International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/21-WP/11
22/11/12
English Only

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

TWENTY-FIRST MEETING

Montréal, 10 to 12 December 2012

Agenda Item 3: Activities of the ICBWG

GUIDANCE MATERIAL ON REGIONAL VISAS AND ADVANCE ELECTRONIC INFORMATION FOR PASSENGER PRE-CLEARANCE

(Presented by ICBWG)

1. INTRODUCTION

1.1 As demands on Border Control Agencies continue to grow and the resources within which they must operate tighten, a number of valuable opportunities have arisen that allow these Agencies to maintain, and in many cases enhance, their effectiveness – particularly through IT solutions, greater information sharing, and agency cooperation.

1.2 In particular, the use of electronically transferred data such as Advance Passenger Information (API), Passenger Names Records (PNR), and pre-clearance systems such as the United States' Electronic System for Travel Authorisation (ESTA), allows Border authorities to target enforcement resources, thereby improving the facilitation of low risk passengers.

1.3 In terms of greater international cooperation, multilateral agreements at a national level have already led to the development of regional approaches to the administration, management and protection of borders; this is most evident in the Schengen Area established by States of the European Union, but also in such initiatives as the Asia Pacific Economic Cooperation's (APEC) Regional Movement Alert System (RMAS).

1.4 Member States planning to implement robust border solutions that incorporate advanced passenger information are increasingly looking to ICAO for guidance. The guidance presented in this working paper is targeted at ICAO Member States that are considering the use of electronic information for pre-clearance, with an interest in how such systems and tools might fit into a regional approach to border management.

2. BACKGROUND

2.1 In 2010, World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO), released the latest version of the *Guidelines on Advance Passenger Information (API).* The Guidelines present some broad contextual information for States considering using API; however, the primary aim of the document is to ensure Member States use API in a standardized, consistent and interoperable way.

2.2 At TAG 20, a number of States requested that ICAO produce guidance for eBorders and eVisas. Upon discussion with the Chair of the ICBWG, the issue was further refined, and it was agreed that the working group would initiate research on pre-clearance systems, and regional Schengen-type visas.

2.3 This technical report, *Guidance Material on Regional Visas and Advance Electronic Information (AEI) for Passenger Pre-clearance,* seeks to explore the issue in such a way as to complement the technical guidance ICAO, WCO and IATA have already developed. It also draws on lessons learned from States that have implemented Advance Electronic Information systems, and regional approaches to border management.

3. CURRENT STATUS

3.1 The potential scope for guidance in this area is huge and complex, spanning from highly technical aspects of implementation, through to the intricacies of developing border policy and legislation.

3.2 The document is not intended to cover all aspects of the topic in detail – but rather is at a relatively high-level, outlining some of the key concepts, considerations and 'lessons learned' from other States that have implemented, and are using, systems and information for passenger clearance – particularly in a regional or multilateral context. The information is not exhaustive, and seeks where possible to identify other sources of information.

3.3 The document draws from excellent research undertaken by Frontex, as well as information from US Customs, Australian Immigration and New Zealand Immigration. However, access to information on lessons learned, which is the aspect most sought by Member States, is difficult to obtain and not necessarily extensively documented (with the exception of Frontex).

3.4 There is a current lack of border representation on the ICBWG and this will impact the Group's ability to deliver what States require, which is effectively insights into the detail of operations, implementations, and policy legislation for Advance Information and regional approaches to border management. This is particularly apparent when exploring and articulating the significant challenges involved in establishing a border area such as Schengen. The establishment of a Schengen-type visa is therefore still to be completed, as it requires a large amount of specialist input.

3.5 The ICBWG suggests using the current draft as a basis to begin work with a wider group, involving expert agencies such as Frontex, WCO, IATA and other key agencies such as Canada Border Services.

3.6 A working draft of the technical report is at Appendix A.

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to:

a) approve the direction of the work, and its continuation; and

b) approve the formation of a wider sub-group, including agencies with expertise or an interest in border, such as IATA, WCO, CBSA and Frontex.

— END —

APPENDIX A

GUIDANCE MATERIAL ON REGIONAL VISAS AND ADVANCE ELECTRONIC INFORMATION (AEI) FOR PASSENGER PRE-CLEARANCE

TECHNICAL REPORT

Status: Draft Version 0.1
Date: 14 November 2012

INTERNATIONAL CIVIL AVIATION ORGANIZATION

IMPLEMENTATION AND CAPACITY BUILDING
WORKING GROUP (ICBWG)

Contents

Acknowledgements

Where relevant, the document draws on and makes reference to existing documentation produced by ICAO and other international authorities, and specialist border agencies such as United States Customs and Border, Australia's Department of Immigration and Citizenship (DIAC), New Zealand Immigration, and Frontex - the agency responsible for the management of operational cooperation at the external borders of the European Union (EU).

In particular, the recent work of Frontex's Research and Development Unit provides excellent insight into best practice, roll out and use of advance information, and the challenges/areas of improvement – specifically for the EU, but applicable to any border context. Frontex has established a working group to undertake this research, and development of advice is ongoing. Some of the Frontex's work is directly used or summarised.

Other regional groups addressing these AEI issues are in operation (such as the Asia Pacific Economic Cooperation's (APEC) Business Mobility Group), and their work has been utilised in this guidance.

1. Introduction

In recent years there has been a dramatic growth in passenger movements, using various modes of scheduled and chartered transportation, in all regions of the world. As demands on the Border Control Agencies continue to grow and the resources within which they must operate tighten, a number of valuable opportunities have arisen that allow these Agencies to maintain, and in many cases enhance, their effectiveness. These opportunities include:

- advances in Information Technology
- greater co-operation between Border Control Agencies domestically
- greater international co-operation between Customs, and with other border control agencies; and
- greater co-operation between Border Control Agencies and carriers.

Co-operation, particularly in relation to intelligence exchange, is extremely important especially as it is now well recognized that success in border enforcement relies much more on carefully targeted efforts based on high quality intelligence than it does on random or systematic action.

The deployment of computerized passenger screening/clearance systems, incorporating passenger selection criteria developed on the basis of high quality intelligence has been shown to have a positive effect on enforcement activities. Details of arriving passengers can be received in advance of the arrival of the flight - thus allowing the Border Control Agencies adequate time to determine their response, and in some cases even prevent boarding of individuals – effectively pushing their border to the point of departure.

In particular, the use of electronically transferred data such as Advance Passenger Information (API), Passenger Names Records (PNR), and pre-clearance systems such as the United States' Electronic System for Travel Authorisation (ESTA), allows Border authorities to target enforcement resources, thereby improving the facilitation of low risk passengers.

In terms of greater international cooperation, multilateral agreements at a national level have already led to the development of regional approaches to the administration, management and protection of borders; this is most evident in the Schengen Area established by States of the European Union, but also in such initiatives as the Asia Pacific Economic Cooperation's (APEC) Regional Movement Alert System (RMAS).

The collective approach to enforcement of a Schengen-type regional border facilitates movement within the zone, by removing the need to control internal borders. To be effective, a regional approach to border management requires significant collaboration between States, including shared systems, information, and enabling policy and legislation. There are, however, many benefits to States in this model – including leveraging current investment, sharing cost, and standardising approaches.

Member States planning to implement robust border solutions that incorporate advanced passenger information are increasingly looking to ICAO for guidance. In 2010, World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO), released the latest version of the *Guidelines on Advance Passenger Information (API).* The Guidance presents broad contextual information for States considering using API; however, the primary aim of the document is to ensure Member States use API in a standardized, consistent and interoperable way. This technical guidance is contained in Appendix II, as the WCO/IATA Passenger List Message (PAXLST) Implementation Guide.

This technical report, *Guidance Material on Regional Visas and Advance Electronic Information (AEI) for Passenger Pre-clearance,* seeks to explore the broader considerations further, to complement the technical guidance ICAO, WCO and IATA have already developed.

It is targeted at ICAO Member States that are considering the use of electronic information for pre-clearance, with an interest in how such systems and tools might fit into a regional approach to border.

2. Scope of Document

The potential scope for guidance in this area is huge and complex, spanning from highly technical aspects of implementation, through to the intricacies of developing border policy and legislation. The document does not cover all aspects of the topic in detail – but rather is at a relatively high-level, outlining some of the key concepts, considerations and 'lessons learned' from other States that have implemented, and are using, systems and information for passenger clearance – particularly in a regional or multilateral context. The information is not exhaustive, and seeks where possible to identify other sources of information. The document covers two key areas:

1. Using electronically transferred information such as Advance Passenger Information (API) and Passenger Name Record (PNR) for pre-clearance; and

2. Regional Schengen-type visas that permit travel in multiple States.

3. Strategic Considerations (incomplete)

Guidelines on Advance Passenger Information (2010) outlines a number of fundamental strategic considerations for States, including the need for a National passenger processing strategy, and within that a Joint Passenger Processing Strategy Plan that includes all of a States' border agencies. Also noted is that:

a) States should consider adoption of API in the context of a total system approach to border management, encompassing the issuance of machine readable passports and visas including electronic visas, migration to automated entry/exit records to replace embarkation/disembarkation cards, and interoperability among the API systems of other participating States.

b) Future configurations of API-based border control systems should include the deployment of biometric technology to assist with the identification and identity confirmation of passengers upon arrival.

4. Desired Outcomes/Target State (to be completed)

5. Advance Electronic Information (AEI)

Advance Electronic Information (AEI) is a term used throughout the present document to unifying concepts of any electronic information about travellers that is forwarded by carriers to border management authorities for the purposes of law enforcement, before the traveller actually arrives at the physical border. This includes existing systems and data exchanges such as ESTA, API and PNR.

This first section of AEI guidance focusses on API and PNR, given they are the most likely cource of AEI a State is likely to access. Online pre-clearance systems are covered in the following section Online Travel Authorisation. APEC's Regional Movement Alert System (RMAS) is covered later in this section.

Firstly, it is important to make the disctinction between API and PNR, which are two very separate sets of information, with different purposes and sources, coming at different times and often stored in different places:

- API is a single point-in-time validation of an individual's identity and their travel, and is valuable for checking whether the entry conditions for crossing the border are met, but is not necessarily useful for assessing the potential risk that this person presents to the destination country.

- PNR is the complete set of booking data captured by airlines or their representatives (i.e. travel agents, reservation companies). It is not a still picture, but a sequence of discrete actions and events, which may reflect particular behaviours of interest to Border. By analysing this information, national authorities can identify situations and actions that might be indicative of possible criminal intentions.

5.1. What is Advance Passenger Information (API)?

API is a requirement imposed on carriers by state border control authorities to transmit information on passengers they will carry to an authorized border crossing point in that state. An API system can be implemented as a batch model or an online model. An economy's choice of API model will depend on the country's business directions, budget and available resources.

Normally API information is sent in batch mode, i.e. a list of passengers, generally after boarding is completed, to the destination country of the flight, and sometimes even to transit destinations. In the destination country the list is used to check passengers against a number of watch lists before the flight arrives. A batch API cannot be used to prevent a passenger from boarding the aircraft because the system does not return a response to the airline

An 'online model' of API, which happens in real time, is the interactive API, also known as "i-API", "Advance Passenger Processing (APP)", "Board/No Board" "Red Light/Green Light System" and "Authority to Carry". It is a system whereby required data elements on each passenger are collected and transmitted by airlines to border control agencies at the time of checkin. Border alert processing is done for each passenger in real time, and a message is returned notifying whether or not the passenger should be allowed to board.

This API model prevents boarding of passengers, effectively pushing the States' border to the point of departure. The online model of API introduces another layer of complexity to

passenger processing, as real-time decisions regarding the Red light/Green light at checkin are made through automated checks within the desitination's border systems. This also involves resolving exceptions in real-time.

Standard batch-mode API involves the capture of a passenger's biographic data contained in his or her passport combined with some details of the passenger's itinerary, and then collated and transmitted in the form of batch flight manifests to border control agencies in the destination country after aircraft departure. API often falls under the responsibility of the border control authority and immigration control institutions of the destination country.

The exact API information required will vary depending on the country, but it will generally include:

- Full name
- Gender
- Date of Birth
- Nationality
- Passport number and expiry date
- Where passport issues
- Country of residence
- Trip origin
- Route origin or initial embarkation point

The obligation to provide correct passenger information also flows down to the passenger. If a passenger fails to provide the required personal data (e.g. failing to show a valid travel document to the carrier upon check in, or providing incomplete information at self service check in), the carrier may deny boarding. It may also happen that even if the carrier would allow the passenger to travel, he/she would not gain access to the country at the other end.

When a passenger is refused to enter, the carrier is typically required to bear the repatriation costs and to pay a penalty for not abiding to API requirements of the destination country. Also, the passenger failing to provide proper personal data where required will inevitably cause the check in process to be slower at the departing country, and will face additional waiting time at the border check of the destination country.

In all cases, API must always be provided to the authorities of the destination country of the flight with some predefined time before the passenger gets to the border crossing point.

API has the capability of bringing substantial advantages to all involved in the movement of passengers. Among others, the WCO, IATA and ICAO strongly support the use of API and thus have lead several initiatives in the elaboration of standards and implementation guidelines.

The widespread use of API depends to a large degree on a common approach by all concerned (carriers and border control agencies) to the question of data standards. In effect this means that the border control agencies worldwide should standardize their data requirements for API, and should also adopt a standard format for the electronic transmission of such data. The de facto data industry standard is the UN/EDIFACT messaging format, which is also recommended by the WCO, IATA and ICAO.

Although API is typically connected with air transport, it can also be extended to passengers using other transportation modes, particularly cruise liner and railway traffic. It is very seldom used for road traffic (coach liners).

API is mainly used for inbound travellers, it is also technically feasible to use it for outbound travellers. By doing this, border authorities may have a better picture on who has actually left the country, and thus a better estimation on the number of possible over-stayers.

5.2. What is Passenger Name Record (PNR)?

Passenger Name Record (PNR) is the complete set of booking data captured by airlines or their representatives - travel agents, reservation companies, etc -. A PNR contains the travel record of a passenger or a group of passengers travelling together. This typically includes among others:

- Ticket and itinerary data
- Frequent flyer numbers
- Special request information
- Payment information
- Baggage information
- Additional contact information

Border Management Authorities (BMA) that require PNR information use it to perform risk assessments, including link analysis and data matching, to identify high-risk travellers even if these have never committed an unlawful activity before. It is one of the many ways to push the "virtual border" away from the "physical border" in order to have earlier and more reliable information on which to base the risk analysis of inbound travellers.

While API provides biographical information on people known to the BMA (e.g. featuring in watch lists), PNR allows identifying unknown passengers whose behaviour (e.g. routes, payment methods) may indicate a criminal intention, thus allowing the BMA to carry out further checks on them.

What is really important about PNR data (and makes it totally different from API) is that it allows the BMAs to identify high risk travellers who are arriving at the border but who are not on any watch-list. In other words, it enables BMAs to identify people matching a risk profile that they were not aware of in advance, as they are not on the list of known suspects. So while the BMA has not had past knowledge of the existence of these passengers, they are able to identify them upon arrival to the border and focus their attention on them. Conversely, they can move the vast majority of travellers, who present no risk whatsoever, across borders more quickly and comfortably.

5.3. Benefits of API and PNR

API and PNR data provides significant benefits by maximising the security of travel and facilitating faster processing of legitimate travellers, while reducing opportunities for travel by unauthorised or improperly documented persons. AEI provides for:

One of the main benefits of API, and one of the principal reasons for undertaking the advance transmission of passenger data, is the potential benefit to the travelling public. The time saved by the legitimate (non-targeted) passenger while undergoing normal arrival formalities will, of course, vary from airport to airport.

The additional passenger data captured at the time reservation is made or during check-in could, in some instances, enhance carrier security and help to ensure that all passengers carry valid official travel documents required for admission to the destination country. This has the potential of reducing carrier exposure to penalties for transporting passengers that are not properly documented.

- Where States have implemented interactive API programs, and are able to provide "Board / Do Not Board" responses at time of check-in, carriers may be more readily able to avoid costs associated with the detention and/or removal of persons who might otherwise be determined, based on specific factors available to the Border Control Agencies, to be inadmissible upon arrival at the final destination.

- Ultimately API should lead to a stabilisation of airport fees assessed to carriers, since its implementation may enable more efficient utilisation of existing facilities.

Border Control Agencies:

- One of the major benefits of API and PNR for the Border Control Agencies is the enhanced enforcement capability realised through advance notification of the arrival of potential offenders. API combined with PNR permits a thorough and rigorous screening of inbound passengers to be accomplished, targeting those passengers that present the highest risk, and allowing for the faster throughput of low risk passengers.

- Since passenger data will be provided in an electronic, readily processed format, there should be a data capture saving, as the Customs/Immigration official will not be required to perform a normal data entry operation when the passenger arrives at the entry point.

- API and PNR provides for more effective allocation of border control and law enforcement resources. In addition, the increased automation of passenger processing can result in reduced staff costs.

- API has the potential to be a catalyst for greater interagency co-operation at both the national and international level.

Airport Authorities:

- API also assists the growth in passenger traffic being accommodated through improved use of technology rather than additional infrastructure.

- Consequently, there should be a reduced need to expand or upgrade current facilities in response to increased traffic, provided data capture can, for the most part, be accomplished through automated means

- Greater passenger satisfaction with facilities, fewer complaints, etc.

- Better public image nationally/internationally, good for tourism etc.

5.4. Key Considerations and Lessons Learned (API and PNR)

Decision Making Process

Outlined in Frontex's *Best Practice on Advance Information in the EU,* key learnings when deciding on adopting API and PNR were:

- According to the experience of most Member States (MS) the first best practice is to start early
- Setting an AEI implementation up and running is not capital intensive and does not

pose technology risks; furthermore, AEI systems are very scalable and can benefit from incremental contributions as needed. Consequently there are no entry barriers (other than lack of favourable regulation) that could justify a delay in beginning an AEI implementation

- Assessing and forecasting activities and specific risks at border control points, using official facts and figures, and historical tendencies, is crucial
- Research other implementations: contact, consult and work with experts from Member States, as little information is available in the public domain. Frontex can provide general advice, contacts, literature and guidance about applicable or similar implementations
- It is important not only to identify the relevant regulation articles and provisions, but also how these are likely to be applied in practice. There are weakly defined or ambiguous regulations that have led to underperforming AEI implementations
- Legal expert judgement should be obtained on what legal risks are, and how the current regulation might be applied to the disputes likely to be originated by the introduction of the AEI system.

Involving Stakeholders

Identifying stakeholders for an AEI implementation should be quite straightforward; the natural stakeholders are the border management authority and the carriers are obliged to provide data, although in some cases engaging other additional stakeholders might be relevant and beneficial as well.

- From the carrier side, preference should be given in incorporating to the project representatives from the carriers holding the largest share where the AEI is to be deployed.
- It may be the case that regulatory decision makers should also be involved if there are perspectives of having regulatory changes ahead that could have a significant impact on the AI implementation.
- Also, legal services, technical prescriptors and finance may be considered as appropriate.

Once stakeholders have been identified, the roles and responsibilities of each one of them should be made clear. These should observe not only the decision making process but the complete lifecycle of the implementation.

- Ensure you assess the specific costs, benefits and implications that the implementation of the AEI project will have on each stakeholder, and anticipate conflicts that will arise
- If conflicts are dealt with at a later stage, there is the risk that concessions have to be made at a point where introducing changes is far more costly and risky.

Defining the Right System

To define the system that best fulfils the present and future needs of end users in the most effective manner, while meeting financial and regulatory constraints, the State should:

- As early as possible, achieve a common understanding of the outcomes and key priorities for the system
- Design the system from an end-user perspective, looking also for long term implications.

Cost and Funding

Guidelines on Advance Passenger Information (2010) outlines a number of areas where costs may be incurred. For Border these include:

- establishing offender/suspect database such a system (ideally a single inter-agency database for passenger clearance)
- costs incurred on the system development side associated with the electronic receipt

of passenger data, and additional outputs associated with the processing of API passengers (lists of passengers for closer investigation, statistical reports, and performance evaluations)
- data transmission costs payable by the Border Control Agencies (e.g. connecting their system to one or more selected data networks to enable them to receive passenger data electronically)
- in some instances, the Border Control Agencies, provision of Machine Readable Passport readers to the carriers in the airport of departure; and
- costs will be incurred in respect of on-going maintenance and upgrading.

The principal costs for carriers are:
- system development/integration and capture of passenger details for transmission to the origin and/or destination country of a flight
- additional check-in staff to cope with the extended period of time required to complete check-in formalities, additional check-in desks, hardware acquisition
- adaptation of carriers automated reservation systems and/or departure control systems (DCS) to collect, convert, and transmit API data, and to respond to expanding data requirements will also give rise to significant cost
- on-going maintenance costs will also likely be incurred in respect of the above-mentioned systems; and
- recurring cost of data transmission in respect of the passenger data for each API flight.

Lack of funds can impose practical limitations onto system implementation. Not having access to enough funding will certainly condition the kind of system that can be practically sourced, and hence what fraction of the final user needs can actually be fulfilled.

The available budget for the development, deployment and operation of the system should be assessed and preferably secured before committing on a design solution. A reasonable estimation of the lifecycle costs (capital and operational costs) of the system should be carried out in parallel with the design phase of the project, so that the proposed alternatives are feasible budget-wise.

In order to assess "how much of a system" can reasonably be obtained for the available budget, the best way to proceed is to benchmark against implementations already in place. For this purpose, States should contact agencies such as Frontex, in order to identify the implementations that were intended to satisfy a similar set of needs.

Communicating System Decision to Stakeholders (to be completed)

Planning for Implementation (incomplete)

There may be a board of airline representatives where States can negotiate a standard Memorandum of Understanding (MOU) or agreement with a core group of airlines.

Develop a change program with airlines - when developing the program, an MOU should be attached ato the process early as possible.

Roll out to airlines slowly, implementing with one airline on a single route. Once this has been successful, move go to multiple routes with that airline. Then begin to incorporate more airlines, using the same approach.

Operational Considerations (incomplete)

Reporting well on where things not working (e.g. airlines not doing checks)
Give airlines report each month

Legislative basis for PNR

Penalties for Carriers (incomplete)

Legislative regime –considering whether a fines regime is required up front, immediately

Processing Data and Profiling (to be completed)

Data Quality Control (to be completed)

Data Privacy Law

Data privacy and data protection legislation have been enacted in many countries in recent years in order to protect the individual's right to privacy and to allow individuals to have access to their own personal data held in computer systems and databases in order to verify its accuracy.

This legislation can vary from country to country. However, there is a large degree of commonality of provisions of such legislation. Data privacy and data protection legislation typically requires that personal data undergoing automated (computer) processing:

- Should be obtained and processed fairly and lawfully;
- should be stored for legitimate purposes and not used in any way incompatible with those purposes;
- should be adequate, relevant and not excessive in relation to the purposes for which they are stored;
- should be accurate and, where necessary, kept up to date;
- should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored.

Such legislation also usually incorporates provisions concerning the right of access by data subjects to their own personal data. There may also be provisions regarding disclosure of personal data to other parties, and about transmission of such data across national borders and beyond the jurisdiction of the country in which it was collected.

It is clear from the above that the existence of such legislation may well have an impact on a carrier's ability to capture personal details of passengers and to transmit this data to a foreign government. However, it is also clear that the nature of API data (basic personal information that appears in an official document) and the use to which it is put, should conform to the national law of most countries.

The long-term archiving of passenger manifests on computer media and the use of such data for purposes other than national security or passenger clearance may pose problems in certain countries.

Authorising Legislation (to be completed)

Systems Infrastructure for Red Light/Green Light or 'Online' API (to be completed)

5.5. Regional Movement Alerts System (RMAS)

The Regional Movement Alert System (RMAS) is an APEC counter-terrorism initiative that enhances regional border security standards for air travel through the close cooperation and collaboration of participating governments. It is currently used by Australia, United States and New Zealand, though other APEC States are currently exploring the use of RMAS.

RMAS enables participating economies to automatically detect the attempted use of lost, stolen and invalid travel documents and to assess whether a document is recognised as validly issued by its document issuing authority by directly verifying each other's passport data. The system's ability to facilitate this type of access is one of the key features distinguishing RMAS from other systems compiling lost and stolen passport data.

This is different from online Advance Passenger Information (Red Light/Green Light), where the States' system validates its own travel document, visa and watchlist information.

Benefits of RMAS

There are currently more than three million lost or stolen passports recorded within the APEC region alone. This presents a significant opportunity for persons of concern to move across borders undetected. RMAS makes this much harder by identifying passengers, at airport check-in, if they attempt to use lost or stolen passports from participating economies.

RMAS strengthens each economy's ability to detect and/or prevent the air travel of people of concern, including criminals and terrorists, and helps ensure that people are travelling using valid documents. RMAS further contributes to international security by enabling authorities to identify and remove counterfeit documents from circulation.

Benefits of RMAS include:

- Verification of accurate and up-to-date lost, stolen and invalid passport data - this is a valuable tool for governments in combating terrorism, illegal immigration and trans-national crime;
- Enhanced Security – the ability to conduct these checks will enhance security as well as facilitating genuine travellers and preventing unwanted persons from crossing national borders; and
- Increased focus on counter-terrorism - initiatives such as RMAS demonstrate the commitment of APEC economies to counter-terrorism efforts, and in particular, to regional counter-terrorism initiatives
- RMAS operates seamlessly with existing border systems and provides another layer of security to all participating economies.

Key considerations and learnings for RMAS-type systems

Trusted Broker

A key component of RMAS is the RMAS Broker. It acts like a switchboard for participating economies, routing queries and answers to and from border systems and the passport

databases of each economy. No data is stored in the RMAS Broker. The advantages of not storing data in a centralised repository are that:

- data is validated at the source and not exchanged, which ensures that the most up-to-date data is accessed; and
- each economy controls how much it will tell another economy.

Because of the sensitivity of the passport databases that require interrogation and the possible tensions between the countries participating in regional passenger pre-clearance systems, some countries may not wish others to have direct access to their passport database (particularly when positive validation is involved).

In these circumstances the parties may wish to appoint a third party to operate the passport database interrogation software (the 'Trusted Broker'). The 'Trusted Broker receives the enquiry from the Departure Control System (DCS) make the enquiry on the target Passport Database and returns to the enquirer an agreed message on the basis of what is found i.e. 'OK to Board' or 'Refer to Immigration.'

Positive or Negative Validation

Positive versus negative validation systems is a key consideration for system development. RMAS currently operates on a negative validation model which checks if a passport is not included on the lost and stolen passport database. Positive validation enhancements to RMAS will enable passport details to be validated against a full passport database, confi rming that the passport is recognised by the Document Issuing Authority and is not lost, stolen or otherwise invalid.

Under negative validation, RMAS is unable to detect counterfeit documents; provided the document is not on the lost and stolen passport database, RMAS does not return a match. Positive validation will help participating economies to detect, and take out of circulation, counterfeit passports being used to travel between participating economies. The system's ability to facilitate this type of access is one of the key features distinguishing RMAS from other systems compiling lost and stolen passport data.

The Positive validation is considered highly preferable as it indicates that there is a valid travel document on issue to the holder named in he presented passport. Highly competent forgeries would not be caught by negative validation as they would not be recorded in a database of lost and stolen travel documents.

Not all travel document issuing authorities are able to provide a single physical or logical database of their validly issued travel documents (a prerequisite for positive validation) but do have a single database of all their documents that have been reported lost or stolen.

24/7 Availability

A vital part of RMAS is the relationship between the 24/7 operational centres for clarifying details and ensuring genuine travellers are not inconvenienced when a participating economy receives a RMAS notification.

RMAS requires a 24/7 availability of the database of either non-valid or valid travel documents (depending on choice of system Positive or Negative validation). The database requires constant updating so that recently issued documents that are used immediately for travel can be checked.

Failure to have a sufficiently available database would lead to unacceptable disruption/delays to airport checkin procedures and resistance from airlines to use the system.

For persons travelling on passports that require a visa or permit to enter their destination access to a database containing details of current visas or permits has to be available on the same basis as the passports/travel documents mentioned above.

While the system will, on the basis of what it finds, not authorise an intending passenger to board the aircraft it is only after consultation with the destination country's Immigration Authority that a final decision as to travel will be made (this may involve overriding the automated RMAS response). Experience has shown that inevitably people will present passports that they have previously reported as lost or stolen. In this case it is the immigration authority of the destination country that has to decide whether the holder should be allowed to travel to that country or be refused entry.

The best way of ensuring that when support centres communicate with each other on matters arising from the operation of RMAS is to ensure that there are common procedures and terminology.

Governance Mechanisms

RMAS systems will need a governance mechanism in place, including a Board, signed agreements between parties, and clear procedures relate to the system.

All full participating members plus representative of the 'trusted broker' (as observer) are on the Board and the chairmanship rotates between members.

As well as the initial development systems updates and enhancements and usage need to be funded. How, and if new members' are to contribute to initial capital costs needs to be decided, and the administrative difficulties of trying to repay the initial investors from new member's contributions should not be minimised.

General agreement on the guiding principles of the system would be in a document that states:

- Purpose of the document
- Scope of the system; preserving the right of a country to determine who shall enter its borders; ownership of the data; system not to be used to monitor other nationals without their country's permission; privacy laws to be satisfied; system to be seamlessly integrated with the departure control systems of airlines to members and interoperable with existing border arrangements; monitoring travel on a real-time basis is the ultimate objective.

Dispute resolution is by negotiation between the parties. In the event that a resolution cannot be achieved by the parties then the Board becomes the decider.

Data Exchange

Data Exchange Agreements (or MoUs) are recommended to be standardised bilateral, though can be between a member and all the parties (a series of bilateral agreements, which can be more difficult to agree). Agreements cover what is disclosed, when and for what purpose/what data and why it may be retained.

A difficult question is when does data become the 'property' of the destination country and subject to its laws as opposed to the property of the document issuing country. The idea generally adopted between States and destination countries is that when a person has travelled to the destination country the passport information relating to that person belongs to the destination country. If a person is refused entry the information is not considered to have been transferred.

5.6. Resources

- APEC Guide to the Regional Movement Alert System
  - http://www.businessmobility.org/RMAL/RMAS%20Guide%202007.pdf

- Australia Department of Immigration and Citizenship (DIAC)
  - Information on Australia's APP, including guidance for airlines http://www.immi.gov.au/managing-australias-borders/border-security/air/airlines/app-checkin.htm

- Frontex
  - Information from recent Frontex studies is summarised throughout this document, though the Frontex work is not open source at this time. States can apporach the Frontex Research and Development unit for additional information on the following EU documents:
    - Roll out and Use of Advance Information in the EU
    - Advance Information Best Practice Guidelines
    - Challenges and Areas of Improvement
  - See also *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems* and *Best Practice Technical Guidelines for Automated Border Control (ABC) Systems* http://www.frontex.europa.eu/publications

- New Zealand Immigration
  - Information for Airlines (including Advanced Passenger Processing (APP) guidelines) and Carrier Infringement Regime brochures http://www.immigration.govt.nz/community/stream/facilitate/airlines/

- United States of America
  - Guidance on the Advanced Passenger Information System (APIS), including additional guidance on the US application of the UN/EDIFACT PAXLST, as combined with the format and syntax rules of their own message set requirements. See UN/EDIFACT Implementation Guide http://www.cbp.gov/xp/cgov/travel/inspections_carriers_facilities/apis/

6. Online Travel Authorisation

6.1. United States' Electronic System for Travel Authorization (ESTA)

Electronic System for Travel Authorization (ESTA) is an automated system used to determine the eligibility of visitors to travel to the United States under the Visa Waiver Program (VWP) and whether such travel poses any law enforcement or security risk.

ESTA approval authorizes a traveller to board a carrier for travel to the United States under the VWP. Private carriers must be a signatory visa waiver program carrier. See list of Signatory Carriers. While it is recommended that travellers apply at least 72 hours before travel, they may apply anytime prior to boarding. In most cases, a response is received within seconds of submitting an application.

ESTA is not a visa. It does not meet the legal requirements to serve in lieu of a U.S. visa when a visa is required. Travelers that possess a valid U.S. visa may travel to the United States on that visa for the purpose it was issued. Travelers traveling on valid visas are not required to apply for an ESTA. In the same way that a valid visa does not guarantee admission to the United States, an approved ESTA is not a guarantee of admission to the United States.

Approved ESTA applications are valid for a period of two years, or until the passport expires, whichever comes first, and multiple trips to the United States without the traveler having to re-apply for another ESTA. The ESTA travel information may be updated before each trip to the U.S., but it is not required. When traveling to the U.S. with the approved ESTA, people may only stay for up to 90 days at a time.

Travelers whose ESTA applications are approved, but whose passports will expire in less than two years, will receive an ESTA valid until the passport's expiration date.
A new ESTA authorization is required if the traveller:

- is issued a new passport,
- changes their name (first and/or last)
- changes gender
- changes country of citizenship
- has a significant change of circumstances related to eligibility, e.g. convicted of a crime of moral turpitude or they develop a contagious disease.

Beginning September 8, 2010, there is a fee required by the Travel Promotion Act of 2009 (Section 9 of the United States Capitol Police Administrative Technical Corrections Act of 2009, Pub. L. No. 111-145). The fee is comprised of two parts:

- **Processing Charge** -- All applicants requesting an electronic travel authorization are charged for the processing of the application. The fee is $4.00.
- **Authorization charge** -- If your application is approved and you receive authorization to travel to the United States under the Visa Waiver Program, an additional $10.00 will be charged to your credit card. If your electronic travel authorization is denied, you are only charged for the processing of your application.

6.2. Australia's Electronic Travel Authority (ETA) System

An Electronic Travel Authority (ETA) provides authorisation to travel to and enter Australia and is electronically linked to your passport. It is only available to nationals of certain States.

It is for short term stays for either tourism or business purposes, and can be applied for online if the applicant meet the criteria.

See https://www.eta.immi.gov.au/ETA/etas.jsp

6.3. Benefits of Online Travel Authorisation Systems

To be completed

6.4. Key considerations and lessons learned

See the US Government Accountability Office's report on ESTA
http://www.gao.gov/products/GAO-11-335

To be completed

7. Regional Visas

7.1. Case Study - Schengen

7.2. Background

7.3. Key considerations and requirements (operational, policy, legislation, technical)

7.4. Resources