

ICAO TRIP

NEWS AND FEATURES ON THE ICAO TRAVELLER IDENTIFICATION PROGRAMME - VOL. 12 - NO. 2

MAKING BORDERS MORE SECURE

THE BENEFITS OF AUTOMATION

ALSO IN THIS ISSUE

EMPOWERING THE FUTURE WITH LEGAL IDENTITY

PARTNERING TO INTENSIFY TRIP STRATEGY
IMPLEMENTATION

THE EVOLUTION OF THE ePASSPORT

RISK ANALYSIS FOR AIRPORT SECURITY

THE UNODC AIRPORT COMMUNICATION PROJECT



ICAO

SECURITY & FACILITATION



**Two eyes are
better than one**

Thanks to the KINEGRAM visual and machine authentication is more secure.
Learn more at kinegram.com.

OVD Kinegram AG | Zaehlerweg 12 | CH-6301 Zug | Switzerland
www.kinegram.com | mail@kinegram.com | A KURZ Company

KINEGRAM®



ICAO

ICAO TRIP MAGAZINE
VOLUME 12, NUMBER 2, 2017

Editorial

TRIP Programme—Aviation Security
and Facilitation Policy Section
Editor-in-Chief: Narjes Abdennebi
Tel: +1 (514) 954-8219 ext. 8374
E-mail: fal@icao.int

Coordinators: Hubert Gattet and 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

Harvey Wong, Advertising Representative
Tel: +1 (514) 954-8219, ext. 6181
Fax: +1 (514) 954-6769
E-mail: hwong@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

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

Copyright © 2017
International Civil Aviation Organization

Printed by ICAO

Contents

3

Message from the Editor-in-Chief

Narjes Abdennebi looks at how regional collaboration can improve security and facilitation

4

Traveller identification Programme (TRIP) Strategy

The roadmap for key components in travel facilitation and aviation security

8

Moving Towards Automated Border Control (ABC)

The history, benefits and future of automated border control

12

Developing Harmonized Automated Border Control Training Capabilities

Frontex, the European Border and Coast Guard Agency, develops a two-tier training programme after working for more than 10 years to harmonize ABC practices

16

The Future Empowered with Legal Identity

Over a billion individuals around the world have minimal or no recognition of their existence. Sanjay Dharwadker focuses on the elements required to harmonize, modernize and establish their legal identities

20

IOM's Commitment to Intensified TRIP Strategy Implementation

A look at the strategic ways the IOM is supporting ICAO to increase ICAO TRIP implementation around the world

27

ICAO's TRIP Regional Seminar in Hong Kong SAR, China

Highlights from the event hosted by the Civil Aviation Department of Hong Kong in July 2017

30

The Evolution of the ePassport

Jasper Mutsaers and Justin Ikura describe how next generation ePassport technologies will allow for seamless travel across international borders

34

ICAO Partner Brief – IATA

As IATA's Control Authorities Working Group (CAWG) celebrates 30 years of working together to recommend solutions and best practices for border management, they extend an invitation to new and returning members

36

Risk Analysis for Airport Security in the Context of European Community (EC) Legislation

Charles de Couessin examines how current EC legislation impacts airport checks and passenger facilitation and whether new solutions could improve airport security

40

AIRCOP: The UNODC Airport Communication Project

Partnering with INTERPOL and the World Customs Organization (WCO), The United Nations Office on Drugs and Crime (UNODC) implements the Airport Communication Project to strengthen the ability of airports to detect and intercept illicit trafficking

44

The Dutch National Verification Solution for eDocuments

Cor de Jonge and Jeen de Swart describe the State architecture and infrastructure that is needed for a National Public Key Directory (NKPD) that would securely verify various identification eDocuments



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)

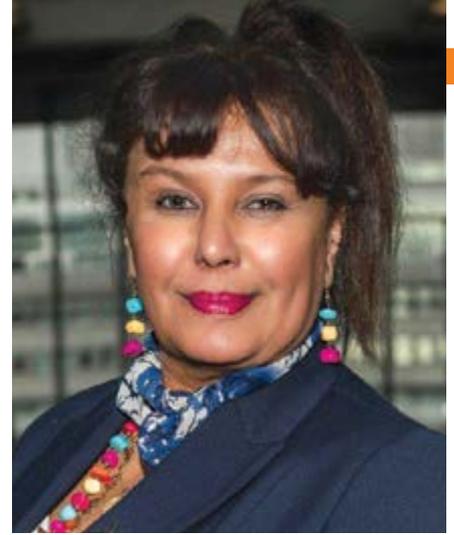
United Nations High Commissioner for Refugees (UNHCR)

United Nations Office on Drugs and Crime (UNODC)

World Tourism Organization (UNWTO)



BETTER TRAVELLER IDENTIFICATION MANAGEMENT FOR ENHANCED BORDER CONTROL INTEGRITY



 Endorsed by the 38th Session of the ICAO Assembly, ICAO's Traveller Identification Programme (TRIP) Strategy provides a framework for enhancing aviation security and facilitation by bringing together the relevant elements of identification management. It also builds on longstanding ICAO leadership on matters related to Machine Readable Travel Documents (MRTDs).

To assist Member States with the task of uniquely identifying individuals by enhancing the security of their travel documents and securing their border integrity, a TRIP implementation roadmap was developed. Supported by the Air Transport Committee (ATC) during its 210th Session, the roadmap was the result of Assembly Resolution A39-20, *Consolidated statement of continuing ICAO policies related to facilitation*. It provides guidance on the entities responsible at the national level, for the implementation of the ICAO TRIP Strategy, through a National Air Transport Facilitation Committee or a similar coordinating body.

Within the framework of this roadmap, Member States are required to coordinate with all entities involved in traveller identification matters, through national focal points, to achieve the "implementation actions". This includes completing the compliance checklist with Annex 9 provisions linked to the ICAO TRIP Strategy (48 Standards and Recommended Practices) and certifying that all interoperable applications are fully functional.

There is a need for ensuring national coordination and international cooperation for each dedicated action linked to effective implementation of the ICAO TRIP roadmap. This was highlighted throughout the TRIP Regional Seminar and Exhibition that was held in Hong Kong SAR, China in July.

National coordination and international cooperation is highlighted in this issue through the work of various International Organizations: the IOM (International Organization for Migration)'s commitment to intensified ICAO TRIP Strategy implementation; as the International Air Transport Association (IATA) Control Authorities Working Group celebrates 30 years of government and industry partnership and with the United Nations Office on Drugs and Crime (UNODC) and their Airport Communication Project (AIRCOP).

Strong identify authentication is the foundation for secure and efficient travel document and border control. It must rely on robust legal identity systems that provide reliable evidence of

identity, which is effective for enhancing security. Around the world there are many cases where there is a lack of strong identity authentication, particularly with data that is collected online.

The INTERPOL Stolen and Lost Travel Documents (SLTD) database, which was created to ascertain the validity of travel documents at border control points, is one of the interoperable applications that forms the basis of the ICAO TRIP Strategy. The ICAO Assembly encouraged Member States to report lost and stolen passports to the database on a regular basis, to protect the security and integrity of passports; to enhance international cooperation to counter threats to civil aviation; and to prevent the use of travel documents for acts of unlawful interference against civil aviation.

In this regard, Member States have been urged to implement the two SLTD-related provisions incorporated into Annex 9 in 2015. Accordingly, ICAO is gathering information on the worldwide application of these provisions to determine what further action, if any, may be taken to promote implementation.

New electronic travel documents must be aligned with national architectures, infrastructures and organizations that allow electronic verification containing a National Public Key Directory (NPKD) and certificates for various e-documents.

National verification brings us closer to Automated Border Control (ABC). While the introduction of ABC systems at an airport may entail substantial investment, there are associated long-term returns (i.e. improvements in security, clearance speed and accuracy of verification) that will be provided by the systems. To support this, FRONTEX has developed harmonized training capabilities in the area of automated border control solutions in the European Union. The next step will involve the evolution of eDocuments that will include digital storage of travel information (visas and stamps) after the document issuance.

Your feedback and suggestions for articles and themes for future issues are always welcome. Feel free to send contributions and comments to ICAOTRIPmagazine@icao.int or directly to your contact at ICAO. We look forward to seeing you at the ICAO TRIP Symposium and Exhibitions in October as well as our upcoming Regional Seminar in Jamaica at the end of November and at the dedicated API and PKD workshop. Until then, happy reading! ■



TRAVELLER IDENTIFICATION: THE KEY COMPONENT IN BOTH TRAVEL FACILITATION AND AVIATION SECURITY

 Following the successful introduction of MRTDs in the eighties, which dramatically enhanced the security features used in passports, ICAO began implementing an initiative that improved both the overall integrity of travel documents and the processes involved in their issuance, as well as security at border control.

THE IMPORTANCE OF RELIABLE AND SECURE TRAVELLER IDENTIFICATION

The ability of terrorists and criminals to operate with anonymity—beyond the knowledge or suspicion of the relevant State and international authorities about their true identity and movements—is a powerful tool and weapon in enabling those with ill intents to further their unlawful and illegitimate activities.

Conversely, the ability of authorities to confirm the true identity and monitor certain movements of travellers—and to do so speedily, cost-effectively, securely and responsibly—is vital for a wide range of purposes:

- maintenance of effective national and global security;
- facilitation of personal and business travel and trade;
- determination and discharge of treaty and other obligations and rights related to the cross-border movement and admission of people;
- cost-effective deployment of security and border admission and clearance personnel and resources on a risk-management basis;
- detection and prevention of crime, including money laundering, smuggling, illegal drug trade, child abduction and human trafficking

DRIVERS FOR ENHANCED TRAVELLER IDENTIFICATION

There are many factors and trends that support the sharing of knowledge, insights and technologies amongst diverse States and international authorities with mandates and interests in the issuance and/or use of traveller identification.

There is strong consumer and business pressure for expedited travel, trade and tourism, and corresponding public resistance to security, border control and other processing activities that add avoidable costs, delays, and restrictions to movement. Conversely, security threats in many sectors—including, but not limited to, the aviation sector—are real, significant and continuously evolving.

In the meantime, innovative technologies and protocols offer new opportunities for the cost-effective deployment of security resources where they are most needed, based on risk-management principles, thereby enhancing both security and facilitation objectives.

In that context, the ICAO Traveller Identification Programme (ICAO TRIP) Strategy was approved by the ICAO Council and endorsed by the 38th Session of the ICAO Assembly in 2013. The TRIP Strategy aims to enhance the integrity of the passport-issuance process and to ensure robust identification-management processes in order to prevent exploitation by terrorists and maximize the effectiveness of border security and the benefits of enhanced facilitation of travel across borders.

The efforts of ICAO to ensure the legitimacy of secure travel documents depends on a holistic and integrated approach to the

traveller identification-management and issuance process. The integrity of travel-document issuance is severely compromised if appropriate safeguards are not incorporated in the traveller-identity management process to ensure confirmation of the identity of the individual to whom the passport is issued.

NATURE OF A ROBUST IDENTIFICATION MANAGEMENT

For this Strategy, a comprehensive and cohesive approach to traveller identification entails five closely linked and mutually-complementary identification management activities:

1. **EVIDENCE OF IDENTITY:** ensure authenticity of the identity of an applicant seeking issuance of a travel document, confirming for that individual a unique identity linked to the applicant, the identified individual’s status as still living and the applicant’s status as an active user of that unique identity.
2. **MACHINE-READABLE TRAVEL DOCUMENTS (MRTDs):** ensure that the design and manufacture of standardized machine-readable passports (MRPs), visas, and identification (ID) cards for travel that meet internationally-accepted standards and practices with respect to global interoperability and effective biometrics as well as high integrity against counterfeiting and forgery.
3. **DOCUMENT ISSUANCE AND CONTROL:** implement effective processes and protocols for the issuance of MRTDs to authorized holders only, including emergency issuance where warranted while ensuring the security against theft, tampering and loss.
4. **INSPECTION SYSTEMS AND TOOLS:** Implement technologies, supporting infrastructure, information-sharing and related protocols and procedures to support timely, efficient, secure and reliable reading of MRTDs at borders and verification of the validity of the MRTD for the holder, including by the use of the ICAO Public Key Directory (PKD) to confirm that e-passports

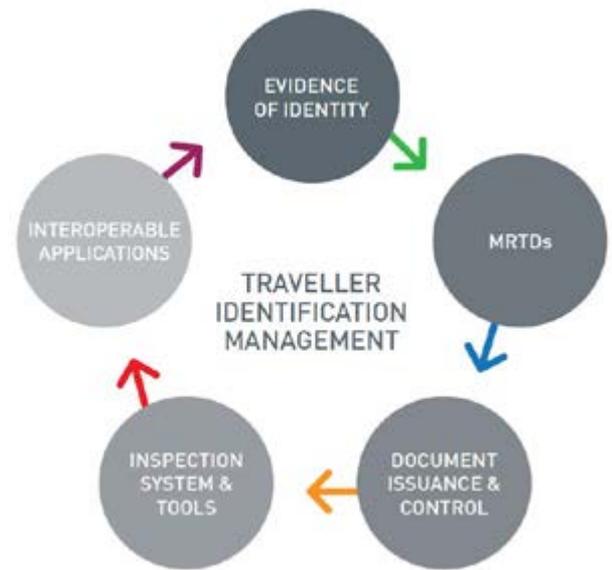


FIGURE 1 – The five elements of the ICAO TRIP strategy

presented to authorities remain legitimately-issued and active (i.e., not lost, stolen, compromised or revoked).

5. **INTEROPERABLE APPLICATIONS:** Implement systems, technologies and protocols that provide for the ready, secure and reliable linkage of MRTDs and their legitimate holders to relevant intelligence and information about the holder and/or his/her background, movements and actions of interest, in support of security and travel facilitation. Interoperable applications include such functions and linkages Passenger Name Record data (PNR), Advance Passenger Information (API), State-managed security “watch lists” and State-recognized “known,” “trusted” and/or “expedited” travellers and shippers (or equivalent).

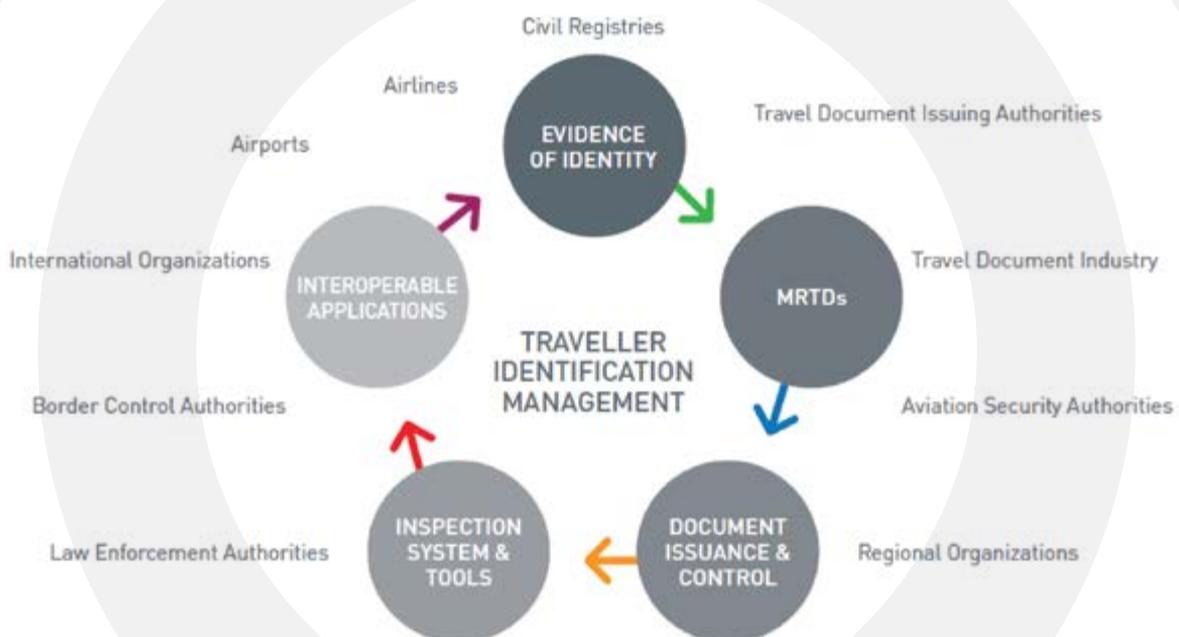


FIGURE 2 – Different stakeholders involved in the ICAO TRIP Strategy

MAIN CHALLENGE: INVOLVEMENT OF DIFFERENT STAKEHOLDERS

As shown in Figure 2, a wide array of Contracting States and other regional and international entities have mandates and interests in traveller identification that include: civil registries, passport issuance, visa issuance, security, trade and tourism, immigration/migration, border controls, law enforcement, treaties—human rights, refugees, stateless persons, special events (i.e. the Olympics, G7/G20) and emergency situations where victims and survivors have to be identified.

All Contracting States have mandates for efficiently and effectively operating their immigration/migration, trade, travel, tourism and border control functions, and all of these require secure, reliable and efficient traveller identification.

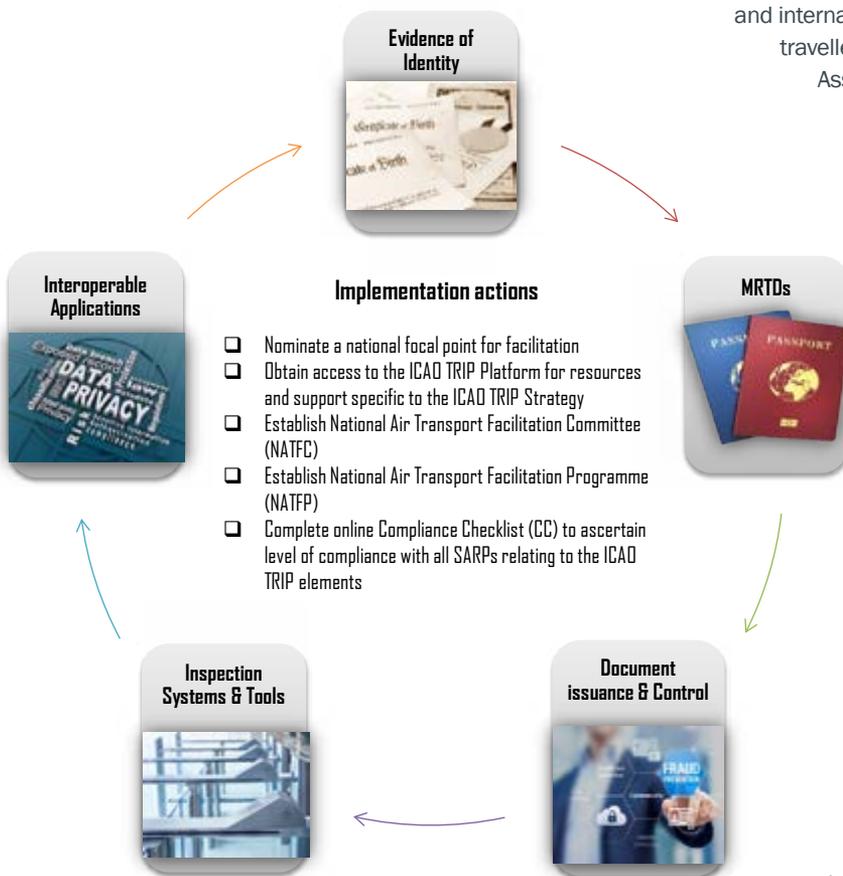
There are also individual travel document applicants and holders who use formal travel documents (most notably passports) for a wide range of purposes beyond border crossing and international travel. These include routine transactions where credible sources of identification are either required or expeditious, such as banking, currency exchange, vehicle and equipment rental, domestic travel, and application processes for access to civil programmes, services and benefits.

The need for secure travel documents and related technologies, tools and processes, extends well beyond the world of international civil aviation. A diverse array of travel document issuers and users require, and will benefit from the leadership, engagement, support and/or collaboration and cooperation of ICAO.

Notably, travel documents and related technologies and processes that meet the needs and standards of international civil aviation security and facilitation will also typically meet other diverse identification needs and standards, with respect to security, functionality, credibility, interoperability and efficiency. In some cases ICAO-compliant travel documents can be directly used for such other applications. In others, ICAO’s knowledge, technologies, insight and experiences in the production, management and use of secure identification documents, tools and processes can be shared, and efficiently adapted and applied to the needs of other travel document issues and users.

THE NEED FOR A TRIP ROADMAP TO ASSIST STATES IN THEIR IMPLEMENTATION EFFORTS

The 39th Session of the Assembly endorsed the priorities for the ICAO TRIP Strategy and expected outcomes for the 2017-2019 triennium. Assembly Resolution A39-20, *Consolidated statement of continuing ICAO policies related to facilitation*, identified national and international action in ensuring the security and integrity of traveller identification and border controls. Specifically, the Assembly urged Member States, through their travel document and border control programmes, to uniquely identify individuals to maximize security and facilitation benefits, including preventing acts of unlawful interference and other threats to civil aviation. Furthermore, the Assembly endorsed the development of a roadmap for the implementation of the ICAO TRIP Strategy.



The ICAO TRIP roadmap has been developed in the context of the *No Country Left Behind* initiative but also in light of the two UN Security Council resolutions 2178 and 2309 that were approved in 2014 and 2016 respectively. The two resolutions address the acute and growing threat posed by foreign terrorist fighters (FTF). The relevant parts of the resolution are: “Reaffirms that all States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents...” and “..calls upon all States to require that airlines operating in their territories provide advance passenger information to the appropriate national authorities in

FIGURE 3 – Mechanism required for facilitation matters

order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015);”

The UN Security Council has mandated States to *require* as the resolution states, advance passenger information from airlines in order to match passenger data against the UN Security Council’s travel ban lists for terrorists.

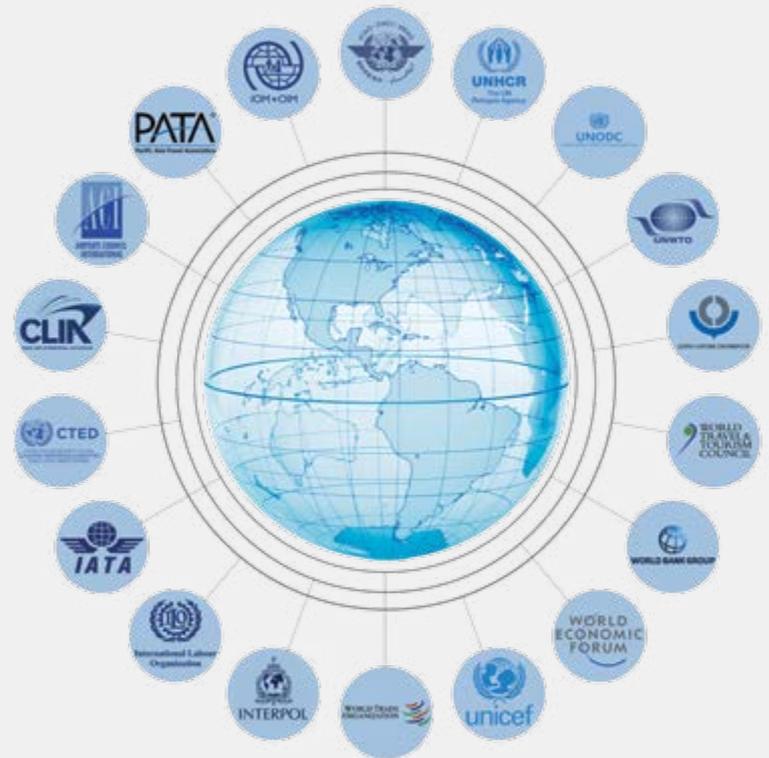
Following resolution 2178, the UN counter-terrorism bodies also included a non-binding recommendation on the use Passenger Name Records (PNR), encouraging airlines to provide them, where appropriate, to the appropriate national authorities. Since most foreign terrorist fighters use legitimate travel documents, the use of PNR will allow States to better understand travel patterns of terrorist fighters, and to share practices in evidence-based traveler risk assessment and border screening. It is likely that more States will begin to demand PNR data as well.

Clearly resolutions 2178 and 2309 have increased the political and legal impetus for States and airlines to implement passenger data exchange programmes, while it is noteworthy that under Annex 9 – Facilitation, the API/PNR aim is to provide target milestones for the implementation by States of the ICAO TRIP Strategy.

The ICAO TRIP roadmap is primarily based on the global analysis of the Universal Security Audit Programme Continuous Monitoring Approach (USAP-CMA) results for Annex 9 security-related Standards and Recommended Practices (SARPs) from 178 second-cycle audit results. When implementing the TRIP roadmap, Member States will first need to continue focusing on implementing the TRIP-related SARPs in Annex 9 and the associated technical specifications for machine readable travel documents contained in Doc 9303. The Secretariat identified 48 SARPs in the fourteenth edition of Annex 9 that relate to the elements of the TRIP Strategy.

At the national level, implementation of the roadmap will require coordinated action between many government and industry entities, such as passport issuing offices, aviation security authorities, civil registries, border control and law enforcement agencies, airlines, airport authorities, the travel document industry, immigration authorities and other interested parties. The mechanism and requirement for coordination on matters relating to facilitation already exists in Annex 9, through national air transport facilitation programmes and their related committees (shown in Figure 3).

Governments, pursuant with their laws, regulations and national programmes on aviation security, and according to the relevant ICAO SARPs, will seek to develop appropriate legislation enabling them to implement effectively the ICAO TRIP Strategy. In the international context, the aim is to systematically collaborate with all interested stakeholders to implement each element of the TRIP Strategy.



International Cooperation: key for successful implementation

Importantly, ICAO’s leadership is essential to the success of the achievement of this roadmap. The focus must be on enhancing aviation security and improving facilitation with the objective of providing States with a blueprint that sets out the elements that must be in place in order to move, for example, from Machine Readable Passports (MRPs) to ePassports, and possess excellent breeder documents and sufficient financial resources.

To this end, there is a need for ensuring both national coordination and international cooperation for all actions are linked to effective implementation, with a view to achieving the effective implementation of the ICAO TRIP roadmap. By definition, this is a constantly-changing and evolving work effort which is supported by the guidance published.

There are a number of broader cross-cutting initiatives that are being pursued. This most notably includes those dealing with outreach to all involved stakeholders, promotion of the integrity and benefits of secure traveller identification, expansion of assistance and capacity building efforts for States in need, and enhancement of assessment missions and assistance from the Regional Offices. ■

MOVING TOWARDS AUTOMATED BORDER CONTROL (ABC)



FAGBEMI OLUWAGBEMIGA

He is currently on secondment to ICAO as a Facilitation Officer under the ICAO/AFCAC Human Resources Development Funds (HRDFs) Programme. He is the Chief Air Transport Officer in the Directorate of Air Transport Regulation of the Nigeria Civil Aviation Authority responsible for ensuring and enforcing ICAO compliance of SARPs Annex 9 – Facilitation by Aviation service providers.



Air transport is an essential driver of economic, social and cultural development around the globe. Though it brings important growth that is projected to continue, as air traffic volumes increase, there will be greater facilitation and security challenges. While the potential benefits of this growth might be far-reaching, there is a good chance they won't materialize unless we create an economically sound global air transport system for all stakeholders.

To facilitate and expedite the clearance of persons entering or departing a State by air, there is a need for adopting border control regulations that are appropriate to the air transport environment, and applied in a manner that prevents unnecessary delays of the travelling public. When developing procedures that will be efficiently applicable to border controls on passengers and crew, ICAO Member States apply aviation security, border integrity, narcotics control and immigration control measures, where appropriate.

It is a fundamental precept, when developing these standards, that public authorities are to facilitate inspection formalities for the vast majority of air travellers. That authorities must have a satisfactory level of confidence in the reliability of travel documents, and in the effectiveness of inspection procedures, brought the concept of specifications into the production of travel documents.

Having standardized specifications for travel documents and the data contained therein builds confidence. Developing standard specifications for passports and other travel documents follows the tradition established by the League of Nations Passport Conferences of the 1920s and the work of the League's successor, the United Nations Organization. The mandate to continue with the leadership role was bestowed on the International Civil Aviation Organization from the Convention on International Civil Aviation (the "Chicago Convention") which covers the full range of requirements for efficient and orderly civil aviation operations, including provisions for clearance of persons through border controls.

In 1998, the establishment of the most effective biometric identification system and associated means of data storage for use in the application of machine readable travel documents (MRTDs), was facilitated by the sub group New Technologies Working Group (NTWG) of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP). After the events of September 2001, States attached greater importance on the security of a travel document and the identification of its holder. Any public authority aiming to facilitate inspection formalities for the vast majority of air travellers must have a satisfactory level of confidence in the reliability of travel documents and in the effectiveness of inspection procedures.

In 2003, ICAO adopted machine readable travel document (MRTD) specifications for passports that included an embedded chip containing the bearer's personal



identification data and photo. A new Standard was approved in 2005 that all States must begin issuing machine readable passports (MRPs) in accordance with ICAO Doc 9303 no later than the year 2010, and by 2015 all non-machine readable travel documents must expire.

In 2004, the 35th Session of the ICAO General Assembly affirmed that cooperative work on specifications to strengthen the security and integrity of travel documents should be pursued by the Organization as a matter of high priority. Some deficiencies were found to be associated with MRTDs:

- Proxy issuance: non-physical appearance of the applicant;
- Multiple issuance: applicants could go to different centres to acquire;
- Identity theft: tempering alteration of age, pictures and pagination;
- Security features: generally weak.

These deficiencies led to the introduction of biometric ePassports in 2007 with embedded electronic chips that stored the photograph and other personal information found on the passport data page. A State-specific digital security feature derived from the State's security certificates (i.e. Document Signer Certificate (DSC) and Country Signing Certificate Authority (CSCA) certificate) was also stored in the chip. These digital signatures are unique to each State's ePassport and can be verified using the public key information of the passport-issuing State. To validate an ePassport, a State is required to join the ICAO Public Key Directory (PKD).

ICAO's PKD and ePassports provide a means of automating border control without requiring pre-enrolment in a separate programme. ABC gates require the use of a biometric, such as facial recognition, to confirm the identity of the traveller. The chip in the ePassport includes the facial photograph of the document holder.

When a border control system performs ePassport validation through ICAO's PKD, which confirms the authenticity and integrity of the data on the chip, the system can confidently rely on the photograph for facial recognition. The use of a fully compliant, contactless integrated chip (IC) in an eMRTD offers excellent possibilities for machine authentication. However, machine authentication using the contactless IC may fail if it is defective. And it is not successful if there are no certificates available for checking the authenticity and integrity of the data on the contactless IC.

Consequently, there is the need for an alternative machine authentication. This is especially relevant in ABC scenarios where the machine reader is used instead of a border official to read and validate the eMRTD. This alternative machine authentication establishes trust in the data used for decisions at the border.

TRAVEL DOCUMENT INSPECTION USING ABCS

According to industry reports, the expansion of ABCs used for inspecting of traveller documents increased between August 2014 and November 2015 from availability in 134 airports in 40 States to 159 airports in 45 Member States. Border agency involvement is a key focus for the ICAO TRIP Strategy.

Expanding the use of ABCs in airports as a means for verifying and authenticating ePassports will enhance security in cross-border movements and facilitate the clearance of passengers. Introducing ABC machines at an airport may entail a substantial investment in relation to costs, regardless of the size of the airport, but there are associated returns in the long run. Improvements in security, clearance speed and verification accuracies are some examples of the benefits the system will provide. It might be easy to quantify the costs in a monetary term, while the expected benefits might be difficult. In the long run, the multiplier effects of the benefits stand to outweigh the costs.

ABCs can even be developed in a strategic way, incorporating various border control agencies. Although the level of cooperation among border control agencies has been variable in a number of States, cooperative efforts can help rationalize procedures, save on manpower and other resources, and facilitate passengers. Such cooperation can result in the clearance process for passengers being reduced in complexity to a level where a single border control officer will be able to process a vast majority of arriving passengers. The officer, representing the various interested agencies, is tasked with conducting a primary inspection of each arriving passenger and referring those requiring additional examination to the appropriate service.

With increasing inter-agency cooperation, the case for developing single inter-agency automated systems, serving the needs of two or more agencies, becomes more compelling. The concept of a single border control officer for all initial and simple controls has been a major passenger facilitation improvement in order to avoid the complexity of a passenger queuing separately to pass multiple border inspections.

The ABC touch points are used by travellers in a self-service way, utilizing biometrics (facial recognition, fingerprint and/or iris) as main identification tokens. This will help speed up traveller processing, decrease waiting times and generate a positive traveller experience at the border.

BENEFITS OF AUTOMATED BORDER CONTROL SYSTEMS

An ABC system ensures the satisfaction of all parties; passengers, airports, airlines, border control authorities, etc. when it comes to border controls. The benefits are enormous. Highlighted below are some of the benefits associated with its introduction:

- ABCs offer the highest security levels at key moments of the passenger journey. eGateway technology is a contactless, biometric passenger identification gateway. It also offers automatic verification of optical security features, electronic security chips, machine readable zone checks, pattern checking under different types of light and security paper checks. It features a full, contactless journey obtaining a facial image on the fly, while the passenger walks naturally, but without eliminating the travel document from the equation.

“Passenger processing is significantly more efficient, waiting times are reduced and more can be processed, in parallel.”

- ABC solutions offer an integrated two-step approach to eGates that combines document reading with biometric verification. Both the requirement for paper documents, such as passenger manifests and embarkation/disembarkation cards and the administrative costs associated with the related manual procedures, are eliminated.
- It reduces transfer times and speeds up arrival and departures.
- The multi-technology approach of these systems enables them to provide far more than evidence of an individual’s personal identity based on their eDocument.
- The holder’s biometric data stored in the chip enables the automation of processes such as border control, making it faster and more convenient.
- ABCs turn border control checks into a simple, intuitive process that any passenger can carry out themselves in just a few seconds. Identification is conducted in a few seconds, without compromising the biometric capture quality or matching accuracy of the single token.
- It provides travelers with a walkthrough identification experience, eliminating stops and direct interaction with officers.
- Passenger processing is significantly more efficient, waiting times are reduced, and more can be processed, in parallel. It is quicker and more convenient for travelers.
- A seamless journey provides a smooth and continuously integrated passenger-centric flow, combining data from different systems to deliver the highest level of security and a modern travel experience to travelers.
- It enables a streamlined, one-solution approach to all touchpoints. With the eGateway technology available to all travellers, it adapts itself to each passenger’s unique behavior and features, and automatically activates alternative identification methods if needed.

CONCLUSION:

Introducing automated border control machines at airports may entail a substantial investment in relation to costs, but there are associated returns in the long run that include improvements in security, clearance speed and verification accuracies that the system will provide. ■

MÜHLBAUER SECURITY®

COMPREHENSIVE GOVERNMENT SOLUTIONS



You need a partner who provides reliable identification for your citizens and secure solutions creating trust and confidence. You are looking for the individuality and the flexibility you need.

We strongly believe in the importance of comprehensive and holistic identity programs in order to increase the integrity of national identification. Our solutions therefore focus on finding an optimized solution for your national ID program, whilst meeting all your requirements.

Mühlbauer – Your Partner for Your National ID Program



DEVELOPING HARMONIZED AUTOMATED BORDER CONTROL (ABC) TRAINING CAPABILITIES



TOM VAN DER HOR

He is a research officer who works for the Research and Innovation Unit of Frontex. He is currently involved in the 'Harmonization of EU Border Control Capacities' project, focusing on promoting common practices between EU member states and identifying capability needs to support the development of best practices and recommendations in the area of border control. He holds an MSc in International and Comparative Criminology and an MA in Politics and Society.

Frontex, the European Border and Coast Guard Agency, promotes, coordinates and develops European border management in line with the EU fundamental rights charter and the concept of Integrated Border Management (IBM). The Agency is responsible for effectively facilitating and rendering the application of the existing and future EU measures that relate to the management of external borders, with a view to contributing to an efficient, high and uniform level of control.



Global traveller flows in air travel have been rapidly increasing and are expected to continue to grow in the years to come. In the European Union (EU) the total number of regular air border crossings is forecast to rise to 602 million in 2025, and many of these movements will be made by non-EU nationals. These developments increase the pressure on EU member states' to successfully process large volumes of travellers, making it increasingly difficult to rely solely on traditional means of border control for assuring both a steady flow of travellers crossing the border, and at the same time, maintaining requisite security levels. To this end, new and innovative border management solutions are being explored and developed to effectively tackle these and other emerging challenges.

One innovation – though not new – is Automated Border Control (ABC) systems. ABC systems have proven to be efficient and reliable tools in the border check process, and are being extensively deployed throughout the EU. Based on data provided by EU member states to Frontex in December 2016, ABC systems are currently operational in 16 member states, primarily at international airports. Another three EU member states have launched pilots, and an additional 10 are planning for the deployment of ABC systems in the near future. These systems play an increasingly important role in the development and delivery of effective and efficient border management capabilities.

FRONTEX AND ABC SYSTEMS

Frontex activities in the area of ABC are well-established and date back more than 10 years. During this period the Agency has worked to achieve harmonization of practices, similar passenger experiences and consistent security levels in the use of ABC systems, by offering support and expertise to EU member states and external stakeholders. In 2014, while witnessing a significant expansion of ABC systems worldwide and a growing interest in their deployment in Europe, Frontex identified the need for developing harmonized training capabilities in the area of ABC. This resulted in the development of a two-tier training programme: an intermediate-level training for

first line border guard officers; and an advance-level training for project managers and experts specialized in ABC systems.

1. AUTOMATED BORDER CONTROL (ABC) SYSTEMS FOR FIRST LINE OFFICERS:

this intermediate-level training acknowledges the importance of ensuring border guard officers in the field receive the proper training and up-to-date information about the border checks processes with the use of ABC systems. The training provides first line officers with a clear understanding of the complex landscape of ABC procedures and functionalities, focusing on the principles of ABC systems, operation of ABC gates, the role of biometrics in identity verification systems, and the associated risks and vulnerabilities.

2. VULNERABILITY ASSESSMENT AND TESTING FOR AUTOMATED BORDER CONTROL (ABC) SYSTEMS:

this advance-level training has been developed for project managers and experts specialized in ABC systems to teach them the concepts and basics of vulnerability assessment in relation to ABC systems to enable them to identify system security weaknesses, develop proper risk management procedures, and propose appropriate mitigation strategies.

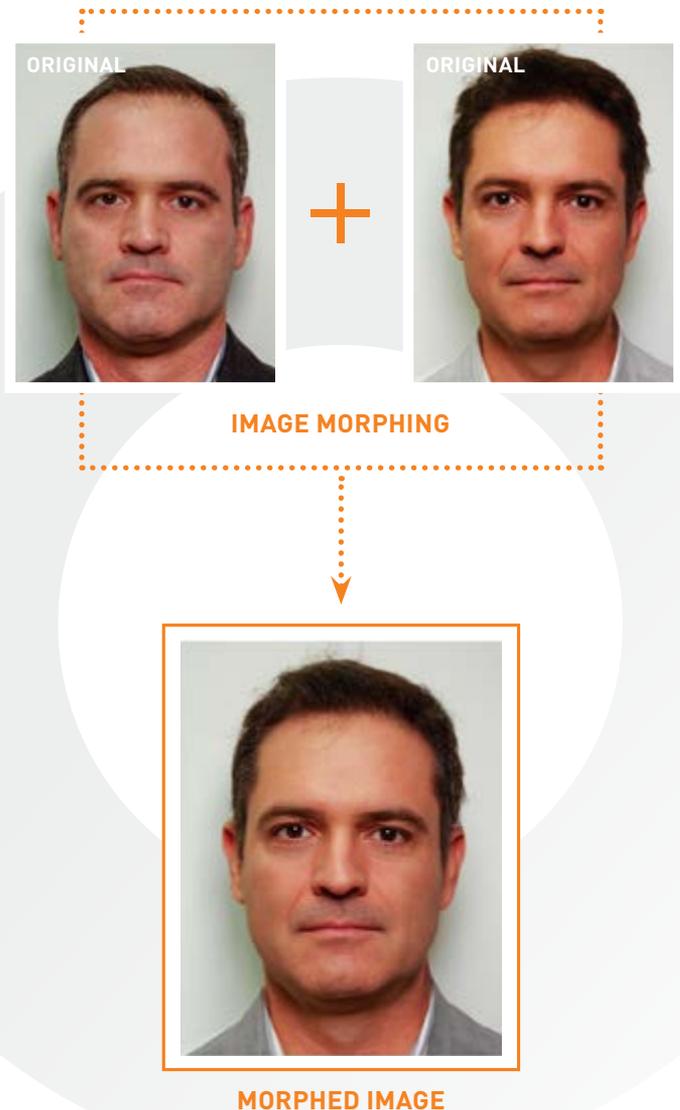
Both training programmes include training manuals and practical class-exercises, as well as a self-directed online training, followed by a self-assessment test. Though the content of the two training programmes are too extensive and detailed to discuss in this article, the implementation of the ABC training in the EU has helped put a focus on a number of interesting topics which are worth mentioning.

IMAGE MORPHING

Since ABC systems have been around for several years, many of the known vulnerability points in the ABC systems have been well-documented. Image morphing, on the other hand, is a relatively new and understudied phenomenon, with the potential for major implications in both automated and manual border control.

Image morphing is an image processing technique used to compute a transformation from one image to another (i.e. an “image morph”) that can be achieved for the face, iris and fingerprint. For face images, fraudulent applicants submit a morphed image to the document issuing authority at the start of an enrolment procedure, in an attempt to obtain a genuine travel document. This is known as a morphing attack. If the attempt is successful it may allow more than one individual to cross the border, giving opportunities for wanted criminal offenders to use an authentic passport to enter a country under a false identity.

Training for the vulnerability assessment and testing for ABC systems included a sample study on the topic of image morphing, conducted in cooperation with the German Federal Office for Information Security (BSI). The study used morphing software readily available in the market, and one of the top-three face recognition algorithms



for computing matching scores. The results demonstrate that image morphing can easily allow for two or more people with varied biometric features to achieve high match scores against the same morphed image, allowing for the face images of up to six persons to still match positively against the final morphed image.

BORDER CONTROL IMAGE MORPHING RISKS AND IMPLICATIONS

Morphing attacks can be extremely difficult to detect, since travel documents are issued by official issuing authorities, with all the official security features of a genuine travel document. This applies not only to ABC, but also to manual border control processes. Human beings have difficulties matching unfamiliar faces, it becomes even more difficult when two unknown individuals look alike. In order to avoid detection, a fraudulent user is likely to exploit that vulnerability by preparing a morphed image of two or more similar looking individuals in an effort to avoid detection.



“Human beings have difficulties matching unfamiliar faces, it becomes even more difficult when two unknown individuals look alike.”

The most effective and secure mitigation strategy against morphing attacks begins at the start of document issuance procedures, during the live-enrolment of ID photographs for travel documents and other official documents. Live-enrolment would allow the national issuing authority to better control the quality and authenticity of the ID photograph, and prevent any tampering with the ID photograph by the applicant, including submission of a morphed image. In the EU, live-enrolment is currently only obligatory for fingerprints, with just a few member states also performing live-enrolment for ID photographs.

RISK MANAGEMENT

Following the launch of the ABC systems training programme, a number of other important risk mitigation strategies are being explored and promoted. In the context of ABC systems and their growing numbers across the EU, Frontex has realized the importance of EU member states supporting and promoting the development of risk management plans for ABC systems, which are currently lacking in many countries with operational ABC systems.

In the context of manual border control, there are ways to manage the risk of morphing attacks. By teaching border guards how to detect possible traces of image morphing, they will be made aware of the existence and potential of these attacks. Having this knowledge included in the national training programmes of EU

member states is useful in the context of manual border control, and while operating ABC systems, since it is the border guard officer who mans the booth and responds to alerts.

WAY FORWARD

During the official launch of training in Portugal earlier this year, 56 officers from 27 EU member states participated. It became clear that the value and importance of developing training extends beyond the external borders of the EU. After receiving multiple expressions of interest from non-EU countries, Frontex is exploring the possibility of adapting the developed training materials for this purpose. The goal is to disseminate training to non-EU countries on a need-to-know basis, so that they too can benefit.

The importance of the ABC systems training programme goes beyond content alone, it is the result of long-standing and successful cooperation between national and international experts. This is the first attempt at developing an EU-wide harmonized and specialized training capability on ABC systems. Furthermore, it shows that the EU is committed to safeguarding an efficient and effective management of ABC systems through the delivery of harmonized trainings that can be taught at the national level in any EU member state.

For more information about the Frontex training on ABC systems, please contact their Research and Innovation Unit: rd@frontex.europa.eu. ■

NATIONAL SECURITY ON A GLOBAL SCALE.

A top priority for any nation is protecting its citizens — and HID Global is the world leader in providing trusted identities for government agencies and the people they serve. With the most advanced technology and the broadest portfolio of secure identity solutions anywhere on the planet, HID has made national security a global priority.

You'll call it world-class security. We call it *powering trusted identities*.

Powering **Trusted Identities** | Visit us at hidglobal.com/government

THE FUTURE EMPOWERED WITH LEGAL IDENTITY

Legal identity is at a crossroads. In its current form, it excludes over a billion individuals. Economic development, security and basic rights such as education, healthcare, employment and the freedom of movement are highly dependent on legal identity. How is this global crisis currently being viewed? What work is being done to assemble the puzzle of complex building blocks? What will the different outcomes mean? This will all be addressed in this article on the future of legal identity.



SANJAY DHARWADKER

He is a Member of ISO/IEC JTC1/ SC17/ WG3 (Machine Readable Travel Documents) as well as CEN/TC224 WG19 (Breeder Documents). He also participates in the ICBWG on Evidence of Identity, and NTWG for the re-writing of ICAO Doc 9303, Part 7, Machine Readable Visas, and is Head of Global ID Consultancy at WCC, Utrecht, The Netherlands.



In everyday life, we often take our legal identity for granted – be it for banking or business, acquiring assets, accessing facilities, travelling, voting, or, however unpleasant, paying taxes. While there is something about legal identity that gives us a sense of empowerment and liberty, it also connects us to our nations, and their histories and geographies.

In modern times, because legal identity is a national responsibility, it has developed in diverse ways and degrees. Today, only about 17 per cent of people worldwide in about 50 States have well-established legal identities. The bottom 15 per cent constitute over a billion individuals who have minimal or no recognition of their existence. This is not just at odds with basic human rights, it deprives these individuals of essential services like health, education and socio-economic opportunities.

LEGAL IDENTITY – WHY NOW?

This alarming situation prompted the United Nations to include legal identity among its Sustainable Development Goals to by the year 2030, provide legal identity for all with birth registration (SDG 16.9). Though briefly stated, this goal is significant for the action it urges – for the State to recognize and record each individual from birth.

People migrate, flee war-zones and look for better lives elsewhere. Unfortunately, individuals with unlawful intent – terrorists, criminals and economic offenders – often use humanitarian channels, causing extraordinary strain at border controls.

In 1924, the League of Nations gave itself one hundred years to end statelessness. Though currently, ten million people remain stateless, by 2024, there should be none. This obligation brought together the diverse disciplines and stakeholders who must shape legal identity more comprehensively for the future. But when we survey the landscape – of constitutions and statutes, cultures and beliefs, administrative practices, wars, refugees and human rights, gender inequalities, health and well-



being, economics and prosperity, crime and terror – the challenge seems overwhelming and yet too urgent to defer.

WHERE IS LEGAL IDENTITY TODAY?

The status of legal identity today, and where it should be, is the subject of intense debate among specializations, a cross-section of which is provided in Figure 1.

Legal identity is nestled among subjects like citizenships, nationalities, residences, voting rights, naturalizations, and the right to hold a passport. There is no single-best definition of legal identity. While many States have a national identity document, many depend on proxies, such as a drivers' license, bank card or passport. Divergence in practices leads to corresponding differences in the

administrative processes and business rules and technologies deployed to register individuals, issue documents and certificates, and to manage and maintain records securely and permanently, with strictly authorized access. The systems currently used also vary widely, from local handwritten village records, to advanced, centrally-managed digital identities.

After analyzing the global picture, a general model for the legal identity eco-system has emerged (depicted in Figure 2). Many of the elements, such as birth and residence, are of primary importance, while others are indicative. This also incorporates information on how citizenships can be determined (i.e.: by place of birth or parents' origins).



FIGURE 1 – Examples of specializations and agencies involved with legal identity

In many situations, either the records are not complete, are unavailable or cannot be authenticated. This requires evaluating other indicative records from the individual’s social footprint such as education and employment or utility bills, that can establish or reinforce an individual’s existence and status.

To establish legal identity for all, effort in the coming years will need to be focused on ensuring that all relevant elements are comprehensively addressed, modernized and harmonized, as well as judiciously inter-connected using both biographics and biometrics.

LEGAL IDENTITY AND ECONOMIC DEVELOPMENT

The current focus on legal identity is an economic necessity given the indication by numerous studies that legal identity facilitates greater opportunities. To address this, the World Bank has launched a significant programme appropriately titled “Identification for Development (ID4D)” that aims to provide comprehensive support that includes capacity-building. The programme will allow developing countries to accelerate their journey from poverty by strengthening legal identity.

In the coming decade, ID4D may act as a powerful catalyst for ensuring that States have bigger, better and more digital legal identity systems. Programmes like Aadhaar (though not fully addressing legal identity) in India have shown that this is achievable in relatively short spans of time on a large scale.

Spin-offs are important. In India, Aadhaar has reduced first-time passport application verification from forty-seven days to one

day. This is significant and includes powerful capabilities such as biometric authentication.

LEGAL IDENTITY AND SECURITY

Robust legal identity systems provide more reliable evidence of identity, which can be effective for enhancing security. Trafficking, for example, is more prone to originate from States with poor identity records, so there is a bigger possibility of criminals and terrorists assuming false identities. Though many States invest in secure eDocument infrastructures, because of weak civil registration processes, documents are issued to wrong persons with potentially disastrous consequences.

Cooperation among States also helps. The Schengen region is a great example and it is supported by the United Nations through the International Organization for Migration (IOM). Other regions like the Economic Community of West African States (ECOWAS) are considering similar strategies.

LEGAL IDENTITY AND STATELESSNESS

War, civil disturbances and natural calamities often displace populations beyond international borders. Affected individuals are at high risk of becoming stateless, deprived of human rights and education, healthcare and employment opportunities. This has already manifested in Europe, where receiving States process the legal identity of millions of individuals originating in other States, affording them asylum and where possible, refugee status.

I	II	III	IV
CIVIL REGISTRATION AND VITAL STATISTICS (CRVS)	FOUNDATIONAL (NATIONAL) ID SYSTEM	FUNCTIONAL ID SYSTEMS	SPECIAL-PURPOSE ID DOCUMENTS
VITAL EVENTS <ul style="list-style-type: none"> • Birth • Death • Marriage/separation • Adoption/naturalization • Etc. 	INDIVIDUAL PARTICULARS <ul style="list-style-type: none"> • Biographics • Biometrics 	<ul style="list-style-type: none"> • Education • Employment • Health • Insurance • Social security • Welfare • Banking • Phone • Utilities • Etc. 	<ul style="list-style-type: none"> • Democracy • Mobility • Travel
<ul style="list-style-type: none"> • Breeder documents certifying vital events • Population Register 	<ul style="list-style-type: none"> • National ID card • Digital Identity 	<ul style="list-style-type: none"> • Authentication • Social footprint generation 	<ul style="list-style-type: none"> • Voter ID card • Driver’s license • Passport

FIGURE 2 – General model for a legal identity eco-system (the four building blocks)

The United Nations High Commissioner for Refugees' office (UNHCR) is mandated to oversee two important international Conventions, for Refugees (signed in 1954) and the Reduction of Statelessness (in 1961). Despite an active role in conflict situations, over ten million individuals remain stateless. ICAO, under special provision, offers to facilitate international travel for them through a Machine-Readable Convention Travel Document (MRCTD). However, with the impending target of 2024 (a century after the League of Nations first addressed this issue), additional steps might be required to reinforce legal identity to prevent further statelessness.

MANIFESTATION OF STATE POWER AND EXTREME IMPACT

There are other aspects that need to be firmly, yet sensitively, addressed. Many States remain indifferent to legal identity requirements; this is often attributed to government ineptitude. Whether this responsibility can be entrusted to private entities has been recently debated. Terms like "self-sovereign identity" have gained currency. This, coupled with the blockchain, a new way of storing and managing data, is being touted as the new "holy grail" for legal identity. There are, however, issues that prevent this from happening.

The existing practice and belief of legal identity as being the essence of the social contract between the citizen and the nation-state, runs deep. More importantly, it lies at the heart of the political power of the State, it determines who can vote, and who can be elected. It can disenfranchise millions with the stroke of a pen. It can be used to divide nations and unleash terror and genocide. In a recent war, a victorious army destroyed the entire civil registries of an annexed State, something that may take years to reconstruct.

Modern technology doesn't seem to help, it actually has the potential to make such acts easier. It is important for States to

provide resilient safeguards, framing which might be challenging, but is not impossible. That said, there is good news at hand.

TECHNOLOGY AND GENERATIONAL CHANGE

Today we live in an interconnected world with mobile phones and the internet. Both technology and generational changes are likely to have an impact on how legal identity could be packaged and shared in the future. Already smartphones are capable of unambiguously verifying physical identity using biometrics. Some say they are just a few steps away from manifesting legal identity, while others say it might not be that simple.

Whether the mobile phone can be a carrier of legal identity documents (like the passport), is currently under intense scrutiny. International standards bodies are already tasked with mapping the details. While consideration will have to be given to many factors, including the risk of greater digital divide, there is little doubt that millennials the world over would embrace it for both its zing and convenience.

There are potential benefits for authorities too, since it would change the way travel documents and border control are managed. Even Advanced Passenger Information (API) and Passenger Name Records (PNR) could be simplified and made increasingly secure and more cost-effective. Given that flights are already booked using mobile-phones, passenger tracking could indeed find its generation-next in all this. There is little doubt that wider consultation and due diligence are required for a universal implementation that benefits all.

This is just one example of the likely directions that legal identity might take in the near future. For now, let us reach 2024, when no person may be stateless, and 2030, when everyone on this planet has a legal identity that is understood, recognized and respected by all. ■

Check eIDs in the blink of an eye.

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

IT security made in Germany.

www.secunet.com/en/eidpki



secunet

IT security partner of the Federal Republic of Germany

IOM'S COMMITMENT TO INTENSIFIED TRIP STRATEGY IMPLEMENTATION



FLORIAN G. FORSTER

He is the Head of IOM's Immigration and Border Management Division (IBM) at IOM Headquarters in Geneva, Switzerland. He oversees a team of IBM specialists and support staff, and provides technical oversight to the senior IBM specialists posted in IOM's eight regional offices and the African Capacity Building Center (ACBC) in Moshi, Tanzania. He is responsible for developing and overseeing IOM's global approach to activities in the field of Border Management and Immigration.



ERIK SLAVENAS

He is an Identity Management and Biometrics Officer at IBM Division, IOM Headquarters in Geneva. His focus is on expanding IOM's IBM programming to provide better technical assistance to States in the areas of identification management, travel documents, border controls and biometric applications. Erik works closely with 150 IOM IBM staff worldwide to identify assistance needs in Member States and translate them into new programming initiatives. Before moving to IOM Geneva, his recent assignments were with IOM Missions in Afghanistan and Mali.



Established in 1951, the IOM - the UN Migration Agency - is the leading intergovernmental organization in the field of migration. IOM is committed to the principle that humane and orderly migration benefits migrants and society.



For decades, the International Organization for Migration (IOM's) global Immigration and Border Management (IBM) programme has been working on numerous areas within the scope of the ICAO TRIP Strategy, but without specific reference to the Strategy's goals. This article provides a summary of IOM's global implementation capacities and its current technical assistance activities related to the ICAO TRIP Strategy. It also looks at the TRIP-related areas that will be expanded in the future.

On 15 November 2016 ICAO and the IOM signed a Memorandum of Understanding (MoU) to highlight the common interests of IOM and ICAO to increase cooperation related to ICAO's work on security and facilitation within the framework of the ICAO Traveller Identification Programme (TRIP) Strategy, including joint development and implementation of capacity-building projects.

CLOSER COOPERATION ON ICAO TRIP STRATEGY IMPLEMENTATION

Though both the IOM and ICAO are United Nations Agencies, the two organizations operate within different policy and legal frameworks, with each contributing unique strengths. The MoU provides an opportunity to combine:

- ICAO's solid mandate rooted in the Chicago Convention, regulatory powers and excellence in developing global Standards and Recommended Practices (SARPs) with;
- IOM's global operational project development and implementation capabilities in the field, fund-raising liaison with donors and its technical expertise on border and identity management.

The IOM-ICAO partnership has great potential for making global borders more secure while contributing to enhanced facilitation for the legitimate flows of travellers. The TRIP framework, and its successful implementation in practice, is vitally important to achieving both of these aims. This partnership offers a perfect strategic-operational nexus, with global coverage, for intensifying the implementation of the ICAO TRIP Strategy.

The IOM is well-placed to use its global project implementation capacities to make ICAO TRIP Strategy SARPs and best practices a reality in Member States. Notably,



this includes implementing the Strategy in developing and fragile States that face security and economic challenges but still need to comply with international norms on border management and traveller documentation.

IOM also brings the following to the implementation of the ICAO TRIP Strategy:

- Human and migrant dimensions: IOM focuses on the needs of migrants, as travellers and the ultimate users of ICAO TRIP SARPs, and new technologies in the fields of identification management, MRTDs and border controls.
- Humanitarian dimension: extending the benefits of the ICAO TRIP framework and new technologies to vulnerable groups in need of protection: displaced persons, stranded migrants, victims of natural disasters or armed conflicts.
- Sustainable development: adding the development dimension to provide technical assistance to States in need, ensuring that the results are more sustainable and long-term, in line with the UN Sustainable Development Goals.
- New funding opportunities: IOM has a well-developed working relationship with the donor community and specializes in donor-funded international assistance projects.
- Regard for good governance: having effective institutions and modern technologies in identity and border management is important but not sufficient. Good governance also calls for integrity, transparency and accountability as key operating principles. In its IBM technical assistance projects, IOM supports States in strengthening their executive control, parliamentary oversight, respect for human rights and the rule of law, and other key values of the UN.
- Going beyond aviation: the ICAO TRIP Strategy and TRIP SARPs, while developed by ICAO with aviation in mind, can be extended to land and sea border controls at no or very little extra cost, enhancing security and facilitation benefits to Member States in these sectors.
- Laying infrastructure foundations for TRIP implementation: in many developing States, MRTD and border management institutions lack the basics, such as stable electricity, water, internet, dust-free premises ability to support IT systems, and telephone or radio connectivity. By supplying the basic infrastructure, IOM IBM projects create a durable foundation on which more advanced components of the TRIP Strategy can be built. This includes MRTD issuance, proper reading of MRTDs/eMRTDs at the border, integration with Advance Passenger Information (API), Public Key Infrastructure (PKI), international alert lists, and others.



IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM acts with its partners in the international community to:

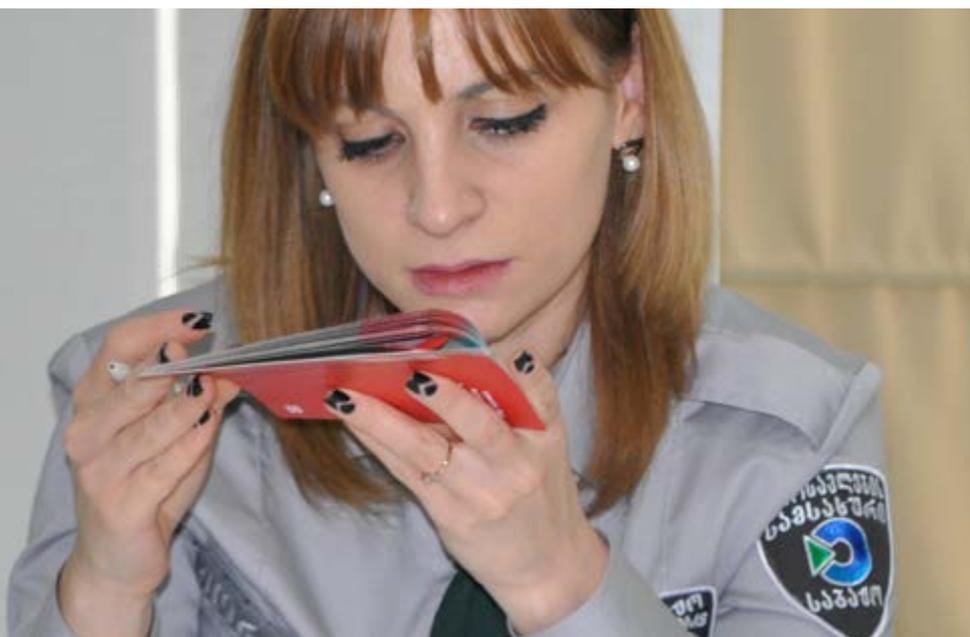
- assist in meeting the operational challenges of migration;
- advance understanding of migration issues;
- encourage social and economic development through migration; and
- work towards effective respect of human dignity and the well-being of migrants.

THE WAY FORWARD

Increasing the cooperation between IOM and ICAO presents a strategic opportunity for intensifying ICAO TRIP implementation world-wide. IOM has both the political will and operational capacity to boost ICAO TRIP implementation in its 166 Member States.

IOM, through its IBM programme, has already been implementing global activities that are relevant to the ICAO TRIP Strategy. It has the potential to expand its IBM work considerably in a more structured manner – by guiding its IBM staff in 150 missions world-wide to include priority ICAO TRIP elements into their project development and implementation.

Based on consultations with the ICAO Secretariat and its Implementation and Capacity-Building Working Group (ICBWG) of the Technical Group on the Traveller Identification Programme (TAG/TRIP), the following thematic areas emerged for IOM's focus on enhancing ICAO TRIP implementation worldwide, subject to the mobilization of the necessary funding from donors:





- MRTD procurement – for passport tenders and roll out, also visa foil and national ID card tenders. The main needs are ensuring ICAO compliance of new MRTDs, assisting States in getting good value for money, and promoting MRTD procurement best practices. IOM has strong procurement capacity and – with further expertise from ICBWG and relying on the ICBWG MRTD Procurement Guide – IOM can play a major assistance role in the MRTD procurement field. In coordination with UNHCR, this work item could also include tenders and implementation of Convention Travel Documents, where the ICAO compliance rate is still low. Additionally, ICBWG’s ongoing work on developing a cost/benefit analysis framework for ePassport procurement for small and developing States, can be integrated with future IOM IBM projects to mutual advantage.
- Evidence of Identification (EoI) – ICBWG is developing EoI guidance materials which could inform IOM’s future EoI advocacy activities. In addition to advocacy and raising awareness, IOM, in close cooperation with ICBWG experts, can assist States in setting up the right processes and workflows

to strengthen EoI. A related area is IOM’s IBM assistance to help States with strengthening civil registries, the security of breeder documents (birth certificates, etc.), digitizing manual civil registry records, and installing civil registry infrastructure and communication capabilities between offices.

- Supplying States with border management information systems, either MIDAS (see text box) or others, depending on the needs and preferences of the beneficiary State. Installing border management systems also opens the door to related border control tools and the possibility of linking the border management information system with them – such as PKI including the ICAO PKD, the INTERPOL SLTD (and other watch lists) and API.
- PKD promotion and increasing the number of active members offers a broad range of assistance activities. Advocacy and awareness raising – national/regional workshops about PKD and its benefits – and technical consultations (only for States that have already expressed commitment to join PKD). Covering PKD membership fees for developing states for 1-2 years, within the duration of a project (in exchange for the



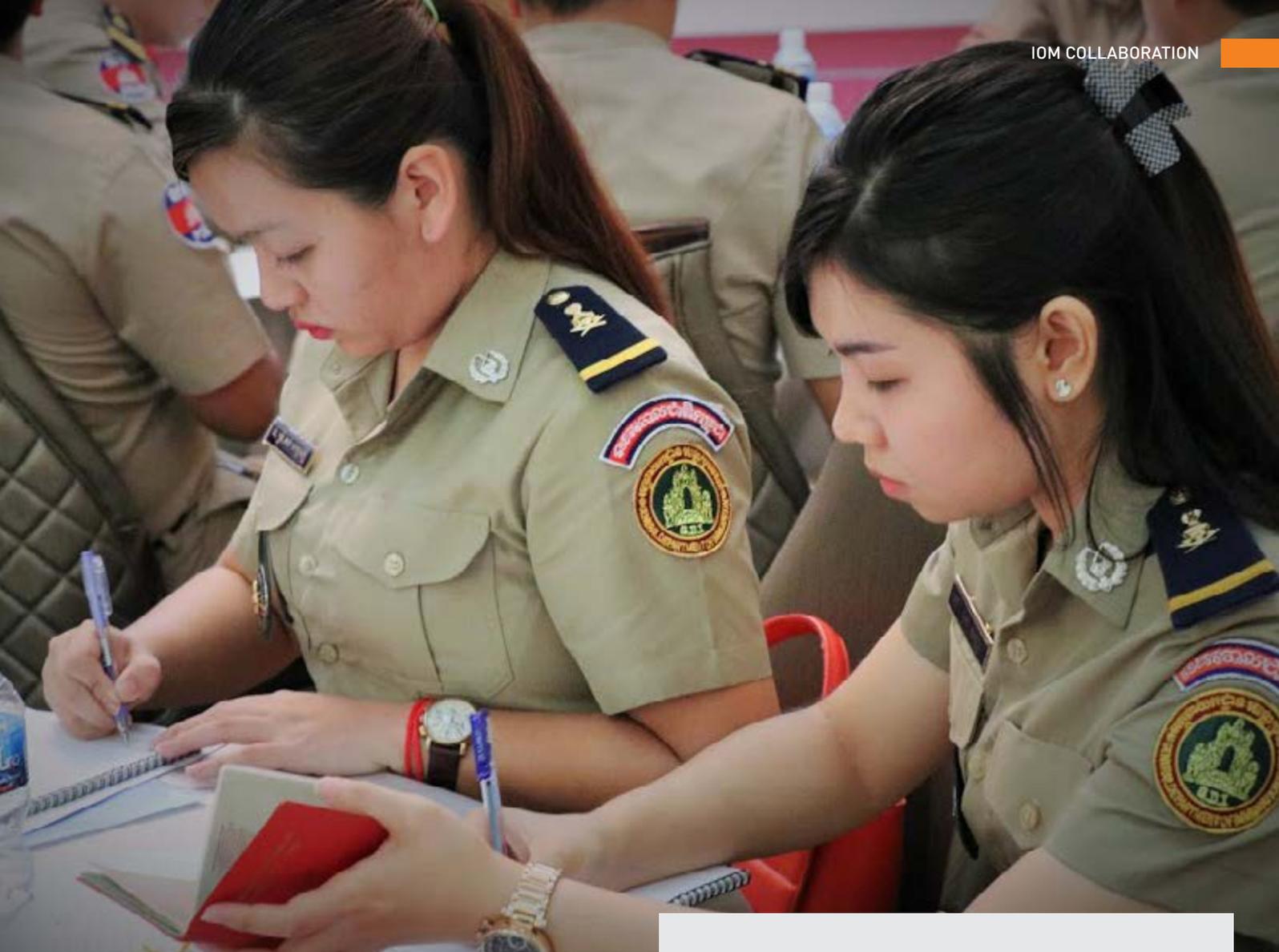


commitment to budget the costs to carry on after the project is over). Study visits and technical consultations for senior decision-makers of ICAO to consult PKD staff directly, which can be combined with attending the TRIP Symposium. Subject to available funding, a related possibility under consideration is covering travel costs for developing States to participate in 2-3 meetings of the PKD Board during the time of the project.

- Providing professional training to border officials on the foundations of travel document production and in-depth training on travel document examination and impostor recognition. Ensuring sustainability through Training-the-Trainers and enhancing in-house training capacities on document fraud. IOM's ACBC training centre in Tanzania, and its curricula and trainers' resources, provide a solid foundation for delivering such training in Africa. Joint ICAO-IOM training initiatives on travel document examination and impostor recognition can also be explored.
- Assessments of national identification management practices and producing recommendations – aligned with ICAO's Guide for Assessing Security of Handling and Issuance of

Travel Documents. For border controls, a new assessment framework is being developed by the ICAO Secretariat as part of the Caribbean TRIP project, which also can be used for assessments in the future. Also, IOM has its own in-house border management assessment framework that is used in performing border assessments. Importantly, assessments provide not just recommendations about corrective action needed, but identify capacity gaps that can be addressed through future project development.

- Helping States with registration, document issuance and biometric data capturing, especially in emergency and crisis environments to migrants in distress, which is a major area on IOM's agenda.
- Promoting other TRIP areas. Some items on the TRIP agenda are important but are sometimes overshadowed by items of greater urgency. ICAO-compliance of passport photos, handling SLTDs, handling ePassports that fail to read, good practices in issuing Emergency Travel Documents, etc., are all relatively minor, yet important, areas that can be included in IOM IBM seminars and workshops globally to promote awareness and best practices.



These focus areas do not exclude IOM from contributing to other ICAO Secretariat TRIP activities along the lines of the joint MoU, including ad hoc assessment missions, seminars and workshops, joint training or research events, and others.

While TRIP implementation challenges are global, certain regions are in far greater need of assistance for infrastructure and technical expertise. In developing TRIP-related IBM project proposals, IOM furthers the goals of the ICAO 'No Country Left Behind' initiative and focuses on States where assistance needs are the greatest.

IOM continues working on building on the success of its Immigration and Border Management programme and becoming a key implementer of the elements of the ICAO TRIP Strategy for the benefit of its Member States around the world. ■

THE SECURITY-DEVELOPMENT NEXUS

Through its technical assistance projects, IOM contributes to economic development through the provision of sustainable solutions:

- Effective border and identification management is a powerful tool for addressing trans-border crime (including terrorism) and enhancing national and regional security. Security is a pre-condition for sustainable development and stabilization for States in transition.
- Development without security is impossible, security without development would be only temporary. By recognizing and addressing the security-development nexus, IOM has the potential to strengthen the sustainability of the implementation of the TRIP Strategy globally.

10,000+
Global Visitors

250+
High-End Exhibitors

100+
Countries Represented

DON'T MISS KEYNOTE FROM:
 UK Security Minister
 Ben Wallace MP
 Day One Global Counter
 Terrorism Conference

LONDON HOSTS WORLD CLASS INTERNATIONAL SECURITY EVENT

TOPICS COVERED:

- ▶ Global Counter Terrorism
- ▶ Protecting Crowded Places
- ▶ Critical National Infrastructure
- ▶ Cyber Security
- ▶ Designing Out Terrorism
- ▶ Major Events & Stadiums
- ▶ Building & Facilities Management
- ▶ Aviation & Borders
- ▶ Transport Security

Featuring:



**250+ High-End Exhibitors,
 200+ Speakers, 250+ Sessions!**

Screening Intrusion Detection X-Ray CCTV ANPR Video Analytics Cyber C-IED Counter Terrorism Protection Personal Security Drones Training Biometrics UAVs Optics Bollards Barriers Radar Armoured Vehicles Fencing

GOVERNMENT AGENCIES & DEPARTMENT ZONE
 Featuring

LIVE DEMONSTRATIONS
 In association with:

NEW CYBER INTELLIGENCE ZONE
 In association with:

Alternatively register a delegate pass to access the high-level Global Counter Terrorism Conference. Readers can save 15% on published rates with discount code UKSEC15

REGISTER FOR A FREE VISITOR PASS NOW www.uksecurityexpo.com/ica0



TRIP REGIONAL SEMINAR IN HONG KONG

ICAO'S TRIP REGIONAL SEMINAR IN HONG KONG SAR, CHINA

✈ Robust ID management frameworks provide a critical foundation for secure and efficient travel document and border control solutions. This was an important focus during the Regional Seminar on the Traveller Identification Programme (ICAO TRIP) that was conducted from 11 to 13 July 2017 in Hong Kong SAR, China. The event was hosted by the Civil Aviation Department of Hong Kong with additional support from Hong Kong International Airport.

Participants from 37 countries and ten international organizations were given updates on the five elements of the ICAO TRIP Strategy: machine readable travel document (MRTD) standards; specifications and best practices; secure travel document issuance; robust evidence of identity processes; and information sharing technologies.

Speaking to the Hong Kong audience, a week after attending a special meeting of the Security Council's Counter-Terrorism Committee (CTC) on "Terrorist Threats to Civil Aviation", ICAO's Secretary General, Dr. Fang Liu informed participants that the special CTC meeting had considered relevant gaps and vulnerabilities and discussed possible instruments and tools to further support ICAO-compliant border control management systems.



Photos provided by the Information Services Department of Hong Kong, China

“Through ICAO’s standards, our Traveller Identification Programme (TRIP) strategy harmonizes the global line of defence in our shared battle to confront international terrorist movements, cross-border crime, and many other threats to civil society and international aviation,” Dr. Liu stressed.

“We will continue to explore new means of addressing the terrorist threat through various ICAO TRIP elements”, she continued. “ICAO works closely with many leading organizations. We encourage States to come together at the regional and sub-regional levels to agree on action plans, and to coordinate efforts aimed at rectifying aviation security and facilitation deficiencies in a robust, affordable and sustainable manner.”

ICAO TRIP Regional Seminars have two main purposes. First, they provide an opportunity for updating participants from

Member States about current ICAO Standards, specifications and new developments, and they allow for clarifying specific and technical questions. Second, they provide a forum for professional discussions about the current and emerging needs of States and other stakeholders. They also provide an opportunity for discussing the practical ways States can work together to strengthen traveller identification management and border control capacity, enhancing security and facilitation.

ICAO’s TRIP Strategy plays a critical role in aviation security for combatting foreign terrorist fighters with a special focus on effective border control management, as reflected in United Nations (UN) Security Council (SC) Resolutions 2178 and 2309, which were adopted in 2014 and 2016 respectively. ■



SAVE THE DATE

ICAO Traveller Identification Programme Jamaica Regional Seminar

Strengthening aviation security through
improved traveller identification

Montego Bay, Jamaica, 28 – 30 November 2017

For more information, please visit our website
www.icao.int/Meetings/



ICAO

SECURITY & FACILITATION

THE EVOLUTION OF THE ePASSPORT

AN OVERVIEW OF NEXT GENERATION ePASSPORT TECHNOLOGY



JASPER MUTSAERS

He is currently a Research and Development Advisor with the National Office for Identity Data of the Ministry of the Interior and Kingdom Relations, the Netherlands. In his current role, he focuses on the electronic and biometric components of travel documents. Jasper holds an MSc in Public Administration and Political Sciences from Erasmus University Rotterdam.

Travel documents have significantly evolved since they were first introduced as a means for facilitating international border crossings. Over the years, features have been added to strengthen the bond to the holder; to improve physical security; and streamline document reading. The incorporation of an integrated circuit chip capable of both storing the holder's biometric data, and assisting in the document's authentication, fundamentally transformed the passport and created new opportunities for passenger management and flow. While these documents, if used to their full potential, play a significant role in securely facilitating passenger and document processing and clearance, they must still be manually inspected, since they contain other information that may be pertinent to determining entry or passage.

Logical Data Structure 2 (LDS2) is an optional and backwards-compatible extension to the ePassport that provides States with the option to fully digitize the travel documents that they issue. This article discusses next generation ePassport technology, the added benefits of its implementation, impacts for border management, and the risks and challenges to its deployment.



JUSTIN IKURA

He is the Deputy Director of the International Unit of the Canadian Passport Programme, which is administered by the Department of Immigration, Refugees and Citizenship Canada (IRCC). Prior to joining the IRCC's Passport Programme, he worked on labour market and services trade policies in a variety of departments. Justin holds an undergraduate degree in International Business and Marketing and Master's Degree in Public Administration, both from the University of Ottawa.



The technology behind the biometrically-enabled integrated circuit chip passport, or ePassport, has also steadily developed since it was first introduced in 1998. The most notable of these changes was the standardization of the technology, to ensure that ePassports could be used seamlessly in the global civil aviation system. Since being standardized, the technology has been adapted to respond to demands for improved performance at the border, increasing pressures for privacy protection, and ongoing attacks from fraudsters. While the ePassport has matured to a state that offers an acceptable balance between security and facilitation, the capacity of fraudsters, coupled with demands for efficiency from border management and airport authorities, continues to advance the international baseline.

To ensure that the biographic and biometric data stored in the ePassport can be accessed by authorities around the world (i.e. globally interoperable), issuing authorities must apply international specifications that have been developed by the International Civil Aviation Organization (ICAO). *ICAO Machine Readable Travel Documents (Doc 9303)* provides explicit guidance about how printed and digitally-stored information in travel documents should be formatted. Specifications relating to the organization of ePassport data are included in Part 10 of Doc 9303 (*Logical Data Structure [LDS] for Storage of Biometrics and Other Data in the Contactless Integrated Circuit*), which provides issuing authorities with technical specifications to guide ePassport issuance that is secure, conducive to authentication, and consistently ordered.



According to these specifications, document issuers must include all details from the machine-readable zone, a facial biometric, and what is known as the document security object (used to validate the integrity of data added by the issuer). Additional optional fields in the LDS include space for secondary/tertiary biometrics, displayed identification features, and encoded security features. ePassport issuing authorities may populate these fields to further bind the document to the holder, improve the facilitation of the traveller and/or ensure that the document can be authenticated.

Using the public key infrastructure (PKI) scheme described in ICAO Doc 9303, issuing authorities can protect the information stored in the ePassport chip from manipulation. The current generation of ePassports are issued on the principle of 'write-once, read-many', meaning that document information is locked at the time of issuance. Despite acting as a very effective security feature, locking the data at the time of issuance limits other pertinent travel information from being digitally added to the document over its lifespan.

OVERVIEW OF LDS2

Recognizing the security and facilitation benefits of making other travel information available in electronic format, ICAO's working groups have developed specifications to support its addition to the ePassport. LDS2 is an optional and backwards compatible extension to the ePassport chip that allows for the digital and secure storage of travel information, after the document has been issued. LDS2 extends the capability of the ePassport through the addition of applications that allow for the digital storage of travel

data (visas and travel stamps), and other information that could facilitate the travel of the holder (additional biometrics), over its validity period. Travel document issuing authorities that choose to implement LDS2 functions would be free to use all, or a selected number, of the endorsed applications available.

KEY PRINCIPLES

Successful global adoption of LDS2 technology hinges on a number of key principles, namely that it be backwards-compatible and optional for States to use. In terms of backwards-compatibility, it is important to note that the LDS2 applications would work alongside the LDS1 application, and would not, in any respect, replace it. As the primary container for the biometric and biographic data of the holder, the LDS1 application must continue to be accessible. In the earliest phases of LDS2 deployment, it is highly likely that LDS2-enabled document holders may be processed in border control systems that have not been updated to support their documents. In these cases, the inspecting authority conducting the ePassport examination will need to access information stored in the LDS1 application.

To provide optional extensions to the ePassport, the existing set of specifications have been designed in such a way that adding all or selected LDS2 applications will remain at the discretion of the issuing State. ePassport-issuing States may choose to add LDS2 applications that facilitate border clearance processes, improve the intelligence of automated or manual travel history analysis, or safeguard additional entries from tampering or fraud.



THE ADDED BENEFITS OF LDS2

Expanding the functionality of the chip affords a host of benefits that may assist States in deciding whether to deploy LDS2-enabled ePassports. These benefits can be realized by key stakeholders in the travel continuum, particularly border management.

ENHANCED SECURITY

Converting paper- or ink-based entries to e-data in an application stored in the ePassport offers strengthened security against tampering and/or attempted reproduction. While visa counterfoils and travel stamps are designed in such a way that tampering is extremely difficult, counterfeiting techniques and tools have become increasingly sophisticated, making this travel information susceptible to fraud. In addition to being stored directly on the chip and physically in the document, data stored in the LDS2 applications would be digitally-signed by the issuing authority, verifiable through the PKI. Coupled with the existing security mechanisms to prevent alterations to LDS1 data, the use of LDS2 applications further safeguards the document from fraud.

STANDARD FORMATTING

Variations in the size, features and materials used for visa and travel stamps can result in confusion at border control and by other stakeholders, such as airlines, involved in clearing passengers. A standard digital format applied to both travel stamps and visas will contribute to enhancing readability and reducing this confusion. Additionally, with access to standard formatted entries, States could deploy facilitation or security-enhancing schemes that make use of this digital information to make automated border clearance decisions.

STREAMLINED PROCESSING

Physically entering information into the document of the holder at either entry or exit points in the border control process is an inhibiting factor to the full automated clearance of a traveller. Automating this critical step in the border control process could reduce the need for interaction with a border control officer, since clearance processes could rely more heavily information on stored in the chip and/or that could be stored in the document. Reduced requirements for interaction with border officials could help to improve the flow of passengers, avoid unnecessary delays and line-ups, and allow States to benefit from a greater return on investments made into automated border clearance (ABC) technologies.

AUTOMATED RISK ASSESSMENT

LDS2 provides border control with the capability to perform an on-the-spot analysis of the risk that travellers presenting themselves at the border pose. One of the advantages of standard, digitally stored data is that it is much simpler to analyse than a plethora of varying travel stamps and visas. LDS2 applications provide states with the ability to detect things such as: unusual travel patterns; disconnects between entry and exit stamps; and attempts to alter travel stamps of visas.

LEVERAGING INVESTMENTS

Launching an ePassport can be a costly endeavour, which is often offset by fees charged to the applicants; justifying these costs to holders is therefore important. Expanding the capability of the ePassport could allow States to more fully reap their benefits and create a better return on investment, provided by the right

supporting systems (e.g. participation in the ICAO Public Key Directory, use of ABCs, etc.).

IMPLICATIONS FOR BORDER MANAGEMENT

The addition of LDS2 technology to the ePassport will also have an impact on border management technologies and practices. While the border control authorities of a State employing LDS2 in its passport may maintain traditional practices (for example manual stamping, primary inspection lines, etc.), the full benefits of LDS2 can only be realized where automation techniques are applied.

TRAFFIC CONTROL

The increased functionality of the ePassport could have an impact on the ways border controls manage their passengers. Travellers with LDS2-enabled ePassports may be directed to automated kiosks to be processed, rather than to a border control officer in an inspection line. As previously discussed, the addition of LDS2 functionality reduces the necessity for travellers to interact with border control officers, since much of this can occur virtually, with the tools equipped to calculate risk and/or record travel data.

AUTOMATED BORDER CLEARANCE

States using ABC kiosks could re-configure their systems to allow for the digital recording of travel data. As a tool for further automation, the use of LDS2 could potentially enhance the capacity of ABC gates, could contribute to traffic management strategies, and may ultimately assist in streamlining border control flows.

ePASSPORT READERS

States that are not employing ABC systems to process travellers, but are already using the equipment to open and read ePassport data will be required to re-programme their readers with the software to access LDS2 applications and data, if they opt to read and/or write LDS2 data.

RISKS AND CHALLENGES OF DEPLOYMENT

While LDS2 technology could improve both the security and facilitation of international travel, there are challenges that could impact its success in the field. The most notable challenge will, for at least the first few years of deployment, be uneven uptake by States around the world. As an advanced technology, it is quite possible that some (or many) States will have operational and financial challenges prohibiting the issuance, data entry and/or validation of LDS2-enabled documents. Another challenge that should be noted is the potential logistical difficulties related to the distribution of certificates to validate the document entries and/or grant authorisations to add entries. Work is underway to determine how best to address these and other issues. For the moment, efforts are focused on developing the foundation to support States as they begin to explore whether, and how, to implement the technology.

FUTURE OPPORTUNITIES

Extending the functionality of the ePassport provides travellers with facilitative benefits and the opportunity to travel across international borders more seamlessly. As a holder of an electronically-enhanced travel document, travellers expect to be processed using the technologies and processes that complement their document, and those that make the most of the costs associated with obtaining them. The potential benefits of LDS2 are, however, contingent on the ways border controls manage their systems and risk thresholds. In a fully automated system, passengers with LDS2-enabled documents, particularly low-risk travellers, could have both their document and identity verified in an entirely automated fashion, which, in turn, could reduce the stress of travellers, avoid unnecessary delays, and ensure that border control officers are focusing on higher-risk travellers. ■

This article has been reprinted with permission from Keesing Technologies, Keesing's Journal of Documents & Identity.



Document Verification Solutions

www.regulaforensics.com

THE IATA/CONTROL AUTHORITIES WORKING GROUP CELEBRATES 30 YEARS OF GOVERNMENT AND INDUSTRY PARTNERSHIP

✈ The IATA/Control Authorities Working Group (CAWG) is comprised of an expert forum of airline and government officials who work collaboratively to recommend solutions and establish best practices for border management. Their work contributes to facilitating legitimate travellers while ensuring secure borders.

Formed in 1987 to tackle mutual facilitation concerns between airlines and governments, CAWG was able to develop guideline documents for the movement of inadmissible and deportee passengers. The group has since enjoyed the benefit of many dedicated members in its 30-year history, keeping pace with and anticipating the many changes in border control and the aviation world. Noticeable output from the group includes guideline documents for Advanced Passenger Information (API), Interactive API (iAPI) and Passenger Name Record (PNR) requirements.

With active members from more than 15 States, the role of CAWG is to provide strategic direction and leadership for integrated border management and aviation facilitation matters for passengers and crew. Offering advanced knowledge in the field of border innovation and border management practices, CAWG interfaces and liaises with IATA groups and the external organizations that have an interest in border management.

The group is currently led by Teresa Hardy (center left) from the United Kingdom Border Force and John Watts (left) from the National Airlines Council of Canada, along with Christopher Hornek (right), who represents IATA. The airline and government co-chair roles rotate every two years.

Teresa, John and Chris have the following to say about why they chose to take on these roles which are in addition to their “day jobs”:



Teresa Hardy (center) from the United Kingdom Border Force and John Watts (left) from the National Airlines Council of Canada, along with Christopher Hornek (right) from IATA

TERESA HARDY – *“The CAWG has an impressive legacy and I wanted to be involved in ensuring that the CAWG remains relevant and a source of expertise for the future. It provides a unique forum for governments and airlines to collaborate and explore the impact of travel for the future and this can only be a good thing.”*

JOHN WATTS – *“It has been very rewarding to be a part of CAWG for the past seven years. It is remarkable to consider the number of guidelines and best practice documents on various facilitation topics CAWG has produced over the past 30 years. As Co-Chair, I look forward to participating in many discussions within the group and with our external partners in the development of global guidance for important future facilitation initiatives.”*



The 2017 CAWG Meeting was hosted in Dubai on 5-6 April 2017 by the United Arab Emirates General Directorate of Residency and Foreigners Affairs.

CHRISTOPHER HORNEK – *“I joined the CAWG in 2015 and have had the honor of learning from the group in a very collegial and constructive atmosphere. The expertise the CAWG pulls together is impressive and the Group’s productivity is a direct function of its inclusive participation, including both border security agencies and airlines.”*

The CAWG shares a global view on border management issues and solutions, providing opportunities for benchmarking and sharing lessons learned. Its very nature enables an open dialogue between airlines and governments which helps to address existing challenges, as well as creating opportunities to innovate. Outcomes from the CAWG assist the implementation of facilitation directives and it is one of the largest Government/Industry contributors to the ICAO Facilitation Panel.

The group has an active agenda of working groups that are currently focussing on:

- **ADVANCE PASSENGER INFORMATION DATA QUALITY** – delivering consistent methodologies and metrics for airlines and governments to have constructive and focussed engagement to resolve issues on data accuracy and provision, crucially linked to the United Nations Security Council resolution 2178 (2014).
- **REGISTERED TRAVELLER PROGRAMMES** – examining the opportunity for governments and carriers to increase the effectiveness of these programmes.
- **DUAL NATIONALITY** – exploring issues with multiple passport holders and offering solutions and best practice for governments and carriers.

- **SEAMLESS TRAVELLER/SINGLE TOKEN INITIATIVES** – ensuring collaborative involvement in the latest initiatives such as IATA One ID and Happy Flow, which may also address data inaccuracy and increase facilitation and security.

Very much in step with current and future thinking, key successes and achievements in its 30-year history include contributions to the development and revision of Standards and Recommended Practices in Annex 9 – Facilitation. ICAO’s publication of best practice documents on a wide variety of issues include electronic travel systems, carriers’ liability/document checking and the code of conduct for immigration liaison officers.

The CAWG is looking forward to many more years of productive partnership and is always looking for new or returning members. States wishing to join for the first time should make a joint approach from a government official and a representative of an airline based in that country.

The next CAWG plenary meeting will be held in Barcelona from 25 to 26 October 2017 alongside the IATA World Passenger Symposium. The co-chairs will also be making a presentation on IATA CAWG during the IATA Passenger Experience Management Group in London in September.

If you would like to find out more about the CAWG, obtain copies of the CAWG Guideline and Best Practice documents, or apply to join, please contact Christopher Hornek at IATA at hornekc@iata.org ■

RISK ANALYSIS FOR AIRPORT SECURITY IN THE CONTEXT OF EUROPEAN COMMUNITY (EC) LEGISLATION



CHARLES DE COUESSIN

He began his career at the Paris Louvre Museum as a curator in charge of scientific analysis of art objects. He moved to the oil industry and then to aviation in 1998 when he was appointed Development Director at SITA, a main provider of aviation communication and IT infrastructures. After pioneering the first European Commission funded biometrics and smart cards programme with IATA and industry stakeholders, he founded ID Partners, a consulting practice based in Paris. Charles is involved in various EC aviation security and border initiatives, and has been an advisor of the French government for both identity and passenger data (PNR) programmes.



Though over the last decade we have seen an optimization of airport control procedures, even with innovation, security remains a tedious process. All passengers undergo similar controls, whatever their risk or the travel scheme they are part of. These processes also have an impact on flight departures and the time travellers spend in retail areas.

It is worth considering how aviation security stakeholders might benefit from available passenger data and other information. One anticipates a need to implement new tools, upstream to the airport terminal, which is still considered the “last line of defence”. Indeed, traffic growth advocates for the implementation of simplified procedures at the two main stages where there are the biggest bottlenecks in terminals: security control and border crossings.

What would be the role of Advance Passenger Information System (APIS) and Passenger Name Record (PNR) data in the view of a “smart security” initiative which aims to simplify procedures for “bona fide” passengers, while tightening the screening of suspicious persons? Do these data represent a tiny piece of the more complex security puzzle? If this is the case, what are their final outcomes: alleviating the airport checks or facilitating the border crossing? Is it possible to transpose at the checkpoint the current procedures currently implemented for automating border management controls?

THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS) DIRECTIVE

In 2004, during a period when Spain was dealing with high immigration flows from South America, the country became instrumental in promoting the API directive. Though most Member States have since transposed it in their national legislation, they haven’t necessarily implemented adhoc processing measures.

Though the initial purpose of the API directive was to combat illegal immigration, it could be extended to other purposes. Furthermore, Article 6 also allows for it to be used for “law enforcement purposes” and “the protection of public policy (public order) and national security”. This means that the regulation should no longer restrict the usage of the directive to immigration staff, but that a risk indicator could be communicated to airport checkpoints.

THE PASSENGER NAME RECORD (PNR) DIRECTIVE

Though the objective of the PNR programme is to prevent organized crime, for the first time it introduced the concept of risk assessment. This was absent from the API initiative, and is highly innovative, since it meets the current trend for an enhanced airport checkpoint. The PNR directive aims to produce an intelligence tool rather than a new instrument for border control. Processing is performed in advance of border crossings and not at the border crossings themselves.

Aviation security is a key outcome of the PNR directive. Indeed Article 7 recalls that “Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime”, which is the typical duty of airport checkpoints.

THE PASSENGER INFORMATION UNIT (PIU)

The PNR Directive (Article 4) details how the Passenger Information Unit (PIU) will be responsible for the collection of PNR data of flights to or from Member States. PNR data should only contain details of reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security irrespective of “a person’s race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation”.

In line with the privacy protection regulation “Member States shall ensure that any positive match resulting from the automated processing of PNR data (...) is individually reviewed by non-automated

means to verify whether the competent authority (...) needs to take action under national law”. In other words, the final decision shall always be taken by authorized persons from competent authorities, and never from a machine or processing system.

Since the legal framework prohibits automated decision-making, only competent authorities should provide a status on the potential risks of passengers. This was a difficult decision since there is no legal context of the Authorization to Carry (ATC) which would prohibit boarding on the sole basis of suspicion. The Commission rejected the idea of a centralized database for collecting and processing PNR in its 2008 report, therefore recommending that each State manages its own system. However Article 11 details how PIUs from Member States might exchange information between themselves and third countries, under certain conditions; this new possibility will certainly contribute to a better cooperation at international level to meet criminal activities.

PASSENGER AUTHENTICATION

Passenger authentication remains a critical concern. Security staff are not allowed to control ID and travel documents within the Schengen area, which is a true paradox. For this reason a reconciliation

Revolutionary Inline Production Equipment for MRTD Products



Multiple Unwind

- ▶ Highest automation level for maximum accuracy, security and yield rates
- ▶ Shortest lamination times
- ▶ Minimum demand of operators, floor space and energy
- ▶ Inline efficiency and flexibility



Collation



Lamination



Punch + Test



INNOVATIVE MACHINERY SOLUTIONS SINCE 1956

MELZER[®]

Please visit us at: 13th ICAO TRIP · Montreal, Canada · Booth: 50
TRUSTECH · Cannes, France · Booth: RIV A054 | INTERGRAF · Dublin, Ireland

www.melzergmbh.com



Automatisierte Grenzkontrolle

Automated border control



procedure shall be implemented between an individual and his evaluated risk to make sure that differentiated measures can be applied if required. Additionally, paperless procedures – online registration, automatic baggage drop-off – tend to eliminate any contact between travelers and carriers until boarding.

For air carriers, Regulation 300/2008 imposes no obligation on airlines to check ID documents. The responsibility of the airline is therefore limited to verifying the possession of a travel document and not their legitimacy. “(b) The carrier shall be obliged to take all the necessary measures to ensure that an alien carried by air or sea is in possession of the travel documents required for entry into the territories of the Contracting Parties.” The highest penalty is not huge but there are costs associated with hosting irregular travellers and incurring legal proceedings; and penalties that are aggravated by Directive 2001/51/EC of 2001.

With hundreds of different passports types in circulation, ID reconciliation at airport checkpoints could be performed by means of a reader interface with a database of existing documents. ICAO's Public Key Directory (PKD) government certificates management system has not been endorsed all States, so the risk remains of legitimizing a 'true-false' passport that contains a traveller's credentials and his biometrics, but has not been issued by a government. This sophisticated deception may diminish the airlines' responsibility in the future if the police themselves are no longer able to confirm the legitimacy of a travel document.

A lack of strong identity authentication procedures seems antithetical to data processing which - collected online – might contain mistakes. This is a weakness that has been identified by IATA with their recommendation of the provision of a 'document check' in the context of their 'Fast Travel' programme. Indeed, the APIS directive imposes no obligation that carriers verify the accuracy of collected data by scanning the passport MRZ. This issue could motivate an evolution of the text by the EC. Various technical solutions already exist to confirm the quality of transmitted data whilst ensuring that a passenger is not 'flagged' by government authorities: Interactive APIs (iAPIs) and Advanced Quick Query (AQQ) systems which are directly operated from checking counters.

Border authorities could certainly also better exploit the various information that individuals currently put on social media (Facebook, Twitter, LinkedIn, etc) since they can be accessed without restriction if the owner decides to make them public. By combining APIs, Departure Control Systems (DCS) and PNR with data analytics, border authorities will be able to build a comprehensive profile which can be further exploited before border crossing. But this approach shall be considered with care, since individuals might artificially display a trustworthy public life for hiding bad intents. For these reasons, security controls shall be complemented by other unpredictable techniques such as random checks or human behavior analysis. ■



ICAO

UNITING AVIATION

For a full list of upcoming events visit: icao.int/meetings



SAVE THE DATE

2017 Events on the horizon

30 Oct. - 17 Nov.	ICAO Council 212th Session - Council phase	Montréal, ICAO HQ
20 - 22 Nov.	Second Global Runway Safety Symposium	Lima, Peru
20 - 22 Nov.	ICAO World Aviation Forum - Financing the Development of Aviation Infrastructure	Abuja, Nigeria
20 - 22 Nov.	ICAO ATFM Global Symposium (ATFM2017)	Singapore
27 - 28 Nov.	ICAO Next Generation of Aviation Professionals (NGAP) Global Summit	Montréal, ICAO HQ
28 - 30 Nov.	ICAO TRIP Regional Seminar Jamaica 2017	Montego Bay, Jamaica
29 - 30 Nov.	Seminar on Green Airports	Montréal, ICAO HQ
4 - 8 Dec.	ICAO Air Services Negotiation Event 2017	Colombo, Sri Lanka
11 - 15 Dec.	Second Global Air Navigation Industry Symposium (GANIS/2) and First Safety and Air Navigation Implementation Symposium (SANIS/1)	Montréal, ICAO HQ

* All event dates are subject to change

For more information regarding sponsorships and exhibitions, please contact mcr@icao.int

AIRCOP

THE UNODC AIRPORT COMMUNICATION PROJECT



Despite global efforts to fight drug trafficking, criminal behavior and corruption affects the security of all States. Every day transnational organized crime occurs through various manifestations – couriers, cargo or postal mail – at airports around the world. To disrupt these activities and networks, the United Nations Office on Drugs and Crime (UNODC), in partnership with INTERPOL and the World Customs Organization (WCO), implemented the Airport Communication Project (AIRCOP).

AIRCOP is aimed at building and strengthening the capacity of participating international airports in the African, Middle East, Latin American and Caribbean Regions to detect and prohibit illicit trafficking (drugs and other illicit goods) and suspicious passengers, in origin, transit and destination countries. The project is funded by the European Union (Cocaine Route Programme), Japan, Canada, Norway and the United States.

BACKGROUND

From 2010, when UNODC launched AIRCOP in partnership with INTERPOL and WCO to today, the project has expanded from eight to 33 countries in Africa, Latin America, the Caribbean, and recently the Middle East, with the potential to further expand to other regions. AIRCOP's initial implementation phase focused on illicit drug trafficking by air passengers and in cargo and air mail parcels. Subsequent project phases have steadily broadened AIRCOP's geographical and substantive scope to include terrorism related passenger and cargo activities.

In the framework of UNODC's mandate as custodian of the three UN Drug Control Conventions of 1961, 1971 and 1988, AIRCOP contributes to strengthening Member States' cooperation, supporting their national agencies to counter the world drug problem and criminal activities related to drugs, as urged by the Commission on Narcotic Drugs through resolution 56/16 dated 2013. AIRCOP further contributes to implementing UN Security Council resolutions 2178 (2014), 2214 (2015), 2253 (2015) and 2309 (2016), by assisting Member States in complying with international obligations to deter travel of suspicious passengers and potential foreign fighters, and counter threats posed to civil aviation.

Training, mentoring and joint operations have led the Joint Airport Interdiction Task Forces (JAITFs) established through AIRCOP, to seize 3,174 kg of cocaine, 1,417 kg of cannabis, 1,230 kg methamphetamine, 168 kg of heroin and 18,5 kg of amphetamine. As AIRCOP expanded its work to include other types of threats, the task forces seized 1,397 kg of counterfeit medicines, 541 kg of ivory, USD 6.5 million, fake passports and ammunitions and intercepted several potential foreign terrorist fighters. From 2011 to 2017, the different task forces recorded over 1,100 arrests and seizures, both in passenger and cargo areas.

PROJECT STRUCTURE

AIRCOP brings together different law enforcement agencies and associates the private sector (airlines) to strengthen capacities in combatting illicit trafficking, organized crime and terrorism. The project is implemented around three pillars.

Firstly, it supports inter-agency cooperation through the establishment and operationalization of Joint Airport Interdiction Task Forces (JAITFs), or through the empowerment of existing structures.

JAITFs are composed of relevant law enforcement authorities who operate at the airport (police, customs, immigration services, national security and airport authorities). AIRCOP encourages governments to include as many relevant agencies as possible in the task force, including specialized police forces and the intelligence units tasked with tracking and fighting terrorism and organized crime. AIRCOP also provides JAITFs with equipment (including office equipment) and detection tools (for drugs, explosives or fraudulent documents) as needed.

“AIRCOP brings together different law enforcement agencies and associates the private sector (airlines) to strengthen capacities in combatting illicit trafficking, organized crime and terrorism.”

The added value of a JAITF is to leverage the skills, competencies and mandate of each of these law enforcement agencies. Such capabilities and mandates allow for detection and interdiction actions with a greater and deeper impact. Additionally, decentralized information sharing among agencies in the context of a JAITF increases the volume of information available, and allows for advanced information which can quantitatively and qualitatively improve operations. JAITFs can adopt a more proactive and analytical approach that contributes to more effective and efficient airport security control.

Secondly, AIRCOP facilitates secure real-time transmission and sharing of information between law enforcement services at national, regional and international levels.

AIRCOP provides JAITFs with a direct connection to INTERPOL I-24/7 databases and the WCO's CENcomm secure communication network to enable real-time, direct airport-to-airport communication of operational information aimed at detecting and intercepting suspicious passengers.

Thirdly, AIRCOP promotes an intelligence-led approach by providing JAITFs with training, mentoring, detection tools and technology and by involving them in exchange programmes and world-wide joint operations.

AIRCOP supports the capacity building of JAITFs and other similar existing structures at different layers of airport security:

- **Physical Screening:** AIRCOP trains and mentors JAITFs and other mandated agencies on basic and advanced physical screening of passengers and luggage, inspection and search techniques and detection technologies.
- **Profiling and targeting:** considering the growing threat to civil aviation, adding layers of screening could create bottlenecks easily targeted by terrorists. AIRCOP therefore advocates for an intelligence-led approach through profiling and behavioural analysis without impacting the day-to-day operations of commercial airports. AIRCOP provides training on the latest profiling and targeting methods with a focus on identifying suspicious passengers, freight and postal packages as well as intelligence collection and sharing.
- **Prevention:** AIRCOP trains JAITFs on risk assessment.

In the framework of AIRCOP, the training and mentoring activities are provided by French Customs and Police, Belgian Customs and Federal Police, Swiss Customs, Italian Guardia di Finanza, Brazilian Federal Police, Brazilian Customs, Portuguese Customs and Police, United Kingdom Border Force and National Crime Agency, Dutch National Police, Canada Border Services Agency, Spanish National Police and Niger Customs, in addition to the three project partners UNODC, INTERPOL and WCO.

With a view to increasing the quantity and quality of data available for the profiling, targeting and risk analysis, AIRCOP supports JAITFs in reaching agreements with airlines companies on the exchange of Advanced Passenger Information (API) and Passenger Name Records (PNR) and to extend its partnership and collaboration with ICAO and IATA, offering JAITFs as privileged entry points.

JAITFs are also involved in world-wide joint operations organized by WCO, INTERPOL and other law enforcement actors, to intensify surveillance and controls at international airports and to facilitate and ensure communication and information exchange between airports.

PROJECT MANAGEMENT

UNODC implements AIRCOP in partnership with INTERPOL and the WCO. The main project offices for AIRCOP are based in the UNODC Regional Office for West and Central Africa in Senegal, at the UNODC Regional Office for Central America and the Caribbean in Panama and at the UNODC Regional Office for the Middle East and North Africa in Egypt. INTERPOL and WCO joint operations are coordinated from their respective headquarters in Lyon and Brussels. ■

↓ FACTS AND FIGURES

33

AIRCOP PARTICIPATING STATES OF WHICH:

- 20 operational JAITFs
- Two JAITFs established
- Three JAITFs under establishment
- Three associate States

16

JOINT OPERATIONS

(including WCO COCAIR, INTERPOL FOLOSA, Ailes Africaines of the French Customs and Europol Global Airport Action Days)

2

CANINE TEAMS TRAINED AND OPERATIONAL

30062

 | PEOPLE TRAINED

- through 200 training and mentoring actions
- 20% women

TOTAL SEIZURES AND ARRESTS:

OVER 1100 PERSONS

USD 6.5 MILLION

of undeclared currency; numerous fraudulent passports and ammunition, as well as five potential foreign terrorist fighters.

	(Kg)
COCAINE	3,174
CANNABIS	1,417
HEROIN	168
METHAMPHETAMINES	1,230
AMPHETAMINE	18.5
COUNTERFEIT MEDICINES	1,397
IVORY	541

↓ PARTICIPATING STATES

AFRICA:

Benin, Burkina Faso, Cabo Verde, Cameroon, Côte d'Ivoire, Ethiopia, Gambia, Ghana, Guinea-Bissau, Kenya, Mali, Mozambique, Niger, Nigeria, Senegal, South Africa and Togo

LATIN AMERICA AND THE CARIBBEAN:

Argentina, Barbados, Bolivia, Brazil, Colombia, Dominican Republic, El Salvador, Jamaica, Panama and Peru

MIDDLE EAST:

Algeria, Jordan, Lebanon, Morocco, Tunisia and Turkey

THE DUTCH NATIONAL VERIFICATION SOLUTION FOR eDOCUMENTS



COR DE JONGE

He is the Manager of PKI, Business Unit Technology at the Ministry of Security and Justice in the Netherlands. In the last 12 years, he was involved in several government projects in the field of Information Technology. Currently he leads the development and implementation of the Public Key Infrastructure Extended Access Control (PKI EAC) for border management and immigration. He is a Member of the ICAO PKD Board and chairs the Contract Support Group that tenders new PKD service providers.



JEEN DE SWART

He is the Senior Information and Security Architect PKI, Business Unit Technology at the Ministry of Security and Justice in the Netherlands. For more than 20 years he has worked for the Ministry of Security and Justice in various roles, with a focus on security, public key infrastructure and identity and access management. He has been the architect and advisor for large scale IT-projects, and for the last five years Jeen he was involved in the PKI EAC of the Netherlands, including biometrics, for the Ministry for Security and Justice on behalf of the Judicial Information Service. Jeen is an alternate Member of the ICAO PKD Board.



States need to be able to validate ePassports if they are going to fully leverage the significant investments they make to develop them. Authentication involves a process that validates the authenticity and integrity of an ePassport by verifying the digital signature on the chip. For border control (of a receiving State) to verify the ePassport of a foreign traveller, the receiving State needs access to information from the issuing State.

ICAO's Public Key Directory (PKD) provides a central repository for the information required to authenticate passports to be exchanged. There are many security and facilitation advantages of having an ePassport that are grounded in the presence of an integrated closed circuit chip, but they can only be realized when border control authorities authenticate the chip.

States would benefit from applying a National Public Key Directory (NPKD) solution, besides ePassports, to other identification documents (i.e. residence permits, driving licenses, etc.), along with a Document Verifier Registration Authority (DVRA) that contains the necessary verification certificates for accessing private, sensitive, biometric information.

Certificates could be provided to the national borders for checking e-documents like automatic or Assisted Border Control (ABC) gates. Besides national borders, these certificates could also be shared with the military, police control and immigration services. This article describes the possible architecture and infrastructure for this kind of solution, based on what has been implemented within the Netherlands; it points to important components without naming vendors or commercial influences.

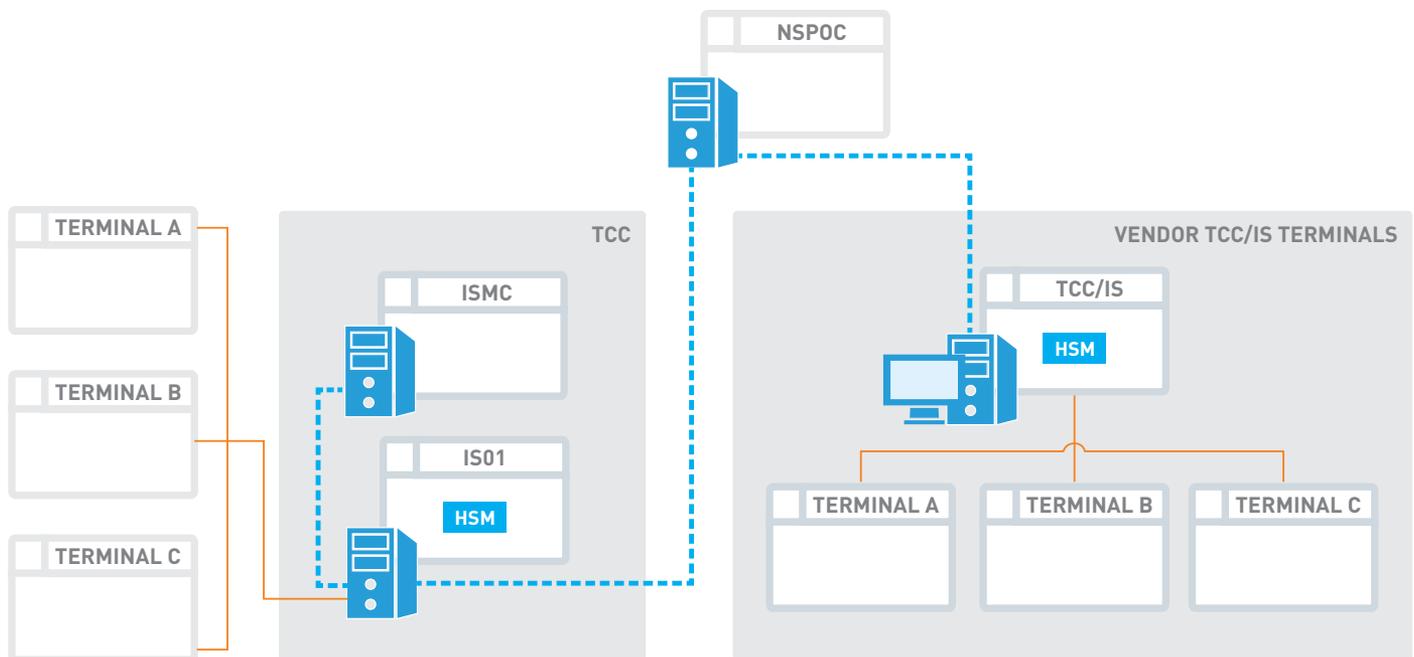
Using a NPKD would allow for responsible governments to be the trustworthy, central body responsible for providing necessary certificates to national and commercial bodies with the purpose of checking the genuinity of the e-document chips' content. It would be at the discretion of the national government to decide to which bodies these certificates – or part of the certificates – are provided.

A NPKD is part of a total (private) infrastructure which serves different domains (for different inspection bodies or organizations), each disclosed by a National Single Point of Contact (NSPOC). Not only the NPKD but also the Verification PKI – which is needed to protect sensitive information on the eDocument chip – can be disclosed through a NSPOC and, possibly, other necessary registers or databases.

Terminals (devices with an eDocument reader) can be managed by a terminal control centre (TCC). These TCC's are connected to the domain's NSPOC and have a specific interface specification to provide all the necessary functionality to the terminals – like providing the certificates from the NPKD.

THE ARCHITECTURE

The Dutch NPKD is a Lightweight Directory Access Protocol (LDAP) directory that contains national and international certificates from the signing hierarchy of eDocuments. These certificates are necessary for terminals (devices with eDocument



readers connected) to check the genuinity of eDocuments (called passive authentication). A NPKD can contain certificates (CSCA certificates and DS certificates), Certificate Revoke Lists (CRLs), Masterlists and Defectlists.

Masterlists and Defectlists can be seen as a signed container of certificates within the NPKD, and are the responsibility of the government. Because the process of importing certificates into the NPKD is never automatic, there is a role of a NPKD Manager who is responsible for importing them. Masterlists and Defectlists are available from trustworthy sources (like ICAO PKD) but it is the NPKD Manager (a governmental employee) who decides which certificate will be imported from trustworthy, or other bilateral sources or websites.

A government should have a policy authority, a responsible body who governs the process of handling and importing the certificates. With these procedures the NPKD Manager is able to import certificates and verify them against ICAO Machine Readable Travel Document (Doc 9303) specifications. It is the NPKD Manager who decides within the NPKD for which Inspection Body the certificates are available.

A NPKD is part of a total (private) infrastructure which serves different domains (groups of inspection bodies with a same functionality) each disclosed by a National Single Point of Contact (NSPOC). Border control as an inspection body is connected to NSPOC. For example, the National Police as an inspection body are connected to another NSPOC, both getting different or the same certificates.

NSPOC's can be seen as virtual querying users to the NPKD. If within a domain (group of inspection bodies with a same functionality), verification of private information (like fingerprints) in the chip is necessary for inspection purposes, the NSPOC can also be connected to the Document Verifier Registration Authority (DVRA).

From this server the necessary certificate chain for the inspection systems (IS) will be provided.

Communication to and from the NPKD and NSPOC is always secure using special certificates. The NPKD and NSPOC are manageable through a graphical user interface (GUI).

The NSPOC delivers a secure web service with Simple Object Access Protocol for exchanging structured information (SOAP) messages which can provide the Signing Certificates (CSCA's and DS'), CRL's, Masterlists and CA Chains (for verification PKI) also called "interface specifications".

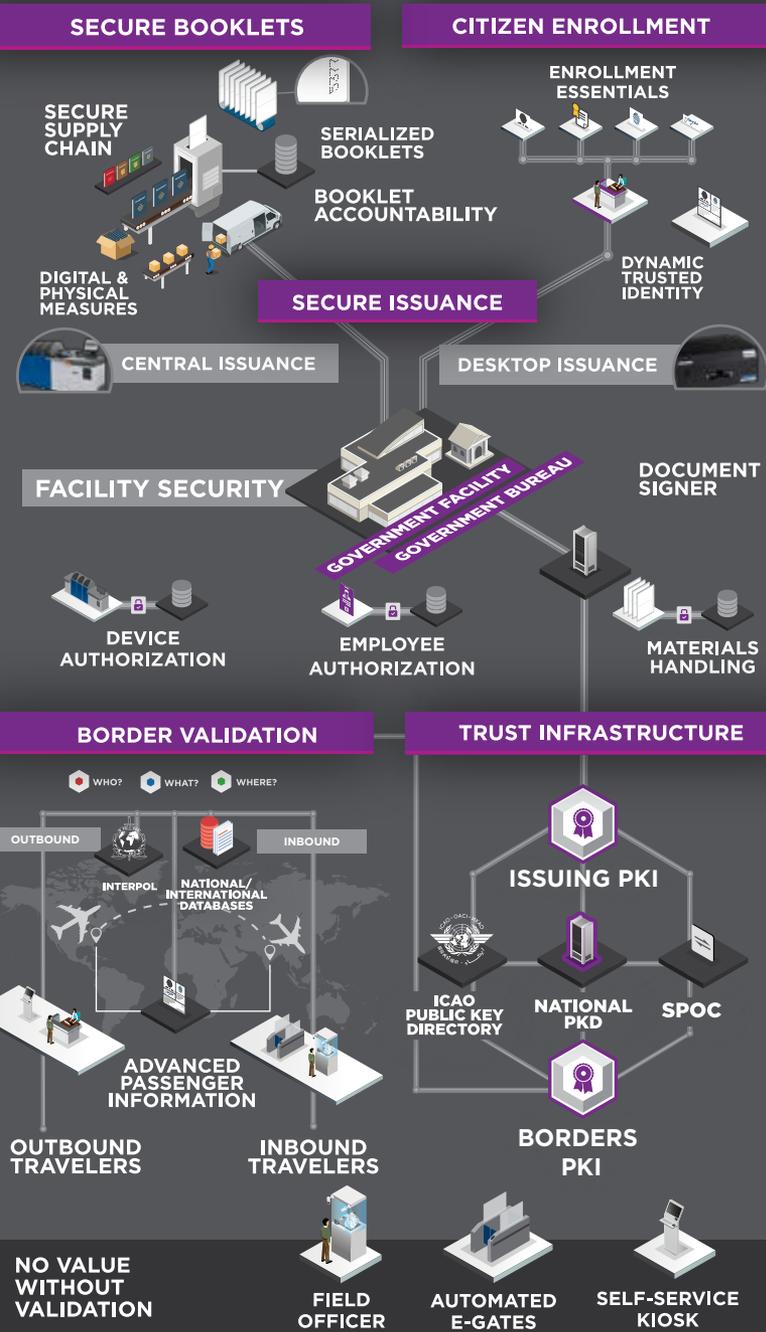
Let's consider the example of border control with Terminal Control Centres (TCCs) that are connected to the NSPOC. There are actually two possibilities of border control terminals (devices with eDocument readers connected, like ABC gates) for border control, with the manufacturer of the terminals delivering his own TCC, or ones that are dependent on a central governmental TCC. In both cases there is an Interface Specification for the necessary SOAP messages.

A dedicated TCC consists at least of two inspection systems (IS) and a management console for the inspection systems (ISMC). The IS contains a certificate store of CSCA's and CRL's (synchronized with the NPKD) and can contain hardware security modules (HSM) for the verification chain (EAC PKI). The most common practice is that the ABC systems only need the Country Signing Certificates (CSCA's), and for secondary inspection the Verification Chain (for fingerprint inspection). A TCC is a secure "black box" with two router-firewalls, one with a secure connection to the NSPOC, and the other with secure connections to the terminals (devices with eDocument readers connected, like ABC gates). Which functionality per terminal is allowed (in the interface specifications as web service) can be managed by the ISMC.

MODERN BORDER SECURITY

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

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



SEE THE TRUST INFRASTRUCTURE INFOGRAPHIC IN FULL DETAIL AT WWW.ENTRUSTDATACARD.COM/BORDERS

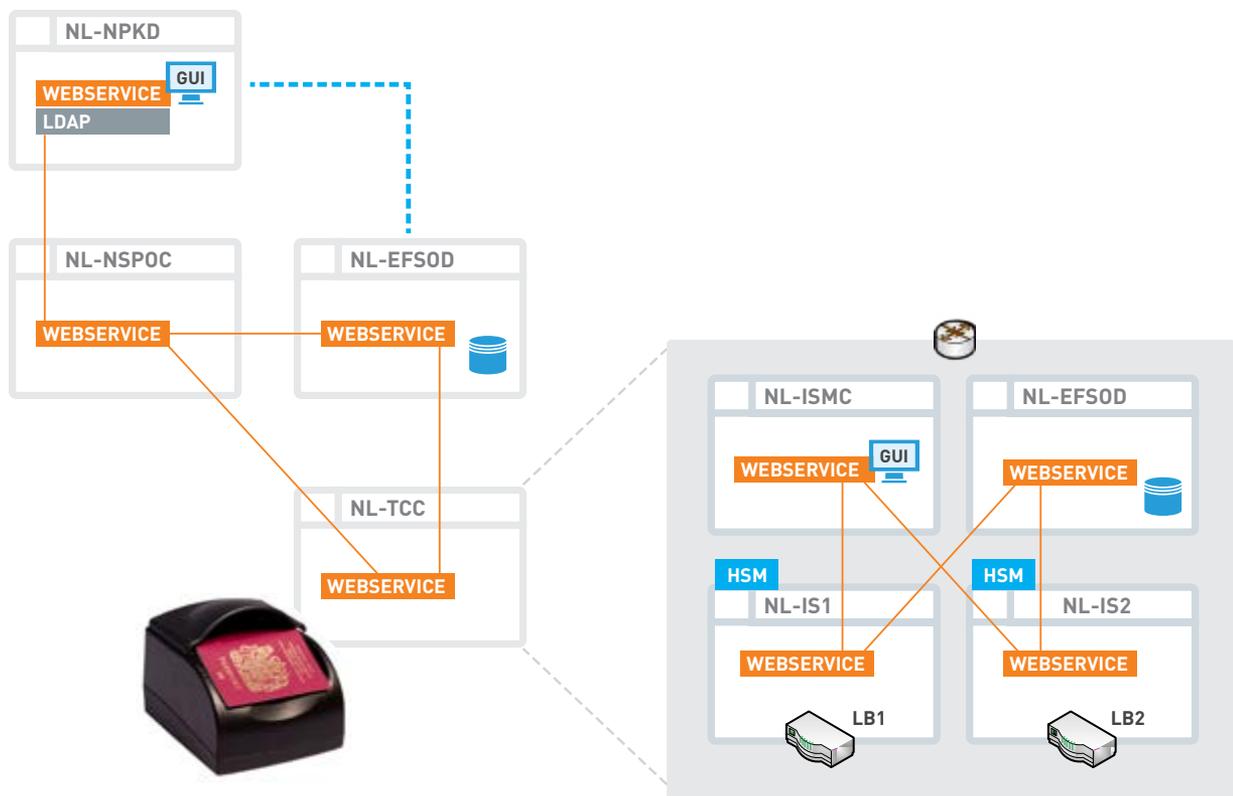
In the case of ABC systems there are two possibilities for getting the CSCA's and CRL's. There is a "pull" mechanism: the ABC gates implemented the interface specifications and asked (pull) for the certificates and CRL's every half an hour, or there is a "push" mechanism: the ABC gates are web service activated, implementing the interface specifications and besides asking (pull) for the certificates, from the NPKD the certificates can be pushed to the ABC systems. Which mechanism is implemented depends on the manufacturer of the ABC gates.

Besides the dedicated TCC there can be a so called "EF.SOD-server" which is a dedicated database server containing all the information about the chip inside an eDocument. If an eDocument is electronically checked, the reader can upload the Secure Object File (EF.SOd) from the chip to the database server using the interface specification given by the TCC. The database server extracts the Document Signer Certificate from the EF.SOd file together with information about the chip security protocols. After collecting this information centrally, the EF.SOd file will be deleted. The central database can be used to verify country certificates against Doc 9303, and can then provide information for setup of the terminals (devices with eDocument readers connected, like ABC gates) to verify the eDocument chip security.

If private information (i.e. fingerprints) in the chip is necessary for inspection purposes, the NSPOC, as a broker, will be connected to the DVRA. The DVRA is the management console for the Verification Certificate Chain to the Inspection Systems within the TCC's. A verification certificate chain contains the Country Verifying Certificate Authority (CVCA), the Document Verifying Certificate Authority (DVCA), the inspection system (IS) and its private key. From every country's eDocument private sensitive information (i.e.fingerprint) needs to be read and their country CVCA and their CVCA signed National DVCA needs to be provided. By uploading these certificates within the DVRA, the authorized Inspection Systems within the TCC automatically creates the IS certificates and keys. With the ISMC, the connected terminals (devices with eDocument- and fingerprint-readers connected) can be authorized to use this functionality.

The DVRA is connected to the National CVCA and DVCA. For exchanging internationally CVCA certificates and DVCA's for authorization, and for reading each other's private sensitive data (like fingerprints) from the chip, there is a Single Point of Contact (SPOC) with functionality that is developed in Europe. For security reasons this SPOC could be split into a SPOC-external and SPOC-internal. The SPOC-external is placed into a demilitarized zone (DMZ) and creates the secure connection to the Foreign SPOC while the SPOC-internal is taking care of the SPOC functionality.

There is a role of a PKI Officer who is responsible for signing a foreign DVCA request by the national CVCA. After thoroughly checking the request procedure and certificates, and with permission of the national policy authority, a foreign DVCA request can be signed. For this procedure there is a Country Verification



“If private information (i.e. fingerprints) in the chip is necessary for inspection purposes, the NSPOC, as a broker, will be connected to the DVRA.”

Registration Authority (CVRA) which is placed between the National CVCA and SPOC-internal.

THE INFRASTRUCTURE

The architecture for the national verification solution described above needs to be placed in a secure environment. This can be carried out by creating several segmented and separated environments by VLAN's (Virtual Local Area Networks). VLAN's are mutually isolated and can only be accessed by routers and firewalls. This solution is a part of the security and input for a risk analysis. Within this architecture there is a demilitarized zone (DMZ) for the systems connecting to the private or public network (for example the NSPOC), a ROOT environment for example the Root CONNECTCA, a production environment (PROD) for the NPKD, a Management environment (MGMT) for the Monitoring and Administrating systems and a Preproduction environment (ACPT).

Beside these environments there is a specimen environment (TEST) for creating, testing and developing. The VLAN environments can be stretched over a wide geographical area; where possible the systems, as described in the architecture, are virtualized (virtual machine) using servers with hypervisors. For systems needing a hardware security module (HSM), the choice would be to use a network attached HSM (netHSM) or within the server installed HSM (PCI-HSM). The benefit of netHSM's is that all the systems can be virtual machines. For storage the virtual machines can use the storage area network (SAN). The final solitary virtual environment for PKI services depends on governmental security procedures regarding networks (firewalls and routers).



Self-service passport control

Passports with  logo | 16+ | No ID card



For passengers with passports from EU / EEA and CH:



EU / EEA



Switzerland

and passengers with passports from:



Australia



Canada



Hong Kong



日本国



New Zealand



대한민국



Singapore



United States
of America

THE ORGANIZATION

Depending on the governmental organization there are different roles and responsibilities for the different systems as described in the architecture. Overall governance falls on a policy authority that gives direction to the signing PKI, verification PKI and authorization to the TCC for connections of terminals and providing certificates. This article doesn't describe in detail all the responsibilities and roles for all the systems but gives a global view.

Roles must be seen as descriptive and can be shared between employees. The total solution is part of the security and input for a risk analysis but it is very important that there is enough knowledge within the governmental organization to manage and operate the different systems as described in the architecture. Furthermore, the role of architect is necessary for keeping track of all worldwide changes and for incorporating these changes in the organizational architecture.

THE SETUP AND COSTS

For the purpose of this article the estimate of costs are given in time, for personnel and necessary devices and it is restricted to the architecture (without terminals and EAC-PKI). The first step in the development must be an architecture that identifies and describes the necessary and future functionality for every system needed. The setup of this architecture and the description of the systems will take approximately three to six months for one architect.

Architecture will be submitted for development or tender. To develop the systems (applications), as described in the architecture, two

developers need approximately six to twelve months. If it is a tender, it could take approximately eighteen to twenty-four months. During setup an auditor and security officer should be involved. The infrastructure is also part of the architecture and must be setup with IT management.

Setting up the physical servers, storage, implement the hypervisor and setting up the virtual machines will take approximately one to two months. While IT management is being setup, the security officer and network management will deal with the virtual network setup and firewall and router rules. To manage all this setup there should be a project manager and Policy Authority already in place. There will be costs of physical hardware (servers), storage (SAN), hypervisors, firewalls and routers. Extra costs will be needed for HSM devices that are needed for CONNECTCA, for inspection systems and for future EAC-PKI. Virtual machines need an operating system (OS) which can be a free or paid OS. Depending if the government wants to go to tender there will be costs of the functional software releases to build the system (applications) as described the architecture. For own development there will be costs of databases, middleware and application software (web services and GUI). With a tender the costs are hard to predict, additional costs will be incurred for training personnel.

While the architecture and infrastructure described in this article provide an overview for how this has been implemented within the Netherlands, technical details are complex and out of scope for this article. We welcome your questions and feedback; you can contact us by email at j.deswart@justid.nl and c.dejonge@justid.nl ■

ICAO TRIP



To download a copy
of this publication
FOR FREE

Simply go to:
unitingaviation.com/tripcompendium

To contribute content or advertise with us
in the next ICAO TRIP Strategy Compendium,
ICAO TRIP Magazine or on unitingaviation.com
contact us at mcr@icao.int

icao.int/ads



ICAO

SECURITY & FACILITATION

VERIDOS

IDENTITY SOLUTIONS

by Giesecke+Devrient
and Bundesdruckerei



Veridos Secures Identities

Identity Solutions. Veridos GmbH is a joint venture between two of Germany's best known providers of secure government solutions, Bundesdruckerei GmbH and Giesecke+Devrient GmbH. Having inherited extensive technological expertise from its parent companies, Veridos has risen to become one of the top-tier companies producing, implementing and managing high-tech and future-proof identity solutions. Find out more about how Veridos can help you make the most secure decision and visit us at ICAO's TRIP Symposium in Montréal, October 24th to 26th, 2017, booth 11.

www.veridos.com/ICAO