**PASSPORT INTEGRITY WORKSHOP**

**Ministry of Foreign Affairs Headquarters**

**Mexico City, Mexico,**

**July 17-18, 2017**

**REPORT DAY 1**

**17 July, 2017**

**Opening Remarks**

UNODC, in its welcome remarks, gave us a historical account of the origins of the passport, dating back to biblical and medieval times, as well as the characteristics of the first passports. Progressively, the passports were folded, the photography and the security paper were inserted.

Mr. Felipe De La Torre commented on how the black market benefits from the falsification of passports. The issuance of apocryphal documents is a crime, from which trafficking and smuggling networks take advantage. UNODC, through its #DeadlyBusiness campaign, is aware of the relationship between smuggling crimes and the use of fraudulent passports.

The United States, represented by Minister Counselor Ian Brownlee, emphasized that governments in the region must work together to combat trafficking and smuggling offenses.

Jason Hollman of Canada, emphasized the use of fraudulent documents and irregular migration and the importance on how the incursion of new technologies can help us to combat organized crime.

Vice-Minister Liduvina Magarín noted the importance of keeping up to date with the international standards for the issuance of passports.

The Undersecretary for Latin America and the Caribbean, Socorro Flores, from the Ministry of Foreign Affairs of Mexico, highlighted the relevance of this workshop, and the challenges we have as a region. The exchange of information is vital to combat organized crime.

**Session 1: International Context and Secure Travel**

Mr. Felipe De La Torre made the reminder that on April 4, UNODC launched the #DeadlyBusiness campaign in Washington DC, to make visible the links of the smuggling of migrants with other manifestations of organized crime, where the use of fake passports is not excluded.

Mr. Arnulfo Cristancho, on behalf of Migration Colombia, recounted extra-regional migrations in Colombia, with reference to the new routes that are taking irregular migratory flows. He emphasized the factors associated with irregular migration in Colombia and the impact of migrant smuggling in countries of transit, destination and origin. Likewise, progress made by institutions in the area of ​​migrant smuggling, with the support of UNODC.

Migration Colombia has readers of passports, mobile equipment and doors for automatic migration.

Since 2010, the Colombian passport complies with ICAO standards and since 2015 the chip has been incorporated.

IOM shared some thoughts on how we can implement actions on passport security.

IOM shared the risk of illegal border crossing methods, with three levels:

Lowest risk: with an official passport (stolen)

Medium risk: As an impostor or pretending to be someone else.

High risk: False or fraudulent passport

Often the use of fraudulent passports is by ignorance, when used by people who are victims of smuggling of migrants or trafficking persons.

The biggest vulnerability is not passport fraud, but the process of issuing passports and the lack of security elements in the integrity of passports.

The basis is the identity management system, followed by document security and then border security.

IOM shared important reflections on the need to make the leap into the electronic passport. An electronic passport does not have much use if it is not used properly. Agencies should support countries in deciding their needs and options, in ensuring quality (including compliance with ICAO standards), and in supporting countries not to waste resources.

IOM shared its priorities for assistance, including support for countries to conduct passport and border integrity procedures, as well as training of border officials and evaluation mechanisms.

The more needs and challenges are known, IOM and ICAO can translate them into technical assistance projects.

**Session 2: International Requirements, Standards and Best Practices.**

Presentation on International Requirements, Standards and Best Practices

Ricardo Delgado, ICAO

As a part of the United Nations, ICAO should harmonize its objectives with the Sustainable Development Goals, including among others, gender equality, decent work, reduction of inequities, land and life protection, justice and peace to reinforce the institutions of different governments.

More than half of international movements are by air, that is why we need to strengthen documentary security at airports.

Annex 9 integrates the standards and recommended methods for the entry of aircrafts, passengers and luggage, cargo and mail.

Countries should have the means to coordinate compliance internally, for example civil aviation authorities with the respective immigration control police.

ICAO standards go beyond recommendations, the application of standards is necessary for international air regulation. Even if they are not "mandatory", uniform application is recognized as necessary and desirable.

Countries should notify ICAO which standards or recommended methods they are unable to comply.

Countries should join the Public Key Directory (PKD), if they issue electronic travel documents, by means of a chip, so that the information is exchanged by other countries that issue electronic passports, so that the information can be read and exchange information in real time.

Countries are required to report to INTERPOL the loss, theft or revoked of passports or passports that have been withdrawn from the system (expired, cancelled, and damaged). Also, a database must be created, with a public nationwide infrastructure.

While travel documents must be machine-readable since 2005, in many countries they were deceived by vendors who sell passports.

Mr. Delgado stressed the importance of sharing limitations with other countries to prevent their electronic travel documents from being blacklisted.

Countries should have an Advance Passenger Information System (API), with data which must be on the first page of the passport. States should look for secure mechanisms for the transmission of information and not use email accounts such as Hotmail or Yahoo, and never use social networks.

Currently, the issuance of electronic passports is not a standard; however an electronic passport provides us with more security than a machine-readable travel document.

It is important to take into account the control in the safekeeping, custody and storage of passports, as well as inspection systems and tools.

Civil Aviation authorities are the direct link with ICAO. They have an immediate contact, without having to report to the Ministries of Foreign Affairs.

ICAO listed the agencies that should be part of the Committee for the implementation of the National Air Transport Program, as well as the National Identity Authenticity Strategy.

Verification and control rests with the border control authorities. Hence the importance of coordination between the authorities in charge of issuing travel documents and the border control authorities.

You have to take into account the privacy of the information.

In the session of questions and comments of session 3, important reflections were made about the protection of minors.

It reiterated the importance of sharing the problems faced by countries, in order to help ICAO solve the problems and provide timely follow-up.

Mexico highlighted the contact with Migration Colombia, within the framework of the dialogue with the South American Conference on Migration, in the follow-up to the ad hoc Group on extra-regional migrants. The issue shared by Migration Colombia is one of the topics to be addressed in the dialogue between CRM and CSM.

**Session 3: Implementation Support Tools**

Ms. Nicoletta Bouwman from the Canadian Ministry of Immigration, Refugees and Citizenship, shared the standards and recommended practices in the ICAO Guide and Annex 9.

The guide includes good practices on the safe issuance of travel documents and a guide for evaluation.

Ms. Bouwman commented on the importance of focusing on the issuance process.

The guide helps authorities to evaluate their emission system by themselves and that qualified evaluators can evaluate the issuance system of another country. The guide is not an exam; it is a tool to improve the process.

Mr. Omar Lemus Loarca of Guatemala shared his experience in the process of custody and issuance of passports, in three phases: 1) purchase of booklets, 2) reception and receipt, and 3) procedure for issuing and delivering passports.

**Session 4: Integrity Touchpoints and Key Challenges**

Mr. Malcolm Eales, Director Risk Integration, from the Canadian Passport Program, Immigration, Refugees and Citizenship, shared key issues regarding passport integrity from the Canadian perspective. Canada highlighted three key components of passport integrity: issuing a secure document, ensuring a solid issuing process, and managing passports in circulation.

One challenge is how to ensure integrity when we have online application processes. The answer is in the same technology. Likewise, challenges regarding lost and stolen documents, integrated fraud and the mitigations that we must face at borders.

Mrs. Martha Martinez Mendoza gave a presentation on the experience of Mexico in the process of issuing passports. It is important to find the balance between security processes and the constant protection of information. The Mexican passport has been built based on what have constantly been attacks on the integrity of the document. Mexico has implemented best practices to prevent fraud, including identity and nationality, with the presence of the applicant, as well as the capture of biometric data. When a user requests their passport on a recurring basis, INTERPOL is contacted and an alert is issued.

**Session 5: Facilities Management**

Mr. Jeff Cooley, Head of the Department of State's Internal Control Division, shared the US experience with the controls and protocols they use at the facilities where passports are issued. Mr. Cooley referred to the numbers, demand, number of employees, agencies, service stations and demand projections for the 2017, 2018 and 2019 passport services.

In terms of security of facilities, multiple protocols are used, for example: entrance of cleaning staff, entrance of guests, security plans, entry of electronic devices, lockers for protection of belongings, waste management, computer systems, etc.

The Internal Control Division implement self-assessment systems and Score Cards to identify achievements and performance.

**CONCLUSIONS DAY 1:**

* Exchange of experiences and learning in the whole process of issuing travel documents, in a regulation, challenges, lessons learned and good practices.

Some points to be taken into account by RCM Member Countries are:

* Consider the substantive increase in the flow of extra-regional migrants in RCM countries and continue to promote campaigns in the regional and sub-regional forums in which they participate, campaigns to combat trafficking and smuggling, as well as their relationship with use of fraudulent passports.
* The UN agencies involved in this workshop, IOM, ICAO, UNODC, are committed to supporting the RCM Member Countries in the decision-making regarding needs and options to ensure integrity in the issuance of travel documents (including compliance with ICAO standards) and to support the countries to concentrate resources.
* As suggested by INTERPOL, RCM Member Countries should have coordination arrangements for internal compliance, such as civil aviation authorities with the respective migration control policies.
* Although ICAO recommendations are not binding, RCM Member Countries should notify to this organization which standards or recommended methods are not compatible with their regulations or installed capabilities.
* Countries must join the Public Key Directory (PKD) if electronic travel documents are issued.
* Countries are required to report to INTERPOL the loss, theft or revoked of passports or passports that have been withdrawn from the system (expired, cancelled, and damaged). Also, a database must be created, with a public nationwide infrastructure.
* Countries should have an Advance Passenger Information System (API), with data which must be on the first page of the passport. States should look for secure mechanisms for the transmission of information and not use email accounts such as Hotmail or Yahoo, and never social networks.
* RCM member countries were urged to use practical tools, such as the ICAO passport issuing guide.
* From the experience of Colombia, Canada, Guatemala, Mexico, Costa Rica and the United States, recognize the common phases of countries to issue a secure document and ensure a solid process of issuance and passport management.

**REPORT DAY 2**

**July 18, 2017**

**Session 6: Identity Management and Physical Security of Documents.**

Mr. Ángel Luis Suárez Sanabria, Technical Deputy Director General, Mexico’s National Registry of Populations (RENAPO) focused on the birth certificate on line as a tool for the security of identity and documents.

Birth certificate on line will improve the recognition of legal identity. Management of identity in Mexico includes biometrical data, as well as codes and electronic signature. The birth certificate can be accessed on line through a QR code. [www.gob.mx/actas](http://www.gob.mx/actas)

Mr. Delgado, from ICAO, presented identity management as an integral system, an “ecosystem” which is interconnected between governmental and intergovernmental agencies.

Identity Evidence (EOI) is the information to establish or verify an unique identity. There should be a balance between risk and enabling or facilitating services.

Regarding improvement of travel documents, it is much harder to produce fake travel documents. As quality and integrity of travel documents is improved, objectives must be focused on the weakness of the documents.

We need a high degree of confidence on the documents we produce.

EOI based on risk: Identity risk is related with identity theft, terrorism, financial fraud. It affects the national image.

One of the main principles is to determine if the requester is related with the identity, in order to make sure that there is only one unique identity.

The requester must have a valid identity, robust, being able to give us confidence when renewing a new passport.

Verification must be done with two or more data bases, as well as other information, such as death records.

Biometrics, facial and eye iris help us to ensure the identity.

There is a Legislative impact on sharing information or protection of information. There is no “one size fits all”. There are geographic issues to be concerned.

Risk matrixes can be used by States as al tool of their “identity ecosystem”.

A high level of trust requires an average evidence rank. For example, questions on the country of origin are useful to determine whether the person is using a fake identity.

Requests must be received and directed to an unique source.

Keys for trust building: it is very important for States to establish unique identity in its system. Member countries recognized that if there is no biometrical data, the challenge is much higher.

Although physical documents are useful, they are vulnerable (baptism certificates, acts, etc.).

EOI evolution. As technology and environment is changing, Member countries should move forward too. It is very important for Member countries to implement a system of trust guide of evidence of identity, capacity building.

Isaías Antonio Maradiaga, from the Ministry of Foreign Affairs of Honduras, shared their experience in their consular agencies. There are several consulates in Central America and North America where passports are produced, while other consulates in Central America, North America, Europe and Asia focus on data collection.

Honduras produces three types of passports: diplomatic, official and ordinary passports.

Mrs. Claudia Cordero, Criminal Fraud Investigator from the U.S. Embassy Regional Security Office outlined the coordination efforts with Mexican authorities on travel documents fraud investigations. Through their training activities, they enhance the authorities capacities in techniques to identify fraud and fake passports.

In order to identify fraud, the interview is one of the first filters, followed by facial recognition.

In the questions and comments section of this session, there was an interesting comment made by Mexico regarding trusting the good will of requesters versus fraud identification techniques.

Member countries shared the information regarding systems for consulting identity on line, and whether they share the ID numbers with other documents, such as driver’s license, ID card and travel documents.

**Session 7: Passport Fraud Downstream – Responses and Law Enforcement.**

Nick Titcombe, Document Analyst & Senior Advisor, National Document Center, Operations Branch, Canada Border Services Agency presented the life cycle of a passport: model issued for 5 years, validity length maximum 10 years. Year two: fraud begins.

Canada provided an analysis on the strongest security features.

Intaglio printing is very secure, although is very expensive.

Background printing is very important too. It is very easy to detect by officers.

It is very difficult when there are simple patterns reproduced.

Sometimes color choices are commercially available. It is suggested to avoid cyan, magenta.

Microprinting

Background printing

Rainbow printing

True colors

See-through register is a feature highly recommended.

After 15 year life cycle, counterfeiters have time to complete their craft.

Tactile features can be subject to fraud too.

Optically variable ink is also an expensive feature.

At a port of entry, officers have 7 seconds to detect fraud.

If RCM Member Countries are going to use e-Passports, they should be used correctly, and join the Public Key Directory (PKD).

About 60 from 120 countries that have e-Passports have PKD.

RCM Member countries are encouraged to produce travel documents with the combination and integration of first, second and third level features.

Do not rely only on one feature, rely both on technology and human review of passports.

Martha Martínez, from the Ministry of Foreign Affairs of Mexico shared the actions in case of high visible fraud reported by Delegations. There are two interventions taken by the General Direction of Delegations: preventive and corrective actions.

Among the corrective actions, they have the void issuance of passports, and when fraud cases are confirmed, the exchange of information through the migratory alerts, and notify INTERPOL.

RCM Member Countries are encouraged to strengthen corrective actions, such as data exchange and the generation of migratory alerts.

It is important to consider good communication between government agencies

If the information is handled electronically, the research results will be more immediate, as well as the ability to respond to requesters.

On behalf of the Embassy of Canada in Mexico, Ana María Coutu, shared the procedures in order to identify fraud, type of fraud, known security characteristics and the confirmation with the issuance authority. If the fraud is confirmed, the authorities of third countries are notified.

RCM Member Countries are encouraged to exchange information and notify third countries for confirmed fraud cases when identified.

Encourage preventive measures: biometrics, facial recognition and kiosks of primary attention.

How to choose the right features when designing a new passport?

What we need is an intelligent design. Is there is no absolutely certainty, do not rely on the vendor advice.

Encourage emerging technologies, as rotation of officers is a challenge. Human component is very valuable, so it is very important to increase training in accordance with the technology innovations. If we have good technology but officers are not trained, we will not have good results. It is important to strengthen technology and training.

Countries are encouraged to identify the security features and find a balance.

**Session 8: Connection between Passport and Border and Visas**

Mr. Erik Slavenas, Identity Management and Biometrics Officer, from IOM, shared important considerations in the field, regarding passport control in borders.

What is the point in using e-Passport if in borders it will be used as a MRD?

Forensic high tech labs cannot replace passport examination capabilities made by trained officers.

Building capacities of front border officers is very important.

“The borders are no longer at the borders”.

There is a raise in the dependency on travel data and less on physical passport.

Border management is every time more based on intelligence and risks.

Mr. Slavenas shared IOM useful tools, such as MIDAS (Migration Information and Data Analysis System).

Alejandro Austria De la Vega, Liaison Director with Foreign Service, National Institute for Migration of Mexico shared the process of visa issuance authorized by the Ministry of Foreign Affairs.

Mrs. Gisela Chung, General Director of National Passport Authority from Panama, shared their experience regarding passport issuance, as well as storage.

It is important to have written procedures. Often procedures exist, but based on the shift supervisor or non-written practices.

**Session 9: International Information Sharing.**

Fabrizio Di Carlo, Specialized Officer from INTERPOL, highlighted that participants have good knowledge of INTERPOL’s activities, as well as the sharing information with this organisation.

INTERPOL shared two resolutions from the UN Security Council (1373, year 2011 and 1624, year 2005), on the importance of combatting fraud on travel documents.

Stolen and lost travel documents (SLTD) have been increasing through the years.

There is a gap between the number of passengers and the number of cases of SLTD.

SLTD has its strategic plan:

* Increment the number of information shared by countries.
* Reduce the number of hits (administrative searches generated by documents).
* Increase data quality with the goal of 99% data accuracy.
* Increase the data search at a worldwide level.

INTERPOL encourages RCM Member countries to implement API/PNR/E-VISA technology, which can be adapted to the authorities systems.

Report to INTERPOL immediately when fraud passports are identified.

There are other databases that can be accessed by free, such as EDISON TD and Document Identification System for Civil Services (DISCS).

Project Dial-Doc V2 is almost ready, and is in-progress by INTERPOL.

Apply FIND solutions, with access to national, regional and international databases.

Apply WISDM to synchronize INTERPOL and national databases.

Integrate INTERPOL FIND in national systems of border controls.

Control every passenger systematically.

Malcolm Eales, Director Risk Integration, from the Canadian Passport Program, Immigration, Refugees and Citizenship, highlighted that Canada has been a strong supporter of SLTD and has sent updated records.

A challenge being faced is when countries introduce false hits on INTERPOL system.

Interoperability is key in order to obtain better results on SLTD.

**Session 10: Electronic Passport**

[Michael Holly](http://www.icao.int/Meetings/TRIP-Symposium-2016/Documents/Holly.pdf), Senior Advisor for International Affairs of USA, Department of State, Bureau of Consular Affairs, United States, Passport Services and Chairperson, ICAO New Technologies Working Group.

Issuing e-Passport is not a ICAO standard. Countries are not obligated to issue e-Passport. Countries must issue MRTD.

The advantage of e-Passport is that it can be validated in real time.

Public Key Infrastructure (PKI) allows an Issuing Authority to protect the data on the e-Passport’s chip.

Data sharing must meet appropriate legal standards.

Robust identity management is the key to producing a secure travel document.

**CONCLUSIONS DAY 2**

* Integrity, security features of travel documents, fraud, interconnectivity and E-Passport.

Some points to be taken into account by RCM Member countries are as follows:

* As quality and integrity of travel documents is improved, our objectives must be focused on the weakness of the documents and the supporting systems.
* Keys for trust building: it is very important for States to establish unique identity in its system and the importance of security and integrity of identity systems. RCM Member countries recognized that if there is no biometrical data, the challenge is much higher.
* It is very important for RCM Member countries to implement a system of trust guide of evidence of identity, capacity building.
* RCM Member countries are encouraged to produce travel documents with the combination and integration of first, second and third level features. There should be a focus on things that are easy to verify and hard to reproduce
* Do not rely only on one feature for validation; rely both on technology and human review of passports.
* RCM Member Countries are encouraged to strengthen corrective actions, such as data exchange and the generation of migratory alerts.
* It is important to consider good communication between government agencies.
* If the information is handled electronically, the research results will be more immediate, as well as the ability to respond to requesters.
* RCM Member Countries are encouraged to exchange information and notify third countries for confirmed fraud cases when identified.
* Forensic high tech labs cannot replace passport examination capabilities made by trained officers.
* INTERPOL encourages RCM Member countries to implement:
  + API/PNR/E-VISA technology, which can be adapted to the authorities systems and integrate such technology with INTERPOL FIND for a complete passenger screening.
  + Report to INTERPOL systems (SLTD and/or Dial-Doc) immediately when fraudulent passports are identified (stolen, lost, revoked, stolen blank to SLTD, false to Dial-Doc).
  + Apply WISDM to timely and accurately synchronize INTERPOL SLTD and national databases on stolen/lost documents.
  + Integrate INTERPOL FIND within existing national police/border systems for systematic checks against both national, regional and INTERPOL SLTD database.
* Control every passenger systematically, using systems, as well as the knowledge of trained officers.
* The use of SLTD is encouraged both for its effectiveness as a system, as well as for the deterrence effect that strong systems to track lost and stolen passports has on people considering their use
* There is also a need for public engagement and awareness for citizens to protect their travel documents and to feel responsible for reporting both lost and stolen documents as well as found documents
* E-passports can be a very effective tool and are linked to the future of passports, but their effectiveness is linked to full use of the PKD systems.
* RCM Member countries recognized that robust identity management is the key to producing a secure travel document.