human resource considerations.

Though States can be expected to have extensive knowledge of their own citizens and residents, they rely on foreign data and information about the identity and nationality of the citizens and residents of other States. Therefore, the SARPs and technical specifications published by ICAO play a critical role in ensuring that travel documents issued by States contain standardized traveller identity information in a standardized machine readable format that can be communicated and shared in a standardized, interoperable way.

The Guide discusses contributions made by other United Nations agencies and international organizations to BCM. The Consolidated UN Security Council Sanctions List and INTERPOL Red Notices identify potential travellers of security and law enforcement concern to States. Checks against INTERPOL's Stolen and Lost Travel Documents database


PRE-DEPARTURE
PRE-ARRIVAL
ENTRY
STAY
EXIT
Phases
Permission
Flight Reservation
Check-in
Boarding
Flight
Transit & Transfer
Border Clearance
Permission
Border Clearance
Document Readers / Biographic Identity Verification / Biometric Identity Verification / eMRTD Biometric Identity Verification / PKI and the PKD
Systems, Tools, Applications and Processes
Visa and ETS
Registered Traveller Programme
PNR
iAPI
Liaison Officer
Batch API
API
Liaison Officer
Entry Database
Primary and secondary examination
Residence Permit
Visa Extension
Exit Database
Primary and secondary examination
National Watchlists / International Watchlists / INTERPOL SLTD database
IDENTIFICATION OF TRAVELLERS
RISK ASSESSMENT OF TRAVELLERS

Traveller identification and risk assessment is repeated throughout the traveller journey as additional information becomes available to the receiving/destination State

TRIP 2017
Second ICAO TRIP Workshop on Border Control Management in the Caribbean region
TRIP
5
2. Travel Document Authentication

ICAO TRIP Workshop on BCM in the Caribbean Region, Jamaica, November 2017

are essential prior to relying on travel documents as evidence of identity.

The two parts of the Guide are complementary and intended to be used together. The Part 1: *Guidance Material* and Part 2: *Assessment Tool* can assist States to achieve better security and facilitation outcomes in BCM.

The ICAO TRIP Guide on BCM is available at: https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx

For questions or to communicate with the Facilitation Section, States are invited to write to: FAL@icao.int.

ICAO extends its appreciation to the subject-matter experts who have developed the content of the ICAO TRIP Guide on BCM and to organizations that have contributed to its review: European Border and Coast Guard Agency (FRONTEX), ICAO Implementation and Capacity Building Working Group (ICBWG), ICAO New Technologies Working Group (NTWG), International Criminal Police Organization (INTERPOL), IOM, Joint Regional Communication Centre (JRCC) of the CARICOM Implementing Agency for Crime and Security (IMPACS), OECS, United Nations CTED, United Nations High Commissioner for Refugees (UNHCR) and United Nations Office on Drugs and Crime (UNODC).

KARINE BOULET GAUDREAULT
Manager, Aviation Facilitation,
International Air Transport Association (IATA)

ROSS GREENWOOD
Expert, Border Control Management

THE CARIBBEAN PROJECT AT A GLANCE

STATES PARTICIPATING IN THE PROJECT	Antigua and Barbuda, Bahamas, Barbados, Belize, Cuba, Dominican Republic, Grenada, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, and Trinidad and Tobago
IMPLEMENTING PARTNERS	United Nations Counter-Terrorism Committee Executive Directorate (CTED) with the support of two regional organizations – the Caribbean Community (CARICOM) and the Organisation of Eastern Caribbean States (OECS)
IMPLEMENTATION PERIOD	2016-2018
ACTIVITIES	1. Development of the ICAO TRIP Guide on Border Control Management; 2. Four Technical Assistance Missions: Barbados; Dominican Republic; Jamaica, jointly with the Counter-Terrorism Executive Directorate (CTED); and Saint Lucia jointly with the International Organization for Migration (IOM); and 3. Two ICAO TRIP Workshops on BCM: Antigua and Barbuda and Jamaica.

THE DOCUMENT SECURITY FEATURES ELECTRONIC LEARNING COURSE

INTRODUCTION

Biometric travel documents, including ePassports, can provide powerful facilitation and security advantages in environments where the capabilities of the chip can be utilized. The challenge is that many countries do not issue ePassports, and passports examined in environments without the appropriate reader and supporting infrastructure cannot utilize ePassport functionality. Additionally, many identity documents (for example, birth records) do not contain machine-readable technologies. Accordingly, physical inspection of documents remains relevant and will continue in border control, consular, vital records, and similar environments. This article introduces the U.S. Department of State's electronic learning course, *Document Security Features*, which the Department intends to make available to a wide audience because visual counterfeit detection training remains an ongoing need in many countries.

COUNTERFEIT DETECTION TRAINING IN THE CLASSROOM

In-depth training on document security features and counterfeit detection has traditionally been delivered in the classroom, with reliance on hands-on exercises with physical documents. This is equally a product of the subject matter of security document training and a historical deficit of alternative instructional technologies.

Many security features require manipulation of a document to visualize the security feature effect. For example, watermarks and see-through register icons must be held up to a light; optically variable devices and color shifting features must be tilted; printing process characteristics and microtext must be viewed through a magnifier; and ultraviolet-reactive features require an ultraviolet light. These technologies are used to deter counterfeiting because they don't photograph or photocopy well. At the same time, this means that their dynamic visual effects can be hard to convey using only still images in slides or handouts, so physical document exemplars are used in the classroom.

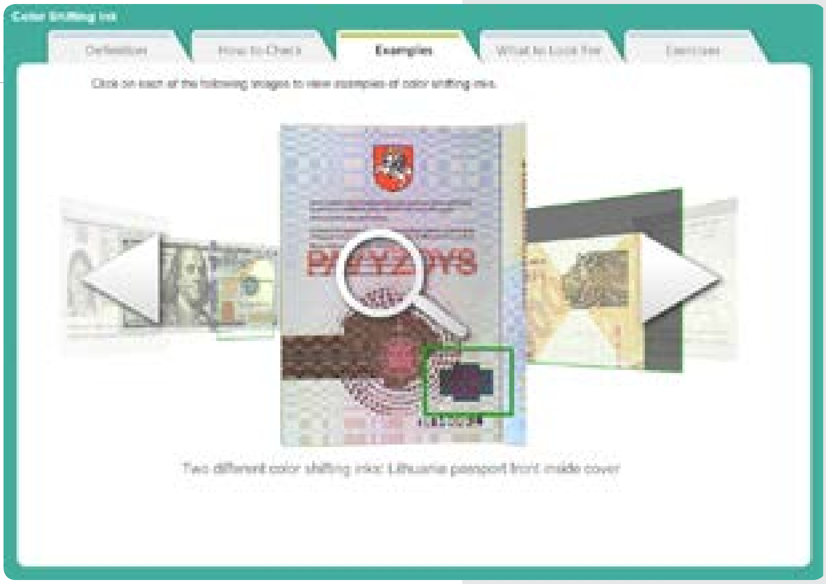
However, the effectiveness of classroom counterfeit detection training suffers from a number of limitations related to resources. Classrooms can only accommodate finite numbers of students at a time, so training for large numbers of staff requires the same classroom course to be hosted repeatedly. Classroom training requires the total attention of both the students and the instructor, who cannot perform other work duties while the course is in session. Travel and logistical complications may further increase costs or the time required to host the training. The availability of exemplar documents can also present a problem. If a particular national passport is to be studied by a group of 24 students, then ideally 24 physical exemplar passports would be available, but this is frequently not possible.

When a country issues a new security document, one (or a few) exemplars may be provided to other States, but usually in very limited quantities. Even then, the exemplars may be used primarily for forensic comparison purposes, preventing them from being used for routine training that would expose them to wear or damage. The result is that although many countries possess collections of exemplar documents, the only exemplars most document trainers can access in quantities sufficient for classroom training are the exemplar documents from their own countries. This limitation can prevent trainers from providing document inspection classroom training that features a diverse set of international documents obtained from a variety of issuers. This problem is shared by many trainers and many document issuers, and it can be addressed through electronic learning.

THE TRANSITION TO ELECTRONIC LEARNING

Electronic learning cannot fully substitute for examining real physical documents. However, electronic learning offers several compelling advantages that overcome many of the resource constraints of classroom training. Electronic learning modules require significant up-front development costs, but once an electronic learning module is created, it can be delivered globally to unlimited numbers of students – over months or years – without the ongoing expenses of classrooms, instructors, or travel. Logistics are simplified, as trainees are able to complete electronic learning modules during incremental periods of down-time in their usual work environments, instead of traveling to another location. Course planning is also reduced because each student completes the training independently, on their own schedule.

Most importantly, electronic learning helps to overcome the availability of

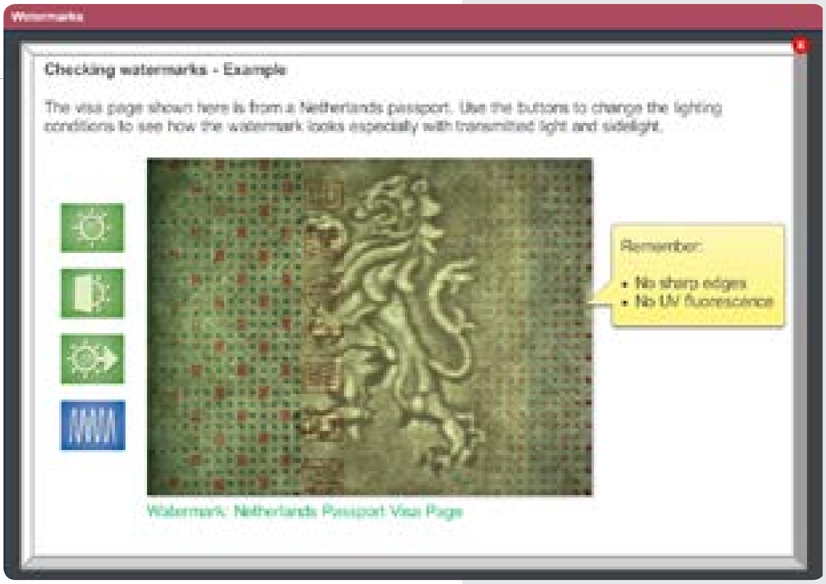


Click on each of the following images to view examples of color shifting inks.

Two different color shifting inks: Lithuania passport front inside cover

Figure 1.

Scrolling menu of document examples from the "Color Shifting Ink" topic in Document Security Features. This menu features thirteen examples of color shifting ink implementations in passports, identity cards and banknotes.



Checking watermarks - Example

The visa page shown here is from a Netherlands passport. Use the buttons to change the lighting conditions to see how the watermark looks especially with transmitted light and sidelight.

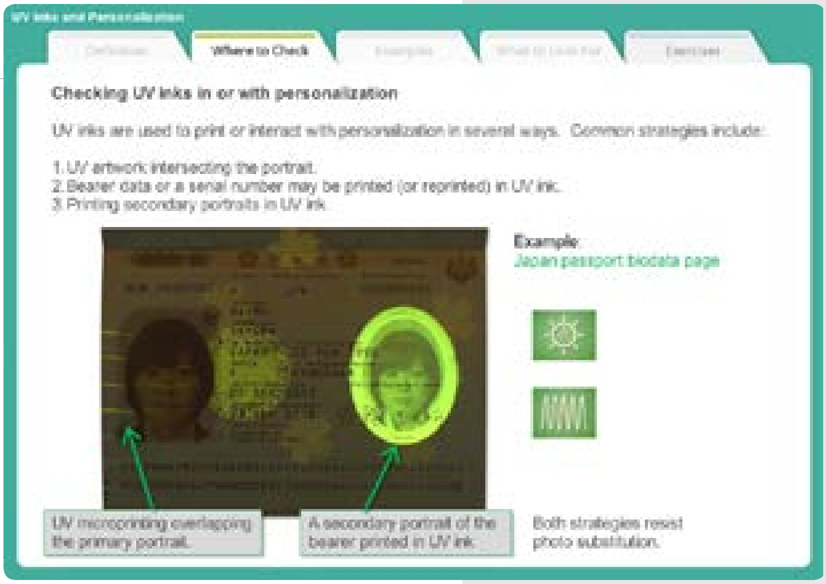
Remember:

- No sharp edges
- No UV fluorescence

Watermark: Netherlands Passport Visa Page

Figure 2.

Transmitted light view of a passport visa page from the "Watermarks" topic in Document Security Features. The buttons at the left allow the user to view this watermark in several different lighting conditions.



Checking UV inks in or with personalization

UV inks are used to print or interact with personalization in several ways. Common strategies include:

1. UV artwork intersecting the portrait.
2. Bearer data or a serial number may be printed (or reprinted) in UV ink.
3. Printing secondary portraits in UV ink.

Example:
Japan passport biodata page

UV microprinting overlapping the primary portrait.

A secondary portrait of the bearer printed in UV ink.

Both strategies resist photo substitution.

Figure 3.

Instruction screen describing how ultraviolet-reactive inks are typically integrated with personalization in a passport data page, from the "UV Inks and Personalization" topic of Document Security Features.

PAPER SUBSTRATE SECURITY FEATURES

- Security Fibers/Planchettes
- Security Threads
- Watermarks
- Die Cuts and Shatter Cuts
- Solvent-Sensitive Components

PLASTIC SUBSTRATE SECURITY FEATURES

- Types of Plastic Cards
- Laser Engraving
- Tactility
- Windows

SECURITY FEATURES IN PRINT

- Microprinting
- Split Fountains
- See-through Register
- Latent Images

SPECIALTY INKS

- Metallic Ink and Hot Foil Stamps
- Iridescent Ink
- Color Shifting Ink
- UV Inks and Artwork
- UV Inks and Personalization
- Other Specialty Inks

OPTICALLY VARIABLE DEVICES

- Metallized OVDs
- Demetallized OVDs
- Multiple OVDs

LENS SECURITY FEATURES

- Lenticular
- Lenticular Decoder
- Micro Optic
- Retroreflective

Table 1

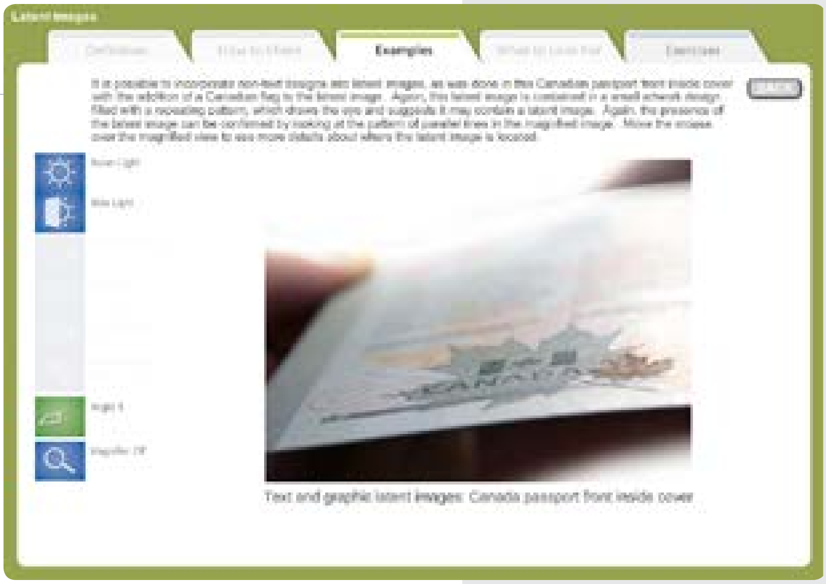
limited physical document exemplars because interactive animation technologies can simulate the effects of even very complex security features on a screen, with no physical documents required. This creates an economy of scale because a single document exemplar is difficult to share between many students in a classroom, but one exemplar can be used to create interactive virtual exercises, animations, or security feature effect simulations that can be shared with unlimited numbers of students worldwide. This approach allows training to migrate from a document-centric paradigm (focusing on only one issuer's documents, examined physically in a classroom) to a technology-centric paradigm (focusing on virtual examination of the most common security technologies used in all security documents, from all issuers).

The goal of the technology-centric paradigm is to provide trainees with a thorough understanding of common security feature technologies as they are implemented across document types, without a focus on a single national issuer. It is impossible to memorize which security features are present in the hundreds of national passports and other documents in use globally, but it is possible to recognize the most common technologies pulled from the same limited pool of physical security features that are used by all security document issuers. For example, a module on how to inspect watermarks could include watermark features in several international passports, birth records, and banknotes to illustrate that watermarks are used in similar ways across documents of different types. This prepares learners to locate and evaluate a watermark when presented with an unfamiliar document, even without reference materials, because the learner already understands watermarks as a technology. The training concept is similar for other classes of common security features.

DOCUMENT SECURITY FEATURES eLEARNING

In alignment with the goals described above, the Bureau of Consular Affairs and the Diplomatic Security Training Center (components of the U.S. Department of State) have jointly developed Document Security Features, an electronic learning primer on the most common counterfeit- and alteration-resistant security technologies used in documents such as passports, identity cards, visas, birth records, and banknotes. Instead of exclusively training on documents issued by the U.S. Department of State, Document Security Features incorporates a wide variety of international document examples. The example documents change between different security feature topics, which ensures that the most appropriate examples of each particular technology are showcased, and that each example contains new information. The goal is for learners to gain the ability to self-train on new and unfamiliar documents by quickly recognizing that they probably contain many of the same security feature technologies they have observed previously in other documents.

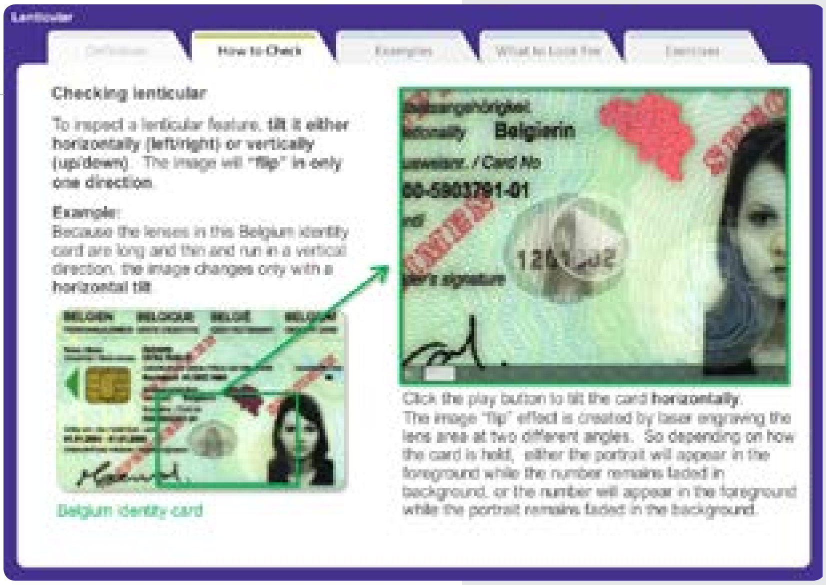
Document Security Features is composed of a series of modules that cover a variety of anti-counterfeiting and anti-alteration technologies used in documents, which have been classified according to the menu structure shown in Table 1. To closely replicate the visual effects of each security feature technology across a range of diverse document examples (see Figure 1), the development of Document Security Features required extensive photography and animations of document manipulation for user interactivity. For example, many of the security feature technologies require transmitted lighting (see Figure 2), ultraviolet light (see Figure 3), tilt actions (see Figure 4) or other specialized viewing conditions to be authenticated, so users of Document Security Features can control lighting conditions and play animations (see Figure 5) that simulate manipulation of virtual documents. Typical users report



It is possible to incorporate non-text designs into latent images, as was done in this Canadian passport front inside cover with the addition of a Canadian flag to the latent image. Again, this latent image is contained in a small artwork design filled with a repeating pattern, which draws the eye and suggests it may contain a latent image. Again, the presence of the latent image can be confirmed by looking at the pattern of parallel lines in the magnified image. Move the scope over the magnified view to see more details about where the latent image is located.

Text and graphic latent images: Canada passport front inside cover

Figure 4.
Tilt view of an intaglio latent image in a passport endsheet, from the "Latent Image" topic of Document Security Features. The buttons at the left allow the user to see this feature in other lighting conditions.



Checking lenticular

To inspect a lenticular feature, **tilt it either horizontally (left/right) or vertically (up/down).** The image will **"flip" in only one direction.**

Example:
Because the lenses in this Belgium identity card are long and thin and run in a vertical direction, the image changes only with a **horizontal tilt.**

Belgium identity card

Click the play button to tilt the card **horizontally**.
The image "flip" effect is created by laser engraving the lens area at two different angles. So depending on how the card is held, either the portrait will appear in the foreground while the number remains faded in background, or the number will appear in the foreground while the portrait remains faded in the background.

Figure 5.
Instruction screen featuring a playable animation of a lenticular image flip in an identity card, from the "Lenticular" topic of Document Security Features. Animations are used for effects that can't be displayed with static images.

spending 8-10 hours to complete all of the content, making Document Security Features one of the most comprehensive low-cost training options available on the subject of counterfeit detection.

REQUESTING THE COURSE

The U.S. Department of State intends to make Document Security Features available to other organizations, subject to Department approval. Document Security Features is expected to be available at no charge. Requesting organizations will be responsible for any IT support or infrastructure required for course deployment. Government agencies and multinational organizations interested in using Document Security Features for their own training purposes are advised to contact the Counterfeit Deterrence Laboratory, Office of Fraud Prevention Programs, Bureau of Consular Affairs, U.S. Department of State at *CA-FPP-CDL@state.gov*.

JOEL ZLOTNICK
Supervisory Physical Scientist
Counterfeit Deterrence Laboratory
Office of Fraud Prevention Programs
Bureau of Consular Affairs
U.S. Department of State

CORRECTION: ICAO incorrectly identified article author Joel Zlotnick in a previous publication of this article. Mr. Zlotnick should have been identified as written above.

THE FEDERAL POLICE OF BRAZIL AND THE ICAO TRIP STRATEGY

At the 39th Assembly of the International Civil Aviation Organization (ICAO) held in 2016, the ICAO Traveller Identification Programme (TRIP) Strategy was adopted to provide the framework for bringing together the elements of identity management in order to maximize the benefits of document and border control.

The ICAO TRIP Strategy serves as a stimulus to Member States to adopt, in a manner that is committed to the terms of the Chicago Convention (in particular, Articles 13, 22, 23, and 37, j), the issuance of documents in accordance with the provisions of Annex-9 to the Chicago Convention and in accordance with best practices set out in Doc 9303 - Machine Readable Travel Documents (MRTDs).

Compliance with Doc 9303 for the issuance of MRTDs entails observing certain technical and legal formalities that result in Member State participation in the ICAO Public Key Directory (PKD), which enables all Member States participating in this directory to automatically verify the data pertinent to the travel document issued (MRTD) when carrying out migration control. This represents a major step forward from the point of view of both facilitation and the security of civil aviation, especially when combined with other tools such as Passenger Name Records (PNR) and Advanced Passenger Information (API) (also referred to in Annex-9).

Brazil enthusiastically supports the TRIP Strategy, having initiated the issuance of MRTD passports according to ICAO Standards and the implementation of the International Traffic System (STI), which is compatible with PKD in 2008. The State has hosted TRIP events in 2012 and, very recently, in 2018.

THE ROLE OF THE FEDERAL POLICE OF BRAZIL IN IMPLEMENTING THE TRIP STRATEGY

Brazil, with all the public and private institutions that make up the Brazilian civil aviation system, is fully committed to the guidelines established by ICAO in all matters related to facilitation and aviation security.

In this regard, it is important to note Brazil's National Programmes, namely: the National Civil Aviation Security Programme – NCASP (PNAVSEC, in Brazil) published by Decree No. 7168/2010; and the National Air Transport Facilitation Programme (PROFAL in Brazil), published by Resolution No. 01/2017 of the National Commission of Airport Authorities (CONAERO).

The Federal Police of Brazil (PF) have a number of responsibilities. They play a prominent role in both executing the programmes, and in promoting the balance and coordination that must exist between the areas of operation. The PF is an institution that exercises the functions of maritime, airport and border police, as provided in article 144, item I, paragraph 1, III of the Federal Constitution. Given its constitutional mandate, the PF is the agency responsible for:

1. Migration control (or border control) - an activity that it executes exclusively, in accordance with Law 13445/2017 and Decree No. 9199/2017;
2. Issuance of travel documents – an activity carried out in coordination with the Ministry of Foreign Affairs (MRE), where the PF is responsible for the issuance of a common passport, foreign passport and laissez-passer in national territory, according to Decree No. 5.978/2006.
3. Airport security – an activity carried out in coordination with the National Civil Aviation Agency – CAA (ANAC in Brazil), where it has responsibility for the supervision of the national civil aviation security system, according to Decree No. 7.168/2010;
4. Airport police – extensive police activity carried out in coordination with all public security institutions regarding the maintenance of order and prevention of crimes committed in an airport environment and/or against the national airport system; and
5. International police cooperation - the PF is the Brazilian institution responsible for carrying out the operations of the International Criminal Police Organization - INTERPOL in Brazil, which, when in an airport environment, are directly related to the four activities mentioned above.

MIGRATION CONTROL (OR BORDER CONTROL)

The PF is historically the Brazilian institution responsible for carrying out migration control in Brazil and since 2008, has fulfilled this mission through the International Traffic System (STI), which is able to automatically recognize issued travel documents (MRTDs) within the ICAO PKD.

Brazil's use of the PKD system has enabled the PF to carry out much safer and faster migration control for Brazilian and foreign passengers entering and leaving the country. This has been a determining factor for the increase in international aviation traffic in Brazil in recent years.

Additionally, STI has made it possible to efficiently manage the human resources and materials available to carry out migration control activities, as well as to establish relevant public policies - in particular, the ongoing search for ways to reduce waiting times for passengers.

ADVANCED PASSENGER INFORMATION (API) AND PASSENGER NAME RECORDS (PNR)

In order to develop the safest and fastest migration control system possible, the PF sought to take full advantage of the possibilities offered by Annex-9 in order to obtain data on international passengers as far in advance as possible.

The API has been a reality in Brazil for international flights since 2013. The PF works with the PNAVSEC, the institution responsible for receiving such data from air operators and sharing it with other public institutions with "barrier" activities, so to speak.

Through the API, the PF has been very proficient in identifying passengers whose names are in the INTERPOL databases, which has generated significant positive results for migration control, as well as for airport security and the airport police.

In addition, by sharing the API data with the other national border agencies namely: Customs (Receita Federal - RF); Phyto-Sanitary Border Control (VIGIAGRO) and Health Border Control (ANVISA), PF has contributed in a decisive way to their results as well.

In this sense, it is worth mentioning the customs control of passengers that has been carried out by the RF since 2014, which has been mentioned previously in this magazine (Vol. 12, No. I, pp. 16-19), as well as the measures taken by the PF in conjunction with ANVISA during the last Ebola epidemic in West Africa in mid-2014.

For the PF, PNR offers great operational potential in coming years. It should be in place, in accordance with Doc 9904 once national and international regulatory and technical obstacles have been overcome.

THE BRAZILIAN ELECTRONIC PASSPORT

The Brazilian passports issued by the PF have been in compliance with the standards of ICAO, in accordance with Annex-9 (MRTD) and Doc 9303 (PKD) since 2008, including by obtaining and automatically comparing biometric data through the Automated Impression Identification System (AFIS).

After a transition period related to the expiration of previously issued documents, Brazil began issuing only electronic passports, which profoundly altered the perception of international security agencies in relation to Brazilian travel documents.

In fact, in the past, the great ethnic diversity that existed in Brazil made the Brazilian passport a target for international criminal organizations, which prejudiced the facilitation of Brazilian passengers on international flights.

With Brazil's participation in the ICAO PKD, Brazilian passports (MRTDs) are now recognized in e-gates - electronic gates for immigration control at airports in countries linked to this directory.

Another recent initiative by the PF (and also by the MRE) which conforms with Doc 9303, following the transitional period required for the expiry of previously issued documents, is the recent change in the validity of passports, from five to ten years, starting in 2014. This has been a major advance for the facilitation of Brazilian passengers on international flights.

AIRPORT SECURITY, AIRPORT POLICE AND INTERPOL

The PF has maintained its commitment to facilitation and has undertaken its activities related to AVSEC, the Airport Police and INTERPOL at airports in the most efficient manner possible.

Although not purely "barrier" or border activities (related to persons, baggage, cargo or aircraft and their international destinations) the inspections, searches and/or interviews related to the activities for security purposes can cause delays in international and domestic flights, directly or indirectly.

This is why the PF has sought to make the most of the API tools already available to it, as well as to pursue effective implementation of the API for domestic flights, in addition to the PNR (and possibly the Pre-Loading Advance Cargo Information (PLACI), still under study) for international and domestic flights. These actions will significantly increase the effectiveness of random inspections (based on risk analysis) or directed at persons, baggage, cargo, vehicles and aircraft (for suspicious situations) without significantly interrupting efficient traffic flows in the airport environment.

CONCLUSION

Brazil's modern and dynamic civil aviation system conforms to ICAO's international Standards and Recommended Practices (SARPs), with facilitation and security being the country's foremost strategic objectives.

The PF shares these objectives as it carries out its various duties in the airport environment. It follows the ICAO TRIP Strategy and makes every effort to guide its activities based on the responsible use of passenger data made available to it, as well to deal with Brazilian citizen/passenger identification in accordance with best practices.

FILIPPI PECORARO
Commissioner of Brazilian Federal Police,
Alternate Representative of
the Brazilian Delegation to ICAO

ICAO TRAINING PACKAGE:

CONTROL OF THE AUTHENTICITY AND VALIDITY OF TRAVEL DOCUMENTS AT AIRPORT BORDERS-LEVEL 1

INTRODUCTION

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 Border – Level 1". The initiative was undertaken through the Canada-funded project "Strengthening Travel Document Security and Identification Management in the Sahel and neighbouring States".

The ITP, a competency-based training course that is based on ICAO's TRAINAIR PLUS methodology, was developed by the Facilitation Section of the Air Transport Bureau, in partnership with the Global Aviation Training Office. Exams are used throughout the course to test trainees.

The target audience for the training includes front-line border control officers (mainly immigration officers) and their supervisors. Front-line border control officers play a critical role in national security by performing screenings of all passengers crossing borders; facilitating the movement of legitimate travellers; and identifying persons of interest.

BACKGROUND AND OBJECTIVES

In keeping with the TRAINAIR PLUS methodology validation process, the delivery of the ITP was validated. Fourteen actively engaged trainees participated in the first French language delivery that took place in Douala, Cameroon in 2016. The course was taught by two instructors, one who was a senior ICAO instructor and the other, an ICAO regional instructor, who served as a commissioner at the International Airport of Bamako, Mali *(for further information, refer to ICAO TRIP Magazine Vol.11 – N°2, page 34 to 36).*

CAPACITY BUILDING

This training course is intended to consolidate the competencies of front-line officers so that they can effectively examine travel documents and assess the intent of the travellers. Front-line border control and immigration officers play a critical role in screening all passengers who cross borders, and they expedite the movement of legitimate travellers while identifying high-risk individuals. The training aims to enhance participants' knowledge and skills in performing travel document examination and traveller risk assessment efficiently (refer to Course Delivery Framework).

The ITP also provides an opportunity to identity national experts who might become ICAO Qualified Instructors to deliver future trainings. Training-the-trainers is critical for capacity building in States and regions where the needs exist.

Since 2016, the objectives have been to increase the deliveries by ensuring the ITP is available in all of ICAO's official languages, and to ensure there are qualified instructors for each.

DELIVERIES

In 2017 and 2018, three training courses were held in the English language.

The two UN organizations' joint efforts to promote and facilitate the safe and orderly development of international civil aviation in global air travel and border and identity management, included the adoption of international standards for customs and immigration procedures. They assisted Member States in meeting the growing operational challenges of migration management, advancing the understanding of migration issues, encouraging social and economic development through migration and upholding the human dignity and well-being of migrants through efficient immigration and border management policies and structures in line with their respective mandates and stipulated in the Memorandum of Understanding (MoU) on identity and integrated border management programmes signed in November 2016.

The first session, held in Moshi, Tanzania, from 31 July to 4 August 2017, brought trainees from Tanzania, Kenya and Uganda together for the first ICAO and International Organization for Migration (IOM) joint training event.

The training was composed of two sessions: Part I – the ICAO Training Package "Control of authenticity and validity of travel documents at airport borders - Level 1" which was carried out by ICAO qualified instructors, and Part II - on the African Capacity Building Centre (ACBC) Passport Examination Procedure Manual II (PEPMII) and biometrics was conducted by an IOM ACBC expert.

Over and above this being the first joint training with IOM, delivery of this session provided an opportunity to validate the course in English, and it qualified instructors at different levels of their process.

The second session was held in Abuja, Nigeria, from 23 to 26 October 2017, with trainees from Nigeria and Ghana. A **third session** was held in New Delhi, India, with attendees from India, observers from Canada, and upcoming qualified instructors from France, Spain and Sudan.

In April 2018, the training course was provided in the French language in Niamey, Niger. Trainees from Burkina Faso, Chad, Mali and Niger attended the course. A representative from Burkina Faso was targeted as a future instructor and is now in the process to become an ICAO qualified-instructor for this ITP.

CURRENT STATUS

At the time of writing, six ITP training sessions were conducted with 96 trainees from 11 States in both English and French. The Spanish and Arabic versions were translated in late 2017, and will be validated in 2018. A total of 10 instructors have qualified or will finalize their qualification in 2018.

COURSE DELIVERY FRAMEWORK

The purpose of this course is to consolidate the competencies of front-line border control officers from immigration (and if applicable, other airport border control agencies) to examine travel documents effectively, allowing them to expedite the movement of legitimate travellers while identifying high-risk individuals. Trainees are taught concepts and techniques for visual, manual and machine inspection of travel documents and for inspecting security elements of a travel document.

LANGUAGE English, Arabic, French and Spanish

MAXIMUN PARTICIPANTS 10 for 1 instructor
11 to 20 for 2 instructors

DURATION 4 days

OBJECTIVES Upon successful completion of this course, participants will be able to:

- describe the basic elements of a travel document;
- identify 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.

TARGET POPULATION Front-line border control officers from immigration (and if applicable, other border control governmental agencies working at the primary line) who in charge of border controls in the airport environment ("National Authority"), specifically:

- border officers who are currently performing the job but have never received formal training on travel document examination;
- border officers who are currently performing the job and need a refresher; or
- border officers who are at the entry level, as part of their training curriculum; and
- direct supervisors (secondary line) of front line officers

HOSTING TERMS AND CONDITIONS

1. Authorization and nomination of participants

This ICAO Training Package (ITP) should be delivered nationally to a cohort of front-line officers and their direct supervisors (secondary line officers). Given the size of the target population within one State, it is recommended that the training be offered to more than one cohort consecutively, in order to optimize training costs (shipping, air fare, settlement of class room, etc.) Given that the training contains sensitive information and materials, trainees must be nominated by their Government.

The National Authority interested in having the course delivered to its officers should write to the ICAO Global Aviation Training (GAT) Office to confirm: 1) the number of participants to the training; 2) the availability of a minimum of 20 seized fraudulent documents (please refer to the next paragraph); and 3) the preferred dates for the training delivery.

2. Fraudulent travel documents

In order to achieve the course's objectives, this training includes hands-on exercises with fraudulent travel documents. These documents are to be provided by the National Authorities or relevant national agencies. The National Authority must confirm that a minimum of 20 seized fraudulent documents will be available to ICAO-qualified instructors for training purposes. The 20 documents will be rendered to the National Authority immediately after the end of the training by the instructors. An inventory list of the documents will be used for tracking purposes.

THE WAY FORWARD AND NEEDS

PLANNED TRAINING COURSES AND TRANSLATIONS:

In 2018, it is expected that validated delivery of the ITP will take place in both the Spanish language (in the South America region) and in Arabic (in the North Africa or Middle East regions). In parallel, the translation process in both Russian and Chinese will commence.

TRAINING MATERIAL:

To give trainees hands-on experience in the course, the ICAO Secretariat is soliciting support in obtaining specimens of national passports. The material donated to ICAO is strictly used for training purposes and remains in the training kits that are stored securely at the Secretariat.

The training needs in this field are high, and in many parts of the world; hence the importance of obtaining specimens from different regions.

The valuable contribution from States empowers trainees to identify real and fraudulent travel documents, and it further supports ICAO initiatives to enhance aviation security, facilitation and related border security aspects.

States willing to provide ICAO with specimen travel documents for this purpose should submit their proposal to the attention of the Director of Air Transport Bureau at the following address:

Director of Air Transport Bureau
International Civil Aviation Organization
999 Robert-Bourassa Boulevard
Montréal, Quebec H3C 5H7, Canada

For any questions on assistance projects related to the ICAO TRIP Strategy, please contact *fal@icao.int* or *aviationtraining@icao.int.*

BRAZIL SEMINAR STRENGTHENS TRIP IMPLEMENTATION

When he opened the TRIP Regional Seminar that took place in Brasília, Brazil in June 2018, the Director of ICAO's Air Transport Bureau, Mr. Boubacar Djibo, addressed the work that States and ICAO still have ahead of them to implement the coordinated activities needed to rectifying aviation security and facilitation deficiencies. He drew attention to the mutual agreement and pursuit of common goals and noted, "I am confident we will build an impressive record of progress in strengthening the global travel document system, and thereby enhance the security and facilitation of international civil aviation."

His remarks underscored the pivotal importance of the ICAO TRIP Strategy in protecting commercial flights and preventing illegitimate travel (including by foreign terrorist fighters), and in improving efficiencies with the civil aviation travel system as a whole. Generously hosted by the Government of Brazil, the Seminar provided a unique opportunity for encouraging full implementation of the Strategy among ICAO's 192 Member States. Brazil's Minister of Transport, Mr. Valter Casimiro Silveira, and Representative on the ICAO Council, Mrs. Mitzi Gurgel Valente da Costa, were in attendance, as was the Ministry of Foreign Affairs of Brazil's Undersecretary General for Economic and Financial Affairs, Ambassador Ronaldo Costa Filho.

The primary objectives of the ICAO TRIP Strategy involve strengthening interconnected State capacities that relate to establishing, protecting and managing citizen identity, and determining secure systems of travel document production and border control facilitation. These efforts also include ensuring the deployment of Machine Readable Travel documents (MRTDs) and modernizing border control management.

ANAC
AGÊNCIA NACIONAL
DE AVIAÇÃO CIVIL

The Director of ICAO's Air Transport Bureau went on to explain that the ICAO TRIP Strategy helps to harmonize the global line of defence in our shared battles: confronting international terrorist movements, cross border crime, and the many other threats to the safety and security of civil society and international aviation. The Strategy has been recognized for its contributions to United Nations Security Council Resolutions 2178, 2309, 2368 and 2396 that were adopted in 2014, 2016, and 2017. He further noted that the Security Council's Counter-Terrorism Committee has also stressed the important role of airlines in tracking the movement of high-risk passengers. More specifically, the Committee recognized the importance of national authorities sharing advanced passenger information (API) to help mitigate associated risks.

Advance Passenger Information (API) sharing, a key element of the TRIP Strategy, became mandatory under Annex 9 of the Convention on International Civil Aviation on 23 October of 2017.

Much progress remains to be achieved in terms of implementing the Strategy, particularly with the global implementation of API systems, but also in light of the fact that some non-MRTD passports continue to circulate despite the fact that their elimination became mandatory in 2015.

The TRIP Seminar in Brazil, contributed to deploying the available tools, and the Strategy as a whole. The Seminar also provided an opportunity for better understanding, and even undertaking,

"...the ICAO TRIP Strategy helps to harmonize the global line of defence in our shared battles: confronting international terrorist movements, cross border crime, and the many other threats to the safety and security of civil society and international aviation"

the complex coordinated action between the many government entities and other stakeholders that help to realize progress on these issues.

A great deal of progress has in fact already been achieved. As of today, most of ICAO's 192 Member States are fully compliant with ICAO's MRTD requirements, and there are more than 800 million ePassports that have been issued by more than 120 Member States, that are currently in circulation. If State participation in the ICAO Public Key Directory (PKD) increased, they would verify and authenticate their ePassports and fully capitalize on the security and facilitation benefits that ePassports are meant to deliver. T

THE TRAVELLER'S IDENTIFICATION PROGRAMME:

PERSPECTIVES IN THE AFRICAN REGION

As long as the scope and impact of terrorist activities varies in intensity in different regions of the world, and terrorists use legitimate travel documents to migrate globally, there will be a need for robust measures to counter their actions.

ICAO's Traveller's Identification Programme (TRIP) provides a strategy for strengthening the security of travel documents around the world. The roadmap for the programme is based on the global analysis of the Universal Security Audit Programme Continuous Monitoring Approach USAP-CMA results for Annex 9, and the associated technical manual Doc 9303. Though TRIP, and its components (i.e. PKD), represent a framework for robust security measures, it has not been implemented in a homogenous manner within and across regions.

In Africa about 21 States are issuing ePassports, but only five of those States are participating in the ICAO Public Key Directory (PKD). There is a significant gap between the number of States issuing ePassports and the number of PKD participants, and those States using PKD in day-to-day border control operations. In Annex 9 to the Chicago Convention, Recommendation 3.9.1 states that "*Contracting States issuing or intending to issue e-MRTDs should join the ICAO PKD*", and Recommendation 3.9.2 states that "*Contracting States implementing checks on e-MRTDs at border controls should join the ICAO Public Key Directory (PKD) and use the information available from the PKD to validate e-MRTDs at border controls*".

There is no doubt that any roadmap for the implementation of ePassports at the national level must consider participation in the PKD, if security and facilitation objectives are to be fully realized.

An ePassport (eMRTD) is only as good as the information contained on its chip. It requires an inspection tool, the ICAO PKD, to act as a central broker by managing the multilateral exchange of certificates and the certificate revocation lists used to validate the digital signature on the chip. Through the PKD, any attempt to alter the chip's data is immediately detected when checks are made. The PKD is recognized as a valuable instrument for implementing the specifications contained in Doc 9303, Machine Readable Travel Documents. These developments assist States in meeting their international obligations on issues that include the fight against terrorism, trans-border crime, and other threats against civil aviation.

Having a robust national identification management system is a pre-condition for security and facilitation benefits provided by ICAO-compliant MRTDs, eMRTDs and modern border control systems.

In an effort to improve implementation of ICAO Traveller Identification Programme (TRIP), in 2013 ICAO signed an MoU with the Economic Community of Central African States (ECCAS) to focus on:

- Promoting regional air transport security and facilitation cooperation between States;
- Cooperating to provide security assistance to States; and

- Promoting the Traveller Identification Programme and other initiations related to MRTD

To sensitize the region to these issues, a series of meetings, workshops, and seminars (including the TRIP Strategy Regional Seminar which took place in Nairobi, Kenya in November 2015), were held in Africa. These events have given rise to various sub-regional initiatives in Africa. An ECCAS High Level meeting was held in Brazzaville in May 2015 on the implementation of the ICAO TRIP. The event, which was attended by senior government officials from the eight ECCAS Member States, provided the opportunity to brief participants about the new developments on MRTDs and technical specifications.

The outcome of this High Level meeting included the signature of a common Declaration that addressed the issues States face as a first step towards developing a roadmap for facilitating travel in the ECCAS States. ECCAS called on ICAO and other partners to assist its Member States in a capacity building project for TRIP implementation that concentrated on the level of State services responsible for data management, security of travel documents and border control, as well as the fight against terrorism and transnational crime.

In line with numerous activities aimed at enhancing aviation Security and Facilitation in Africa, assistance to States under the ICAO TRIP Strategy began in the Sahel Region. The Government of Canada generously funded a technical assistance project that includes workshops, specialized training and technical assessment missions that address capacity gaps.

ICAO is partnering on this project with the UN Counter-Terrorism Committee Executive Directorate (CTED), in collaboration with the Economic Community of West African States (ECOWAS) and the International Criminal Police Organization (INTERPOL), among others. It is an excellent example of joint efforts linking States' needs, ICAO expertise, and essential resources provided by the donor community.

During the Meetings of Experts and Ministers in charge of Civil Aviation in the Region of the Economic Community of Central African States (ECCAS) that took place in April 2018 in Brazzaville, the Ministers decided to endorse the ICAO TRIP Strategy and the implementation of the Brazzaville Declaration that was adopted in May 2015.

There are various challenges facing the implementation of TRIP within the African region. While it is true that some States are further advanced than others, they all share commonality in the difficulties and

"While it is true that some States are further advanced than others, they all share commonality in the difficulties and hindrances that need to be overcome."

hindrances that need to be overcome. There is an overriding challenge of mobilizing funding for the required undertaking; be it from government sources or other alternatives.

On one hand, there is a lack of documentation to support citizenships, but there is also an ongoing complaint that agencies within these countries take a "silo approach" that impacts the implementation of digital identity as a whole. There are also technical challenges in implementing the system for those under 16 years of age, as their biometrics change rapidly. Another problem is that there are no integrations or links between current manual paper-based registrations and other ID-based systems (such as health management and driving licences).

In an attempt to address the broader picture at the continental level, as opposed to the piecemeal sub-regional steps, the African Union (AU) is nurturing the idea of a common African passport. The initiative, which was introduced at the AU Summit in Kigali, would allow for every African to eligible for the same centralized passport that would affirm the continent of Africa as their point of origin.

Having a common passport will make it easier: for Africans to travel within the continent; to cross border traders to conduct business; for employers to hire across borders; and for Africans to migrate to different parts of the continent for economic purposes. It will improve intra-African trade and will go a long way in easing the movement of domestic goods and services between Member States. T

ICAO

SECURITY & FACILITATION

TRIP-ICBWG

HAVING PROBLEMS READING PASSPORTS?

Millions of passports are issued every year. On rare occasions, passport authorities have issued passports with data formatting issues that create problems for immigration officials, airlines and the passport holder. This creates delays and unnecessary scrutiny of both the document, and the traveller carrying it.

WHAT ARE DATA FORMATTING ISSUES?

Data formatting issues might include the incorrect format or printing of the machine readable zone, discrepancies in the visual inspection zone, or errors in the data formatting within an ePassport's electronic Document Security Object (SOD). These issues are not always obvious to those inspecting the document.

If you have encountered a specific MRTD with a readability issue, the ICBWG can help.

THE SOLUTION

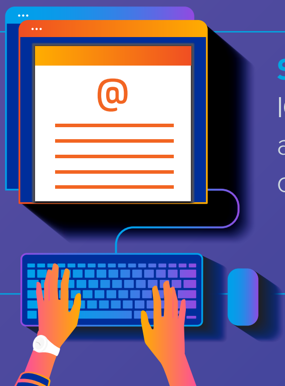
ICAO's Implementation and Capacity Building Working Group (ICBWG) monitors the conformance of machine readable travel documents (MRTDs) against the accepted international specifications contained in Doc 9303. Working with stakeholders in the travel continuum, the ICBWG has a subgroup dedicated to investigating suspected cases of non-compliance and assisting the issuing State to correct the problem.

HOW TO REPORT AN ISSUE?

The reporting process is simple:

STEP 1

Send an email to the *icbwg@icao.int* along with a brief description of the concern and an image of the data page. For issues related to ePassports, include the SOD.



STEP 2

ICBWG will assess the reported issue and supporting information in context of the Doc 9303 standards.