Facilitation of Aviation Security:
Feasibility Study of
"Registered Passenger" Concept

accenture

High performance. Delivered.

FINAL REPORT

TREN/J2/114-2006

November 2007

European Commission Directorate-General
Energy & Transport

accenture

Daon IRISH AVIATION AUTHORITY

Table of Contents

Executive Summary

Context

According to the International Air Transport Association (IATA), international passenger demand in the first half of 2007 has increased 6.3% year on year and airports are seeing more passenger traffic and more aircraft. Indeed, according to Giovanni Bisignani, IATA's Director General and CEO, "*Passenger demand continues to exceed expectations*".

This growth is taking place in the shadow of an ongoing terrorist threat that has led to changes in the security checks that passengers face before embarking on their journey - such as the introduction of airport security restrictions on liquids and gels in the summer of 2006. These restrictions were in addition to the existing Regulation 2320/2002, which mandates a baseline level of security for all passengers.

Against this backdrop of increased terrorist threats, new security regulations, increased volume of travel and finite resources, the aviation industry is seeking new ways to help maintain and enhance the attractiveness of air travel. Around the world, many Registered Passenger (RP) or Registered Traveler schemes have been trialled or are already operational. These schemes are designed to reduce delays and make travel more convenient, whilst maintaining or increasing levels of security. Most of these schemes focus on border control functions.

This Study reviews the feasibility of an RP scheme with a specific aviation security focus.

Purpose

This Study addresses the essential question of feasibility – that is, whether criteria could be found for identifying groups of passengers that present low risk to aviation security and whether such passengers could be exempted from certain controls without compromising security. It considers the following issues: recognition of a passenger registered in one Member State by another Member State; the legal implications of simplifying security controls; data storage and access, and the process of identifying Registered Passengers at airports. Finally, the Study looks at the potential benefits of such schemes for passengers, airlines, airports and Control Authorities.

A Definition of a Registered Passenger Scheme

The Terms of Reference for this Study define a Registered Passenger scheme as one '*where interested passengers would apply to a national authority, be subjected to a risk assessment and, if that were successful, be registered as someone presenting a low risk to aviation security. When departing from an airport in the European Community, RPs would be exempted from certain security checks after identification.*'

In certain places, an alternative definition of an RP scheme is introduced in this report – one that does not exempt or minimise the security checks to which RPs would be subject. Instead, this approach offers RPs an improved passenger experience through privileges such as fast tracking through accelerated security checks coupled with better customer service. The report explicitly specifies when this definition is being used.

Methodology

To compile and develop this report, the Study Team conducted desk research, attended various forums and consulted with over 30 government agencies and industry organisations.[1]

Key Findings

Aviation security requires that both the passengers and the objects they may be carrying have to be assessed. The information submitted by a passenger for enrollment into an RP scheme may enable a 'not high-risk' judgement and provide reassurance from an identity perspective (i.e. that the person concerned does not match a certain profile, is not wanted for terrorism, or is not on a watch list). However, precise criteria to assess passengers as 'lower than average risk' are hard to define because of a lack of clear criteria. The fact that passengers are not classified as 'high-risk' does not automatically mean that they qualify as 'lower than average' risk.

In addition, completion of passenger security clearance checks does not mitigate the risk related to the objects that a passenger may be carrying. The following possible scenarios must also be kept in mind:

- Absence from a watch list or database is not a definitive measure of lower risk. It might be that a person is not yet on the list, that the list is inaccurate, or that a different identity has been used for enrollment into the RP scheme

- A passenger could be a sleeper terrorist or so-called 'clean skin' who may have a perfect background profile yet have the intention of conducting terror-related activities

- Innocent travelers can be coerced or duped into carrying objects

The focus for RP schemes should be the streamlining of the security process, using people, technology and process improvements to help enhance the passenger experience. The availability of more information about RPs, and an increase in the use of new or better technology for security checks can bring considerable benefits for passengers, airports, airlines and governments, including an enhanced customer experience, new opportunities for revenue generation and the facilitation of more convenient air travel for all passengers.

---

[1] See Appendix A for a full list of Stakeholders that were consulted in this Study

Summary of Questions and Answers

The twelve questions posed by the EC Directorate-General Energy and Transport (EC DG TREN) are detailed below and form the basis of this study. They are outlined in this section along with the headline conclusions from the report.

(Question 1 of 12) On what grounds could a set of passengers be reliably assessed as presenting lower risks than others? The contractor should suggest precise criteria for identifying passengers presenting low risks to aviation security (care should be taken to avoid discrimination by sex, race or ethnic origin, religion or belief, disability, age or sexual orientation).

Security measures are currently geared around the identification of high-risk passengers. A combination of criteria and methods such as checking against watch lists and databases, scrutiny of immigration status, and profiling can be effective in identifying passengers who pose a significant threat to security. When the same security principles are applied to identifying a 'lower risk' passenger the chances of error are much higher and the potential consequences are severe.

The conclusion of this section is that a passenger who is not considered to be 'high risk' cannot be regarded as posing so little threat to security as to gain access to a lighter security check process. As a number of Control Authorities consulted during this report made clear, the lack of a clear terrorist profile and the adaptable nature of the modern terrorist means it is difficult to foresee when RP schemes could offer security related privileges without putting passenger safety at risk.

(Question 2 of 12) What would be the most promising approach to facilitating the recognition of a passenger registered in one Member State by others that operated "RP" schemes: harmonisation of criteria, mutual recognition (whether or not within a European Community framework) or something else?

There are three key stages to an RP scheme that need to be considered when assessing the most promising approach to international recognition:

- Enrollment

- Risk assessment

- Identification at the airport

Mutual recognition can be achieved for enrollment and identification at the airport. Whilst in-depth checks would not be suitable due to the number of schemes involved, acceptance of other schemes processes based on common standards could enable mutual recognition.

For risk assessment, the feedback from Control Authorities is that mutual recognition would not be acceptable, and each country is likely to conduct their own assessment.

(Question 3 of 12) What are the arguments for and against:

- **Limiting a "Registered Passenger" scheme to nationals of Member States;**

- **Or extending them to nationals of third countries legally resident in a Member State?**

Arguments against the extension of membership are based on the difficulties encountered in sharing data and gaining access to the requisite information from third countries, and even when this is possible, the time and costs incurred in doing this.

Arguments in favour of extending membership to third country nationals include increasing the size of the potential customer base, the avoidance of negative publicity and meeting the legal and political aims of extending EC travel rights to third country nationals.

(Question 4 of 12) From which security checks could "Registered Passengers" be exempted without compromising security? What is the scope for lightening or accelerating certain checks without going as far as exemption?

The research and interviews conducted during this review show that it is not possible to exempt RPs from any security checks, or indeed lighten any of them, without compromising security.

The possibility of reducing random checks for RPs was examined, and this met with mixed reaction from stakeholders. Most Control Authorities were against such an idea although some were in favour. Airlines and airports would like to see a reduction in random checks for RPs. However, the inability to accurately define a lower risk passenger makes this option questionable and the creation of a lower security level has several impacts. The most serious of these is the creation of a weak link in the aviation security chain, which could have severe consequences.

One area where there is more scope for feasible change without compromising security is in accelerating checks. This acceleration is most likely to be realised through a combination of improved technology and processes and the increased capacity of security screening areas and personnel.

The potential impact of such developments will depend on the airport in question. One issue raised with stakeholders on such improvements related to how they would be funded. There are several business models that can be considered. The most feasible of these entails the RPs paying membership fees.

Central to a number of business propositions around RP schemes is the eventual benefit all passengers will gain from the advances and improvements that they expedite. This is difficult to assess in existing RP schemes given the commercially sensitive nature of the relationships between suppliers, airports, airlines and Control Authorities.

(Question 5 of 12) Would either existing or proposed Community legislation on aviation security allow such changes in procedures? What changes in Community law might be required to permit them?

At the time of writing, the existing and proposed legislation does not contain special procedures for the benefit of RPs. They are thus subject to the same security measures as all other passengers. If required, procedures for the benefit of RPs might be achieved by amending the regulations.

Since the proposal for a regulation which is designed to repeal Regulation 2320/2002 is at an advanced stage of adoption, the position of RPs would need to be considered under the implementing measures provided for the text of the Proposed Regulation (repealing Regulation 2320/2002) as agreed upon between the Community institutions. Special

procedures for the benefit of RPs would be difficult to construe under the current text of the Proposed Regulation.

(Question 6 of 12) Would the revised version of Appendix 17 to the Chicago Convention allow such changes to procedures?

The ICAO measures – apart from those pertaining to disruptive passengers and passengers who have been subject to legal proceedings – apply without exception to RP schemes. As such there are no exemption procedures for RPs under Appendix 17 of the Chicago Convention.

(Question 7 of 12) What would be the impact on operations at airports of a two-tier system of passenger screening?

Options for the implementation of a two-tier system of passenger screening include:

- A dedicated channel for RP at both authentication and screening

- A dedicated channel for RP authentication with passengers then entering the normal security screening area

- A shared staff search/RP channel with re-use of existing equipment and resources

The impacts of such implementations include:

- Accelerated processing for normal passengers as well as RPs

- Possible loss of retail space and associated revenues in some airports

- Additional capital expenditure to set up the additional facilities

- Potential confusion and conflict between normal passengers and RP's if shared security screening lanes are used

- Additional training for staff to manage both types of passengers and the associated process differences

The extent of these impacts will vary according to the airport and the type of RP implementation used.

(Question 8 of 12) How best should data on "Registered Passengers" be stored so that national authorities could access it when controlling departing passengers at airports? How could authorities of one Member State be given rapid and easy access to lists of passengers registered by other Member States, when it recognised their registration? The contractor should analyse whether other data bases (existing or planned) would serve this purpose.

Three approaches to the storage and access to RP data were considered:

- Centralised

- Federated

- Distributed

These approaches were analysed under several headings:

- Responsiveness

- Trust

- Legal Requirements

- Rapid & Easy Access

The conclusion is that a Distributed approach best satisfies the requirements through the utilisation of RP tokens or the use of ePassports.

(Question 9 of 12) As for the identification of "Registered Passengers" when presenting themselves at airports, what system(s) for identifying travelers for border control purposes (existing or planned) might serve this purpose?

When RPs present themselves at airports, accurate and fast identification and authentication of the RP is essential to the success of the scheme.

The use of a multi-modal biometrics system (i.e. with the capability to operate on several different biometric types) along with an identity token is strongly recommended as the means to achieve this. This will reduce human error and increase the integrity and credibility of the scheme.

There are many practical considerations to consider when using biometrics, but advances in technology, use of the multi-modal approach and the increased use of biometrics by the public in other aspects of their lives is helping to overcome the issues that may have been faced in the past.

(Question 10 of 12) To what extent would the introduction of a 'Registered Passenger' scheme at Community level facilitate air transport? In particular, what reductions in delays might typically be expected, and at which types of airports and at what periods of time?

An RP scheme could be one of the ways to improve the passenger experience in the face of challenges from increased security levels, growing demand and limited resources. The potential exists for RP schemes to facilitate air transport by creating a more convenient and faster experience at the security checkpoint. Other industries and organisations are continually looking to improve the customer experience through advances in technology and process; the RP scheme could be a vehicle for such changes in the aviation industry.

RP schemes could facilitate air transport for all passengers, not just RPs – particularly if the infrastructure (including staff, lanes and equipment) is in addition to that provided for normal passengers. As to the type of airport to which the RP scheme is best suited, the consultation with stakeholders suggests that large hub airports with high volumes of passengers and possibly some regional airports with a high percentage of frequent fliers are the most likely candidates.

The key time of day when air transport could be facilitated most effectively by an RP system would be during the peak hours for business and holiday flights – this is typically when most congestion occurs.

The reduction in delays is difficult to estimate as it will vary from airport to airport depending on a number of factors including; type of scheme, quality of implementation, and the scope for improvement.

(Question 11 of 12) To what extent would the introduction of a "Registered Passenger scheme" at Community level benefit the operations of air carriers and airports and what might be the impact on their costs?

Benefits to airports include:

- Passenger satisfaction and retention

- Revenue generation

- Revenue protection

- Positive PR

- Other Benefits including frequent flier programme tie-in

Benefits to carriers include

- Better service

- Unique selling point

- Cost reduction

- Positive PR

However, it should be noted that RP schemes will not be applicable to every passenger, air carrier, airport or Control Authority. Amongst some of the Control Authorities and airports interviewed there was a lack of appetite for change and innovation, and a lack of demand to alter security screening processes. Equally, the US RT programme has experienced a mixed reaction in the US, from organisations and passengers alike.

The costs associated with an RP scheme for air carriers, airports and Control Authorities vary according to the business model used. There is a range of cost centres that need to be considered in the development of such a model that include home country costs and international costs.

(Question 12 of 12) How far might common approaches lessen the costs of identifying passengers and maintaining their databases?

Common approaches can lessen the costs of RP schemes through the adoption of:

- Common standards

- Common scheme elements such as:

  - o Standard tokens

  - o Common biometric templates and matching algorithms

- o Shared data storage

- o Common IT architecture and infrastructure

- Standard business processes including shared services

- Leverage of existing EC systems

Conclusion

This study concludes that an RP scheme, as defined in the Terms of Reference, where RPs experience exemptions from, or lightening of security checks, is not possible without compromising passenger safety. The rationale behind this conclusion is based on the difficulty of developing a "lower risk" passenger profile and the compelling arguments for not giving any specific group a lower level security status (i.e. the creation of a weak link in the security process that could be exploited).

There are however, other types of RP schemes that do not offer exemptions from, or lightening of, security checks for their members, but which offer benefits to a range of stakeholders including passengers, airlines, airports and Control Authorities. As shown by Registered Traveler and Passenger programmes around the world, a scheme can be envisaged that enhances the customer experience and accelerates passengers through the same or increased levels of security.

This is feasible through a combination of technology, process and people-related advances accessed by RPs who are assessed as 'not high risk'. Such schemes will not be suitable for all airports and the scale of their impact and cost will be dependent on a number of factors, not least the type of airport and the business model upon which the scheme is based.

Section A – Context, Methodology and Definition

Context

Set against the backdrop of increased terrorist threats, new security regulations, an increased volume of travel and finite resources, the aviation industry is continually looking for new ways to help maintain and enhance the attractiveness of air travel. Around the world there are many Registered Traveler schemes that have been trialled or that are already operational, designed to reduce delays and make travel more convenient whilst at the same time maintaining or increasing levels of security at the border. Most of these schemes are focused on immigration. However, the purpose of this Study is to review the feasibility of an RP scheme with an aviation security focus.

The European Commission Directorate-General Energy and Transport (EC DG TREN) commissioned a Study on the feasibility of RP schemes in the European Union focused on Aviation Security. Such schemes would provide for passengers identified as presenting low security risks to undergo simplified screening, without compromising security. This would ease the flow of passengers through airports and reduce the operational and financial burden of security measures on airports and airlines.

The Study addresses the essential questions of feasibility – that is, whether criteria could be found for identifying groups of passengers that present low risks to aviation security and whether these passengers could be exempted from certain controls without compromising security. It considers the recognition of a passenger registered in one Member State by another Member State, the legal implications of simplifying security controls, the storage of data on RPs, and the process of identifying them at airports. Finally, the Study looks at the potential benefits of such schemes for passengers, airlines and airports.

Definition of a Registered Passenger scheme

The Terms of Reference for this Study define an RP scheme as one 'where interested passengers would apply to a national authority, be subjected to a risk assessment and, if that were successful, be registered as someone presenting a low risk to aviation security. When departing from an airport in the European Community, RPs would be exempted from certain security checks after identification.'

In certain places, an alternative definition of an RP scheme is introduced in this report – one that does not provide exemptions from or lightening of security checks to RPs. Instead this type of RP scheme offers RPs a better passenger experience through privileges such as fast tracking through accelerated security checks and better customer service. The report explicitly specifies when this definition is being used.

Scope

For the purposes of this Study, aviation security is defined as the prevention of both the entry of unauthorised persons (i.e. 'access control[2]') and the introduction of potential weapons or other prohibited articles (i.e. screening and protection of what has been screened) into the security restricted areas of airports and into aircraft. This does not include other security measures at the airport such as security at the perimeter and other parts of the airport including check-in and parking.

---

[2] Access Control is currently focused on the passenger having the 'right to fly' i.e. they have a valid and unique boarding pass.

The scope of this Study is aviation security and specifically an RP scheme that is very different to the existing schemes in place at the moment around the world. The scope is:

• To review the feasibility of setting criteria for a 'lower risk' passenger as an RP

• To review the feasibility of reducing or exempting security checks for the RP

Different Schemes, Different Purposes

RP schemes around the world are driven by a variety of purposes and have varying scopes. Examples include:

• *Security* – The US Registered Traveler Programme[3] conducts a risk assessment to remove the 'high-risk' passenger through security checks and other means. This programme does not reduce security levels (see the response to Question 11 for more detail on the US scheme)

• *Immigration* – The UK IRIS Scheme[4] revolves around the ability to confirm the immigration status of the passenger as well as checking watch lists to confirm that the passenger is not a national security risk

• *Customer service* – the Privium[5] scheme operating in Schiphol airport helps the passenger journey through border control checks and does not focus on the security screening area. Following security checks, the passenger is offered a wide range of services such as expedited check-in and reserved parking

• *The full passenger international journey*– the miSense[6] Trial, which operated at London Heathrow airport, was designed to test the IATA Ideal Process Flow. This trial did not focus on aviation security apart from facilitating entry into the Secure Restricted Area

Purpose of this Document

The Report answers the 12 questions set out by the EC DG TREN in the original ITT Document:

Risk Assessment (Questions 1 to 3)

(Question 1) On what grounds could a set of passengers be reliably assessed as presenting lower risks than others? The contractor should suggest precise criteria for identifying passengers presenting low risks to aviation security (care should be taken to avoid discrimination by sex, race or ethnic origin, religion or belief, disability, age or sexual orientation).

---

[3] http://www.tsa.gov/what_we_do/layers/rt/rt-faqs.shtm

[4] http://www.ind.homeoffice.gov.uk/applying/iris/applying

[5] http://www.schiphol.com/privium/privium.jsp?ASSORTMENT%3c%3east_id=1408474395729234&FOLDER%3c%3efolder_id=2534374302572265&bmLocale=en

[6] www.miSense.org

(Question 2) What would be the most promising approach to facilitating the recognition of a passenger registered in one Member State by others that operated "Registered Passenger" schemes: harmonisation of criteria, mutual recognition (whether or not within a European Community framework) or something else?

(Question 3) What are the arguments for and against:
- limiting a "Registered Passenger" scheme to nationals of Member States,
- extending them to nationals of third countries legally resident in a Member State?

Exemption from certain security checks (Questions 4 to 7)

(Question 4) From which security checks could "Registered Passengers" be exempted without compromising security? What is the scope for lightening or accelerating certain checks without going as far as exemption?

(Question 5) Would either existing or proposed Community legislation on aviation security allow such changes in procedures? What changes in Community law might be required

(Question 6) Would the revised version of Appendix 17 to the Chicago Convention allow such changes to procedures?

(Question 7) What would be the impact on operations at airports of a two-tier system of passenger screening?

Identification of RPs (Questions 8 to 9)

(Question 8) How best should data on "Registered Passengers" be stored so that national authorities could access it when controlling departing passengers at airports? How could authorities of one Member State be given rapid and easy access to lists of passengers registered by other Member States, when it recognised their registration? The contractor should analyse whether other data bases (existing or planned) would serve this purpose.

(Question 9) As for the identification of "Registered Passengers" when presenting themselves at airports, what system(s) for identifying travelers for border control purposes (existing or planned) might serve this purpose?

Potential benefits to passengers, airlines and airports (Questions 10 to 12)

(Question 10) To what extent would the introduction of a "Registered Passenger" scheme at Community level facilitate air transport? In particular, what reductions in delays might typically be expected, and at which types of airports and at what periods of time?

(Question 11) To what extent would the introduction of a "Registered Passenger scheme" at Community level benefit the operations of air carriers and airports and what might the impact on their costs?

(Question 12) How far might common approaches lessen the costs of identifying passengers and maintaining their data bases?

Client & Consultant

The Client is EC DG TREN.

The following consortium developed the Study;

- Accenture (lead partner)

- Irish Aviation Authority

- Daon

In addition, the consortium was assisted by:

- The University of Leiden – International Institute of Air Space Law

- Max Snijder (Biometrics Expertise Group)

- SITA

Methodology

To obtain and develop information on the feasibility of an RP concept, the Study Team conducted an extensive search of existing information and carried out interviews with key stakeholders. These interviews included officials from governments and representatives from the aviation industry including airports, airlines and associations (a full list of interviews is provided in Appendix A).

The Study Team conducted a literature search that identified existing studies, policy papers, and articles from government, the aviation industry, and other organisations on numerous issues associated with designing and implementing an RP scheme and how existing schemes are developing. An overview of the methodology used to complete the Study is provided in Appendix H.

Section B – Questions and Answers

The first three questions relate to Risk Assessment.

Risk Assessment (Questions 1 to 3)

(Question 1) On what grounds could a set of passengers be reliably assessed as presenting lower risks than others? The contractor should suggest precise criteria for identifying passengers presenting low risks to aviation security (care should be taken to avoid discrimination by sex, race or ethnic origin, religion or belief, disability, age or sexual orientation).

(Question 2) What would be the most promising approach to facilitating the recognition of a passenger registered in one Member State by others that operated "Registered Passenger" schemes: harmonisation of criteria, mutual recognition (whether or not within a European Community framework) or something else?

(Question 3) What are the arguments for and against:
- limiting a "Registered Passenger" scheme to nationals of Member States,
- extending them to nationals of third countries legally resident in a Member State?

1   (Question 1) On what grounds could a set of passengers be reliably assessed as presenting lower risks than others? The contractor should suggest precise criteria for identifying passengers presenting low risks to aviation security (care should be taken to avoid discrimination by sex, race or ethnic origin, religion or belief, disability, age or sexual orientation).

1.1   Introduction

Section 1 of the report provides an overview of criteria used to allow admission to existing RP schemes, where the privileges on offer amount to an improved customer service - without security exemptions. The report then examines current criteria and methods utilised to identify 'high-risk' passengers before explaining why they are not suitable for the identification of 'lower risk' passengers.

[7]*Note: The detail in the answer to this question is derived largely from desk research and consultation – security agencies are reluctant to share assessment criteria and detailed information for reasons of national security.*

1.2   The challenge of developing criteria for identifying "lower risk" passengers

There is a clear need for Control Authorities[8] to have lead responsibility for the definition of passenger risk due to their insight and statutory responsibilities. To date their focus has been on the identification of high-risk passengers who pose a threat to aviation security and border control depending on the type of RP scheme. The RP scheme, as defined in the Terms of Reference, would necessitate the identification of 'lower risk' passengers prior to gaining admission to a scheme and its associated benefits (e.g. exemption from certain security checks or a lighter security process).

There are very few precedents for categorising passengers as 'lower risk' and at present this is restricted to travelers such as Heads of State and other nominated officials. This category of passenger has a lower level of security checks, but is very much an exception. At present even airport staff and flight crew who have been security cleared do not receive lesser checks than travelling customers.

Control Authority feedback on the possibility of identifying and defining 'lower risk' criteria for a wider group of passengers has been that knowing the identity of the person does not change the level of risk in the traditional sense of aviation security. There is no guarantee that an RP will not become a security threat between the point of admission to the scheme and the point of travel - consequently it is not feasible to exempt these passengers from security checks.

Current criteria and methods for identifying 'high risk' passengers are not transferable for the identification of 'low risk' passengers with the certainty that would be required to exempt them from or lighten security checks.

1.2.1   Criteria and methods used by existing Registered Passenger schemes for identifying 'high risk' passengers

---

[7] http://www.ag.gov.au/www/agd/agd.nsf/Page/AbouttheDepartment_Speeches_2005_Astrategicapproachtonationalsecurity

[8] Control Authorities are defined as the departments or organisations responsible for aviation security and national security within a Member State.

At enrollment, existing RP schemes look to ensure that RPs do not exist on a national watch list and other forms of database (such as criminal records or international watch lists); with the aim of preventing any high risk passengers joining the scheme. Once the would-be RP has passed the initial inspection at enrollment and had the relevant items of information recorded (such as biographic data from the passport, other biographic data and biometrics such as fingerprints and facial scans) the next stage is to assess the risk that the individual poses. Some schemes do part of this immediately in-situ (for example, immigration RP schemes where the risk is primarily mitigated by the information in the passengers' passports) and use immediate checks of the databases available from the enrollment location. Some schemes send the information to a central processing point.

This is not sufficient for the type of RP scheme under review in this Study, which aims to assess 'lower risk' passengers because;

- Absence from a watch list or database is not a definitive measure of lower risk. It might be that the person should be on the list but has not yet been added, that the list is inaccurate, or that a different identity has been used for enrollment into the RP scheme

- Passengers could be 'sleeper' terrorists or so-called 'clean skins' whose clean background profiles mean that their names will not currently appear on any lists. Yet, these people may have every intention to conduct terror related activities

- Innocent travelers can be coerced or duped into carrying objects

The use of identity and security checks at enrollment helps rule out the high risk passengers but leaves a large percentage of RPs that need to be assessed as lower risk. The following sections review the various mechanisms available to conduct this assessment.

1.3 Is Official Security Clearance applicable for RPs?

The checks and processes used to conduct security clearance for airport, government and security personnel could also be applied in vetting RPs. Whilst the security checks may vary according to the level of the role, the initial checking processes undertaken before employees are allowed to start employment typically include reviews of in-depth personal information and checks made against security watch lists. In addition, the applicant must declare any criminal background. As the level of the role increases in sensitivity there may be interviews with family and close friends, bank account and credit reference checks for the applicant and their partner, and additional interviews for reference purposes.

This level of checking is still not sufficiently robust to allow employees to benefit from a lower level of security checks. There are many problems in granting this type of privilege - not least that if it became widely known that a person in a certain role or function was subject to lower security checks at airports, then the role or, more importantly, the personnel in this role could become a new weak link in the security chain.

A further problem with the application of detailed staff security clearance to a wider passenger market is the capacity to undertake these checks at the required speed. In reality, detailed security checking processes take a long time and the resources to cope with this are somewhat limited. If (as with the US RT Scheme) the RP programme helps enhance the existing security clearance process and timelines, then the very existence of an RP scheme starts to have benefits for the stakeholders involved. However, the ability to vet individuals using interviews and checks of financial backgrounds is expensive and time

consuming and may be neither practicable to undertake nor attractive to the person applying for RP status.

1.4 Passenger profiling

1.4.1 Passenger profiling and its use in identifying high risk passengers

The methods and criteria used to assess passenger risk need to be robust and systematic. Apart from watch lists, one of the main methods used for risk assessment is passenger profiling, which typically compares a range of passenger information against a 'high-risk' profile. Before reviewing the use of passenger profiling to assess a lower risk passenger, it is important to confirm the definition of passenger profiling.

"[Passenger] Profiling is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics."[9]

Passenger profiling is not the same as a watch-list check – it involves more than a name and passport match and a Yes/No response. Profiling can also be described as risk-scoring and is essentially a predictive device.

The aim of passenger profiling is to compare a person's identity, travel data and in some cases financial and other information, with a designated profile. Profiling is also a useful tool to help remove human bias and mistakes and allows for matching to be undertaken at speed and in advance

Some countries firmly believe in passenger profiling to help create an additional layer of security and are embarking on programmes to implement this. However, to publish the exact criteria of such a profile would give the terrorist valuable information and put security at risk. Despite questions regarding effectiveness and the controversy surrounding profiling, countries are moving forward with passenger profiling systems to assist in their on-going fight against terrorism.

In the UK, there are trials[10] to move from existing watch-list checks using the Semaphore system to more in-depth risk assessment and analysis. In the US, there has been a lot of work conducted in this area with the most recent examples being Secure Flight and the Automated Targeting System (ATS). The former is for internal US flights and the latter is for international flights. There are also plans for a Future Attribute Screening Technology (FAST). This will use real-time data captured from cameras and from sources such as passport, flight and civilian databases.

1.4.2 The challenge of developing sufficiently robust criteria for a 'lower risk' profile

This section analyses some of the criteria often put forward for lower risk assessments and explores their suitability for identifying lower risk passengers.

---

[9] Roger Clarke, Profiling: a hidden challenge to the regulation of Data Surveillance, 1993

[10] http://www.theregister.co.uk/2007/06/15/semaphore_risk_scores/

Notwithstanding the secrecy surrounding the subject, there are some simple criteria that many people point to when asked how to identify lower risk passengers:

- **Age/Data of Birth;** it is often argued that the elderly or the very young could be considered as being 'low risk'. However, there is always the possibility that they are duped or coerced into doing something; for example their family could be being held hostage or they could be the subject of an innocent dupe. Also, in an RP scheme, there is likely to be a minimum age as a result of data protection issues and usage of the automated gates or kiosks that are part of the RP scheme.

- **Passport type and contents;** testing the authenticity of a passport has been suggested as one of the criteria for identifying a 'lower risk' passenger**.** However passports are often forged, stolen or acquired legally but with a different identity. It is argued that in an RP scheme the passport and identity check must be verified by the initial interview/data capture process. In addition, the contents of a passport and previous visa and travel documents would be used to help review where a passenger has been travelling to and from. This could be used to help create a profile and as such a passenger with a clean passport can be considered to be a lower risk in comparison to a traveler with visas and entry stamps to some of the countries that are suspected or known to assist in terrorist activities. This however does not guard against the 'clean skin' terrorist.

- **Nationality;** as has been shown by many incidents throughout the world, terrorist organisations have the ability to recruit from many countries and nationalities and if relied upon solely for assessment these criteria could lead to 'risk blindness', where a certain racial profile is targeted and terrorists use this to their benefit, by recruiting exactly what is not expected.

- **Home Address;** terrorist organisations have the ability to recruit from many locations and to relocate individuals as necessary. As with the watch lists, a person living in an area that has had no previous connection with terrorism cannot automatically be taken to represent a low risk. An example of this was shown by the alleged terrorist attack at Glasgow airport in 2007 where the addresses of the suspects varied between quiet suburbs and hospital accommodation.

- **Employment and Education;** previous events have shown that terrorists come from a broad range of educational and social backgrounds, as evidenced by events at Glasgow Airport in 2007 where several of the alleged terrorists were trainee doctors. Setting criteria such as specific employment only for an RP scheme would not be a very attractive idea to the scheme operators and to the travelling public and further complications would occur in trying to confirm the employment record and what would happen if the person left employment, etc.

- **Existing Security clearance;** it has been suggested that the existing security clearance procedures necessary for employment in the security, government or air travel industry could be the basis for a 'lower risk' assessment for a select few passengers. However, these checks are normally based on watch lists and as such are not sufficiently robust to classify passengers as 'lower risk'. In addition, the potential issues associated with trying to verify the identity and clearance level of the person and the risk of publicising 'privileged' status mean this is unlikely to be used as a basis for assessing lower level risk for aviation security purposes.

- **Income and Financial status;** previous assumptions that the level of risk is inversely related to income and financial status can be dismissed owing to the financial power of

terrorist organisations. An analysis of a person's bank account may allow risk assessment to occur but this is unlikely to be acceptable or achievable on a mass scale for an RP scheme. Some schemes around the world do charge for membership and require a credit card for payment, which provides an opportunity to gather more information about the passenger. A sound financial history with no suspicious transfers is useful but not sufficient to categorise the passenger as 'lower risk' as defined in the Terms of Reference.

- **Flight history and being a member of a Frequent Flyer scheme;** terrorist organisations have significant resources at their disposal and could build up a large flight history for a person, including membership of a Frequent Flyer scheme. For an RP scheme offering security-based privileges these are not sufficiently strong criteria for defining a lower risk passenger.

- **Criminal history;** a mechanism frequently used to identify 'high-risk' passengers is a review of the criminal record that the passenger may or may not have. An advantage of conducting criminal checks is that the obvious cases where a person has been involved in terror related tasks – be it directly or indirectly – can be readily identified. An example of this could have been a history of conspiring to commit an act of terror or supporting terrorist organisations in the past through financing or logistical support. However the absence of a criminal record does not necessarily mean the passenger is sufficiently 'lower risk' to benefit from lighter checks. There are numerous examples where people with no criminal history have been involved in incidents.

  A criminal check is critical to ensure that any obvious 'high-risk' passengers are flagged at enrollment and their potential membership reviewed by the relevant authorities. However, research suggests that the "*direct relationship between criminal history and terrorism is debatable.*"[11] If this relationship is true of higher risk passengers, the validity of using criminal checks to assess lower risk passengers is questionable. For example; passengers may have committed a crime but never been caught; they may have committed a crime and been convicted, but the database has not been updated with the correct information; they may have served their sentence and in society's eyes have 'served their time'; they may have committed a crime, been convicted and the database correctly updated, but the crime is not related to aviation security e.g. non-payment of a parking ticket. These scenarios provide insight into how unreliable it can be to use the lack of a criminal record to identify a low risk passenger.

- **Immigration status;** Most RP schemes check the immigration status of the applicant during enrollment or as part of the security checking process. As with other checks against watch lists and criminal databases, the main aim of this is to ensure no 'high-risk' passengers can enroll, as opposed to helping to further assess a lower risk status once this preliminary step has been taken. However, the confirmation that a passenger is not 'high risk' from an immigration perspective is not sufficiently robust to exempt them from security checks. For example, just because a passenger has a valid passport and/or visa does not necessarily mean they are lower risk. The use of immigration and asylum databases will not help to complete the lower risk assessment, but will help the first stage elimination of any high-risk passengers and also allow for the identity to be fixed and checked through the use of biometrics.

---

[11] Guarding America: Security Guards and U.S. Critical Infrastructure Protection' Congress Report, November 2004.

Even when the criteria are pooled together to create an overall profile the individual weakness of each criterion means that a profile cannot be developed that is sufficiently strong to facilitate the lightening of the security checking process.

1.4.3 Weaknesses in the profiling method

The operational effectiveness of profiling is much debated. Whilst it has been continually argued and stated that no well-defined terrorist profile exists, countries are pushing ahead to use profiling as part of their security toolset. However, as Michael Chertoff (US Secretary of State for DHS) stated:

"Our enemy constantly changes and adapts."[12]

Terrorism suspects with atypical backgrounds are becoming increasingly common. The profiles range across gender, age, race and religion. For example, among those arrested in August 2006 in London in connection with the alleged transatlantic plot, was a young mother married to another suspect in the case. British investigators apparently suspect that she or her husband planned to smuggle liquid explosives onto a flight.

"Al-Qaeda is likely to evolve with knowledge and try to fit a profile of a tourist as opposed to a terrorist." [13] Mr J Turley, Shapiro Professor of Public Interest Law, George Washington University Law School

As soon as a profile is created it will be tested, understood and then worked around. In the aviation security context, a terrorist organisation could send many travelers with different profiles to see if they are flagged as a potential risk and then on subsequent attempts continue to modify the passengers' background and details in an attempt to create the low-risk traveler profile.

Therefore, profiles must be continually updated and a random element introduced. The creation of a profile and a false positive (that is, where a person is incorrectly believed to be a terrorist due to the name match) has the ability to create a media or political backlash.

There is considerable controversy and debate around the use of profiling to help identify lower or higher risk passengers. In addition to doubts about effectiveness, there is strong concern around how data is gathered, used, stored and accessed and the potential for the use of the data to extend beyond the initial scope over time. In the US, the development and advance of profiling systems has fallen foul of data privacy experts and civil rights organisations.

1.5 Conclusion

Security measures are currently geared around the identification of high-risk passengers. A combination of criteria and methods such as checking against watch lists and databases, scrutiny of immigration status, and profiling can be effective in identifying passengers who pose a significant threat to security. When the same security principles are applied to

---

[12] The Economist. 14th July 2005

[13] Mr J Turley, Shapiro Professor of Public Interest Law, George Washington University Law Schoolhttp://commdocs.house.gov/committees/Trans/hpw107-64.000/hpw107-64_0.HTM

identifying a 'lower risk' passenger the chances of error are much higher and the potential consequences are severe.

The conclusion of this section is that a passenger who is not considered to be 'high risk' cannot be regarded as posing so little threat to security as to gain access to a lighter security check process. As a number of Control Authorities consulted during this report made clear, the lack of a clear terrorist profile and the adaptable nature of the modern terrorist means it is difficult to foresee when RP schemes could offer security related privileges without putting passenger safety at risk.

(Question 2) What would be the most promising approach to facilitating the recognition of a passenger registered in one Member State by others that operated "Registered Passenger" schemes: harmonisation of criteria, mutual recognition (whether or not within a European Community framework) or something else?

2.1 Introduction

If an RP scheme was to be unilateral, then international recognition would not be required. However, one of the ultimate aims of an RP scheme is to join up the travel process and create a simplified journey regardless of destination.

This section first examines the three key stages of the RP process; enrollment, risk assessment and identification at the airport. It then reviews mechanisms that would facilitate mutual recognition (that is where a decision from one country is automatically accepted in another country and vice versa) for each of the three key stages.

2.2 The Different Stages of the RP Process

There are three key stages of the RP process that require recognition:

- Enrollment

- Risk Assessment

- Identification at the Airport

2.2.1   Enrollment

The creation of a strong and credible RP enrollment process starts with the setting of enrollment criteria and implementing a clear enrollment process. This includes the confirmation of the applicant's identity and the recording of any required biometrics and biographical information.

2.2.2   Risk Assessment

The next step in the process is the completion of a risk assessment and a decision on whether to approve the membership of the passenger.

On the assumption that the home country approves the membership, the RP can now use the RP scheme in the home country only. An assumption is made that the RP is issued with a membership token at this point.

Depending on the passenger requirements and the availability of other interoperable schemes, the next step is for the 'destination' country or countries to approve membership and give the right to use the RP facilities in their respective countries. This will enhance the value of an RP scheme by allowing people to benefit from the scheme's security checking on their return flight as well as on the outward journey.

2.2.3   Identification at the Airport

An RP could present themselves in any participating country and simply produce the RP membership token and demand to use the RP scheme in that country. A visual inspection of

the membership token could be carried out by a scheme official at this point, but they would have no idea if the RP membership is indeed a valid one.

There is therefore the need for the country to check that the RP identity matches that of the membership token and that the RP is a valid member of the scheme.

2.3 Mutual Recognition

2.3.1 Definition

Mutual Recognition is often used for trade and border control purposes. Mutual recognition means that the certification and approval process undertaken in Country A is automatically recognised in Country B as being valid. For trade purposes, goods that meet inspection processes and are certified in Country A are relied upon as approved in Country B and vice versa. Mutual recognition implies both that country B recognises country A and that country A recognises country B.

2.3.2 Ways to Achieve Mutual Recognition

Mutual recognition can be achieved in a number of different ways:

- 'In-depth' Approach – requiring full visibility and periodic inspections of each member's protocols, testing and facilities and an automated acceptance of the outcome;

- 'Acceptance' Approach – where each country accepts the arrangements that the other has put in place and agrees with their decision (and vice versa).

- 'Harmonisation' Approach – harmonisation of standards, requirements and approval processes. This can be done at different levels of detail, by different bodies and involve either binding rules or recommendations.

Each of the three key stages in the RP scheme is now reviewed to examine how mutual recognition can be achieved.

2.3.3 Enrollment

The 'In-depth' approach could be used where a rigorous and formal inspection process of the enrollment process is carried out by each country on the other to ensure they are content with the arrangements put in place. This has draw-backs as more schemes join and require lengthy and on-going checks.

Instead, a more promising approach uses 'Acceptance' where each country relies on the other to put in place a strong and secure enrollment process and accepts the enrollment process as valid.

This can be further enhanced through the use of a set of harmonised standards. Each step of the enrollment process should use a common set of standards (such as ICAO) to ensure that if an RP interacts with another Member State scheme then their initial enrollment is recognised as standard and accepted. For example, there is a clear need to agree on the standard for eligibility, technical standards and business processes to ensure the schemes can inter-operate.

2.3.4 Risk Assessment

The research and consultation in this study shows that each country will want to conduct its own risk assessment – despite what may have already been completed by the home enrollment country. In interviews, the majority of Control Authorities expressed a key requirement for those countries to conduct their own local risk assessments of passengers resulting in approval or denial. As such, this means that mutual recognition is not achievable at this stage in the process.

2.3.5   Identification at the airport

The RP scheme needs to ensure that the passenger presenting is the right RP who is authorised to use the security lane at that particular point in time.

When the RP visits an airport that has an RP scheme, it is assumed that they will present a token or identification to prove that they are in an RP scheme. A visual inspection of the membership token could be carried out by a scheme official at this point but they would have no idea if the RP membership is a valid one – all they have is a token which suggests that at some point in the past their membership was approved. Also, visual inspection of photographs is not as reliable as biometric checks to ensure the identity on the membership token matches the person who is presenting it.

Therefore, other checks would be needed to ensure that mutual recognition can occur. These checks would be based on harmonised and agreed common standards that allow for technical verification and authentication of:

Identity: Using biometrics will enable the RP scheme to confirm the identity of the person against the membership token. This ensures that the card has not been passed to another person to use. Common standards and protocols will help this process and ensure the end point of the scheme is as strong and secure as the enrollment process.

Authorisation: Following identity verification and authentication, the RP scheme next needs to ensure that the RP is authorised to use the RP scheme. It would do this by checking that a risk assessment had been completed and that the person can use the RP scheme in that particular country.

2.4 Conclusion

There are three key stages to an RP scheme that need to be considered when assessing the most promising approach to international recognition:

- Enrollment

- Risk assessment

- Identification at the airport

Mutual recognition can be achieved for enrollment and identification at the airport. Whilst in-depth checks would not be suitable due to the number of schemes involved, acceptance of other schemes processes based on common standards could enable mutual recognition.

For risk assessment, the feedback from Control Authorities is that mutual recognition would not be acceptable, and each country is likely to conduct their own assessment.

3 (Question 3) What are the arguments for and against:
– limiting a "Registered Passenger" scheme to nationals of Member States
– extending them to nationals of third countries legally resident in a Member State?

3.1 Introduction

Interviews with Control Authorities suggest there is a balance to be struck between giving customers the opportunity to join RP schemes wherever possible and maintaining the credibility of such schemes by ensuring those applicants who become members have passed through a rigorous risk assessment.

An assumption is made that RP schemes are designed to facilitate the movement of people throughout Europe, regardless of whether they are nationals of Member States or nationals of third countries legally resident in Member States.

The remainder of this section examines the arguments for and against the membership parameters set out in the question.

3.2 Arguments for limiting a Registered Passenger scheme to nationals of Member States and against extending membership to nationals of third countries legally resident in a Member State:

There are a number of arguments put forth for limiting an RP scheme to nationals of Member States and against extending membership to nationals of third countries, they include:

- *Availability of Data:* In many cases nationals of Member States will have a profile built up within the State from birth. This provides a high level of confidence in the vetting system, as a comprehensive history of the individual is available to national authorities to complete a risk assessment. There may be a lack of information relating to a third country national's history prior to taking up residency in a Member State. This could negatively impact the strength of the risk assessment completed.

- *Sharing of Data:* Full risk assessments of non-nationals legally resident may be more difficult to conduct as the sharing of information, due to data privacy, may be limited or even deemed to be illegal. However, if the RP gives explicit permission for information to be shared and accessed this may be overcome.

- *Availability, Timeliness and Cost of risk assessment:* Unlike local checks for nationals of Member States, having the authorities in a third country perform a risk assessment on an applicant from that country may not be possible, may be too costly or may be too time consuming. Some countries see this as virtually impossible.[14] However the home country could request the enrollee to assist this process by giving their permission for the necessary assessment to be completed, and sign up to the understanding that if the findings are not satisfactory then their enrollment may be denied.

---

[14] Interview with Maltese Ministry of Justice & Home Affairs (OMAS – Office of the Airport, 18th April 2007)

The arguments for limiting membership are based on the premise that it is easier to conduct a risk assessment of a national of a Member State than that of a national of a third country legally resident in the Member State – in respect of availability of information, speed and cost of data sharing.

However, if this risk assessment is based on a set of standard security checks and if these can be carried out equally on nationals of Third Countries this argument for restriction is weakened. These arguments are further weakened if RP schemes fully inform third country applicants that they will not become scheme members if sufficiently robust risk assessments cannot be completed on their applications. The question of cost feasibility might also be challenged if applicants are willing to pay for the additional costs.

3.3 Arguments against limiting a Registered Passenger scheme to nationals of Member States and for extending membership to nationals of third countries legally resident in a Member State:

- *Economic:* Limiting the scheme reduces the potential eligible passenger population and potential economic benefits to be gained. For example, the US RT scheme is only open to US citizens, US nationals and permanent legal residents. There is demand for inclusion from other travelers who regularly travel to the US.

- *Legal:* Limiting the scheme projects an image that air travel is less user-friendly to nationals of third countries legally resident in Member States and may expose the RP scheme to legal challenge. The rights of non-EU nationals legally residing in the territory of a Member State to travel within the European Union are outlined in the EU Charter of Fundamental Rights. The charter asserts the right of every European citizen to move and reside freely within the territory of the Member States. It adds that these rights may be granted to third-country nationals (depending on entry requirements and eligibility).

- *Social:* It is probable that if the scheme is introduced in a limited form, there would be severe pressure to allow certain categories of non-nationals to take part, for example, those who have held residency for a prolonged period of time. In this case a qualifying number of residency years could be set to enable legal residents to be considered. If the applicant is resident for a significant period of time there should be enough information for a thorough risk assessment to be carried out.

- *Practical Issues:* Issues would arise with families or couples that have mixed nationality – how do RP schemes deal with the situation where one passenger can join but their partner or colleague (who is on the same flight) cannot? This may affect the commercial viability of the scheme.

Arguments against such restrictions are based on economic, legal, social and practical considerations. On the economic front, fewer restrictions mean the potential for more customers and the ability for the benefits from an RP scheme to extend to a wider population. Socially, there is likely to be significant pressure from lobby groups against restrictions based on country of origin, which could lead to negative publicity about RP schemes and the aviation industry in general.

3.4 Conclusion

Arguments against the extension of membership are based on the difficulties encountered in sharing data and gaining access to the requisite information from third countries, and even when this is possible, the time and costs incurred in doing this.

Arguments in favour of extending membership to third country nationals include increasing the size of the potential customer base, the avoidance of negative publicity and meeting the legal and political aim of extending EC travel rights to third country nationals.

Exemption from certain security checks (Questions 4 to 7)

Questions 4 to 7 relate to exemptions from Certain Security Checks:

(Question 4) From which security checks could "RPs" be exempted without compromising security? What is the scope for lightening or accelerating certain checks without going as far as exemption?

(Question 5) Would either existing or proposed Community legislation on aviation security allow such changes in procedures? What changes in Community law might be required

(Question 6) Would the revised version of Appendix 17 to the Chicago Convention allow such changes to procedures?

((Question 7) What would be the impact on operations at airports of a two-tier system of passenger screening?

4 (Question 4) From which security checks could "Registered Passengers" be exempted without compromising security? What is the scope for lightening or accelerating certain checks without going as far as exemption?

4.1 Introduction

Up to section 4.4 the definition of an RP scheme used is that defined in the Terms of Reference, which rewards members with exemptions from certain security checks or lightens the security checking process. From section 4.4 onwards, where the scope for accelerating security checks is outlined, RP schemes are considered that offer an improved customer experience, but do not include exemptions to or the lightening of security checks.

This section outlines existing primary and random checks, examines the arguments around exemptions to or lightening of security checks, and finally considers options for accelerating checks for RPs.

4.2 The current position - existing security screening processes

Regulation 2320/2002 details specific measures for passengers and their cabin baggage:

- **Screening of Passenger**s; shall be conducted by hand, or Walk-Through-Metal-Detection equipment, and/or a hand-held metal detector if needed. There shall also be re-screening of any passengers that cause the alarm to sound and a continuous random search for passengers that do not cause the alarm to sound.

- **Screening of Cabin luggage;** shall be conducted by hand or conventional x-ray equipment with hand searching of bags conducted on a continuous random basis or those with which the operator has concerns. For high definition x-ray equipment that has Threat Image Protection (TIP)[15] installed, only bags about which the operator has concerns need be searched by hand and supported (if needed) by Trace Detection Equipment.

For the purposes of this Study, the measures have been grouped into primary and random checks, which relate to the way a traveler is normally processed at an airport:

- **Primary Checks;** where the passengers pass through the Walk-Through Metal Detector (WTMD) and put their cabin luggage in the x-ray scanning devices. In cases where the passenger causes the alarm to sound, they may be requested to be screened again by WTMD equipment or searched by hand where a handheld metal detector may be employed.

- **Random Checks;** where WTMD equipment is used it is mandated that a continuous random hand search of screened passengers will occur. Hand luggage is also checked on a continuous random basis, where the percentage of luggage searched is not less than a stipulated amount.

---

[15] TIP inserts digital threat images at configurable frequencies into the regular flow of bags displayed on the computer screen.

4.2.1 Primary Checks

Research and consultation consistently supported the view that primary checks should be the same for everyone and there should be no exceptions for a specific group of passengers.

For thoroughness, the Study Team consulted on the need for any security check at the airport. Whilst a few airports and airlines pointed to comparisons at public meeting places such as shopping malls and sports stadia where no checks are undertaken, there was a strong recognition of the value and impact of air travel and the global impact of any incidents. As one official explained;

"Aviation is iconic and unique; there is a major impact if a plane changes course and becomes a weapon. It is also a powerful media tool – capturing the mindset and imagination."[16]

Another stakeholder commented;

"No free access to the Secure Restricted Zone should be given to any person. This would not be acceptable to the government, border control and passengers".[17]

The existing exemptions in Regulation 2320/2002 (as per the response to Question 5) relate to designated individuals only, such as Heads of States and some government and armed security officers – which represent a minute percentage of the total airport passenger number. A primary level (or baseline) search is considered essential due to the fact that no RP scheme will remove the possibility of a sleeper terrorist. Terrorists could successfully enroll in an RP scheme because:

- The risk assessment was inadequately performed

- There was collusion with risk assessment personnel

- They were sleeper terrorists with no previous record to suggest they were indeed a threat in the first place.

In addition, there are people who may be legitimate RPs and have a clean background but could at some point become innocent dupes. There are various examples of this, but the example of Anne Murphy was given by one Control Authority official[18] as a clear reason why exemptions to security checks or access to lighter security checks are not feasible.

An example of the innocent dupe

Anne Murphy was a 32-year-old hotel chambermaid from Dublin, Ireland, who was six months pregnant and on her way to marry her fiancé in Israel. Authorities discovered a bomb in her carry-on bag as she boarded a plane in London on her way to Tel Aviv; this had been planted there by her fiancé.

---

[16] Interview with UK Home Office, 1st May 2007

[17] Interview with Polish Civil Aviation and Facilitation Department, 12th April 2007

[18] Interview with Frank Durinckx, 24th April 2007

In addition to the threat of the sleeper terrorist and the dupe, the threat of the RP becoming a target for coercion is another compelling reason why baseline checks should be applicable across the board.

4.2.2   Random hand searches

Random hand searches are an integral part of a multi-layered approach to security. They are necessary for four reasons:

- By their very nature - walk through metal detectors only detect metal and not other potential threats

- The walk through metal detectors do not always have a 100% success rate in detection

- Cabin baggage checks using X-ray machines may have difficulty in detecting explosives, although some newer machines do have this capability[19]

- Systems, including explosive detection systems, are not 100% error-proof

Control Authorities confirmed that searches done as a result of an alarm (and based on the mandated percentage of searches) are an important part of the security system and not an addition. Some interviewees would have liked to see these increased to 100% but were aware of the need to balance security with facilitation.

Countries have the right to increase the percentage of random checks from the mandatory minimum depending on the threat level and also to introduce other more stringent security measures if they wish. The latter accounts for some of the variation in processes across Europe, e.g. where shoes are removed or a belt scanned. The percentage of actual checks conducted in each nation is not widely discussed and is often related to the national threat level. In the UK, the national threat level is now published to give the public and media more insight into why security may be increased.

Section 4.3 assesses the feasibility of lightening security for RPs through reducing these random checks. Section 4.4 goes on to assess the scope for accelerating security checks for RPs.

4.3 An option for lightening security for RPs – reduced random screening

Section 4.2.1 illustrates why Control Authority interviewees felt so strongly that no option exists for reducing primary/baseline checks for all passengers. The risk associated with this in the context of such an adaptable threat and imperfect intelligence is too high. However, one option discussed with stakeholders was that of reducing random screening.

4.3.1   Reduced Random Screening

---

[19] Produced by the Smiths Group, advanced X-ray machines incorporate an Advanced Threat Identification X-ray (aTiX) facility which detects explosives and liquid.

There is a potential option for RPs and their cabin bags to be subject to random screening procedures, but at a lower frequency than those of non-RPs or even a zero percentage. This option would not include any checks required as a result of an alarm at the Walk Through Metal Detector (WTMD) or cabin baggage x-ray, which should still remain in place for RPs as well as ordinary passengers.

The current minimum percentage of random checks stipulated in Regulation 2320/2002 could be reduced towards a lower or zero percentage of RPs' bags with the ability to increase these at random to ensure that patterns are not created that in turn provide the terrorist with a potential weak point.

There were mixed views over the ability to reduce random screening;

• Most of the Control Authorities consulted were firmly against the option of reduced random checks, since providing a 'guarantee' of lesser random checks for an RP scheme would advertise a potential weak link to terrorists. Some of the Control Authorities believed there was potential for reduced levels of random checks.

• Airports and airlines were of a different mindset – believing that it is possible to reduce the secondary checks for lower risk passengers and use this as part of a risk-based approach.

There are two key points for consideration – (1) could an RP scheme guarantee fewer or zero random checks? and (2) can you assess a lower risk passenger?

1. Could an RP scheme guarantee fewer or zero random checks? It is easy to see that this could be used as a key benefit of an RP scheme and so would be advertised as such to the traveler. If so, and assuming existing technology remains the same in terms of level of screening, this creates an issue for security as it would in effect advertise a loophole that could be exploited. If the scheme does not advertise this and the benefit is still given, then this is still likely to be eventually exposed as a potential security risk.

2. The more fundamental point is around the accurate assessment of lower risk passengers – as outlined in the answer to Question 1, the ability to systematically confirm a lower risk profile for a passenger is questionable.

Other impacts of reduced random checks are detailed in the next section.

4.3.2   Impact of Reduced Random Checks

If this option were to be adopted as part of the RP scheme, the impact on operations would be marginal from a staffing perspective, as there would still need to be a member of security staff in attendance to conduct the (albeit reduced) percentage of checks. If the funding for the RP scheme is separate from the normal security budget, and if the RP lane staff are in addition to the existing pool of security personnel, then there would be a benefit for the overall security resources available.

Operational management of security staff would also need to be handled carefully to ensure the on-duty management and staff are aware of the RP concept and operating procedures. This is to ensure that the staff not only understand the lesser checks, but are also aware of the potential reaction from RPs if stopped for the random search, or if the security threat level has increased. One airport representative summarised this as the "Do you know who I am?" issue – where the customer believes the service they have signed up to is not the one they are experiencing. Therefore, if this option were to be included in the RP scheme, both

passengers and stakeholders would need to have expectations and service levels clearly set.

From a customer perspective, the advantage of lesser random checks is clear if the throughput of passengers is increased and the amount of people needing a check reduced. However, despite these benefits there is a fundamental issue with the very existence of an RP scheme that allows lesser security to a subset of passengers, which undermines its validity. As one airline representative accurately summarised,

"The day there is an issue and the passenger involved is an RP, then this could render the whole scheme redundant." [20]

The Study Team agrees that the logic of less random screening for lower risk passengers is appealing, but only if lower risk passengers can be identified without increasing risk to the system. The view expressed throughout this report is that that is not possible.

Any reduction of random screening for a specific group of passengers (with the exception of those identified in Regulation 2320/2002 for operational or political reasons i.e. Head of State) would create a weak link in the security process that could be exploited and bring with it severe consequences.

4.4 Creating a better customer experience - options for accelerating existing checks

"The government cannot afford or feasibly implement the means to protect everyone against everything. We can however, focus on the right combinations of People, Processes and Technology to support the most secure and cost-effective security solutions" [21] Airport Operations of the Future, Accenture White Paper. March 2007

A more realistic option than reduced random checks is to review the process, technology and people that are the foundations of security checks in order to make them faster, more convenient and less frustrating for travelers. The aim would be to create a better travel experience initially for RPs and eventually for the ordinary non-registered travelers.

The scope for improvement is dependent on the type of airport under consideration and current performance levels. In some circumstances, significant improvements might be realised. For example, future technology and screening devices may remove the need for random checks to occur, as this could be built in to a new one-stop check. In addition, RPs may not be required to remove laptops from their cabin baggage or indeed have to remove jackets or shoes. The aim of this assessment of technology, process and people would be twofold:

- To increase speed and minimise inconvenience

- To maintain (or even increase) security checks by applying new improved technology

It is possible to envisage an RP scheme that has a commercial focus based on increasing speed and minimising inconvenience whilst maintaining or improving aviation security. A wide range of schemes currently exist, ranging from examples such as the US RT

---

[20] Interview with Ryanair, 30th April 2007

[21] Airport Operations of the Future, Accenture White Paper. March 2007

programme in which the focus is solely aviation security to the Privium scheme in which the quality of customer service is the prime consideration, with some attention being given to the automation of border control checks.

The improvements that could be effected through RP schemes will most likely reflect a more general trajectory in aviation security as it responds to customer demand. Any such changes might be easier to implement if additional funding is available from RPs, whose membership fees secure early access to improved security arrangements.

4.4.1 Registered Passenger schemes that use existing technology but improve screening process and / or increase resources supporting RPs

Process reengineering

RP schemes could be based on improving the security checkpoint process through process reengineering to make it easier and quicker for the users, especially for frequent travelers who understand the process quite well already. Airports are not just using new technology to help the passenger journey; they are using insights from other industries where queue and people management are a key priority. For example, Orlando airport has introduced an appointment-based security process giving the passenger a dedicated slot and time for security screening; this trial is on-going but results have been good. In the course of the review no evidence was made available to assert the exact acceleration such improvements might achieve.

Some direction might be taken from case studies in the retail sector (such as large supermarkets) in the way they position their check-outs (mitigating space constraints) and differentiate between customer types (e.g. families, large parties, people that need assistance and people that need no assistance and are travelling alone).

Increasing resource capacity and capability

Another option would be to increase staffing capacity and use resources more effectively. For example, if an RP is selected to have a random hand search or their bag needs to be checked, this might be completed by an additional resource and not the resource managing the RP throughput. In a similar way to other industries there could be extra assistance and space made available for RPs to increase throughput, increase customer satisfaction and at the same time reduce the frustration of people waiting to collect bags due to the people in front of them being checked.

4.4.2 Registered Passenger schemes that adopt new technologies to improve the screening process and / or fund developments through their fees

In the US and in Europe there are advances in technology that are being tested or rolled out to help facilitate passenger security checks. These include, but are not limited to:

- Backscatter Technology

- Millimetre Wave

- Explosive Detection

- Other technologies

Note: These technologies are described in more detail in Appendix E.

An aim referenced by a number of stakeholders is the application of new technology to create a 'one-stop-shop' for existing checks that are currently conducted in a sequential order. Whilst it may not be faster, as one airport representative stated - "*New technology is often expensive and slower,*"[22] - it could be more convenient for passengers. Another airport representative also raised the point that new technology may be more secure, but could be slower than existing checks[23]. Even with slower technology conducting the security check, there is the potential for a 'one-stop check' to reduce the effort of divesting clothing and laptops and when combined with reduced queuing time for RPs, improve the overall experience.

Much of this debate is largely hypothetical as this one stop system is not currently established anywhere. The combination of innovation and customer service is perhaps most strongly evidenced in the US RT[24] programme where different schemes are introducing integrated devices to check the passenger at check-in. The RPs place a fingertip on an explosives scanning device and stand on a scanning platform that determines if their luggage contains dangerous devices. The potential for technology to accelerate the end-to-end security experience for customers is clear from such examples and some control authorities and airports view the implementation of RP schemes as a means of developing, certifying and implementing new technology at a quicker pace. The premise for this argument is that the additional funding from RP schemes be reinvested into the trial of new and faster technologies, and also to support the updating of processes and the provision of additional staff. Eventually this new technology could be rolled out to all passengers with newer advances offered to RPs.

The degree to which there is a sufficient market to support the level of R&D and implementation costs such technological advancement requires needs to be tested more thoroughly before the feasibility of this business model can be confirmed.

4.4.3 Funding options for improving the customer experience

Whilst the quicker screening technology may not be immediately available to increase throughput from a screening perspective, the ability to put new lanes, people and processes in place could represent a quick win for the RP schemes. New technology can be expensive and innovation involving people, process and technology is not cheap. This has a clear impact on the set-up and funding of an RP scheme; for example, biometric verification kiosks (to ensure only valid RPs can access the dedicated screening lane) can cost more than $150,000 each[25].

The method of funding RP schemes was the subject of much interest from stakeholders. There are several potential business models that can be used to fund RP schemes each of which has a level of uncertainty associated with them, they include:

---

[22] Interview with Maltese International Airport, 18th April 2007

[23] Interview with BAA, 20th April 2007

[24] It is interesting to note that the US RT programme is the only scheme that focuses exclusively on aviation security as opposed to border control; this is the reason why it is a key scheme to include in this Study.

[25] http://www.bakercapital.com/press/pdf/12-13-06-vip.pdf

Fees paid by RPs

This appears the most likely option with RPs paying for the service. Existing US examples suggest that such a demand exists - the following statistics are from a recent survey from FLO Corporation and the Business Traveler Coalition:

• More than 82 percent of respondents indicated they would like the airlines they travel on to embrace Registered Traveler schemes.

• Eighty percent of respondents would pay $99 for a programme membership in return for consistently expeditious security checkpoint processing, without any other in-lane benefits, such as not having to remove shoes, laptops and coats.

"Travelers are indicating that not having to remove shoes or laptops would be a convenience," said FLO Corp. CEO Glenn Argenbright. "However, what is truly important to them is expeditious security lane processing that is predictable and consistent from airport to airport such that a business executive would not have to leave a customer's office 45 minutes early because of not knowing what to expect at an airport on any given day."[26] However, more market research is required into whether RPs would be willing to pay for research that in the long run might benefit everyone, not just themselves.

An example of a security focused scheme is the US RT programme which is funded by the applicant and managed at a local level by the airport. The airport may outsource the operation to a private company but they remain at the heart of the decision, which is critical as they own the infrastructure. The TSA is the overall approving body and also responsible for the risk assessment, approval mechanism and associated liabilities. They receive part of the application fee to cover such costs and management.

RP schemes facilitating a better customer experience for all…

An idea suggested to the Report Team in the course of the review was that a European RP scheme could mandate a percentage of fees to be used to help fund research at a European level into new technology, or at the very least, help to fund trials and early installations of new technology.

This would help to bring a real benefit for all travelers and not just RPs. In the short term the main benefits would be for the RP, but in the longer term this would filter down to all passengers as technologies become cheaper. An alternative model might be developed for mandating fees from commercially run RP schemes into a central pool for improving the experience for all passengers (through technology, process, and people). However, there are clear obstacles in implementing such a model – not least selecting which airports would benefit from funding from this central pool and getting agreement from the schemes already operating in Europe.

Non–research based benefits are likely to be more immediate to all passengers. RP fees might finance the early purchase of screening machines using new technology, which at some point might be used by non-RPs (e.g. when there are no RPs using the equipment). Depending on the take up of such schemes and the revenues they generate there is also

---

[26] The above quotes comes from an article at: http://secprodonline.com/articles/49544/

the potential for new machines to reduce the pressure (volume of passengers) on existing machines and systems, which could improve the experience for all passengers.

Free of charge schemes

Alongside the passenger paying to completely fund a scheme, there are other business models that exist extending to the other extreme i.e. free of charge for the customer - for example the IRIS scheme run at London Heathrow is currently provided free of charge. IRIS is funded by government and is seen as a pilot or forerunner for larger scale schemes for all passengers that carry ePassports.[27] The IRIS scheme was a trial and has evolved into a permanent programme. It currently has over 100,000 members. The RAPID System being tested in Portugal uses second generation ePassports and facial biometrics to help automate border control. The feasibility of this model being rolled out for other RP schemes will be dependent on the type of benefits it offers and to whom. Research has shown that schemes that are free of charge to the customer are mostly at trial or in the early stages of deployment.

Other Funding Models

Between the two extremes (i.e. full payment or free of charge) there are many models that include schemes being part subsidised by other organisations. Such organisations include:

- Airlines looking for ways to differentiate themselves in the market place

- Airports looking to enhance the customer service offering or create a frequent flier scheme

- Governments that may be interested in some of the benefits for their citizens and look to share the costs of a scheme

- Other organisations (such as large businesses that will buy cards for their employees, or those interested in the same type of market e.g. credit card companies or hotel chains).

The costs of such schemes, and the methods by which they are funded, would need to be reviewed in detail. As with benefits, costs will vary depending on the organisations involved and the location of the scheme. The ability to charge for a premium service without incurring legal challenge must also be assessed early in the planning and assessment phase for each of the participating Member States.

A Time for Change?

Some airports and airlines questioned the current complexity of the baseline and random checks and how additional layers have been applied as a reaction to threats. Some see this

---

[27] The Border and Immigration Agency's iris recognition immigration system (IRIS) provides an automated biometric barrier entry system using iris recognition technology for pre-registered travelers at selected ports in the United Kingdom. IRIS provides fast, secure clearance through UK immigration controls for pre-assessed passengers, enabling immigration control staff to concentrate on higher priorities and reduce the possibility of identity fraud. The scheme is voluntary and is principally targeted at frequent travelers; permanent residents, visa holders and work permit holders. It is anticipated that IRIS will remain a feature of the arrivals control at least until the emergence of the e-borders solution. IRIS is currently free to enroll in – it is unknown whether this will be the case in perpetuity.

as the wrong way to approach security and instead want to start again with a variety of checks and devices and a random allocation of ordinary customers. Whilst this is not within the scope of the report, it is clear that the sentiment is strong and that industry believes that the security process needs a thorough review in light of the continued additions.

4.5 Conclusion

The research and interviews conducted during this review show that it is not possible to exempt RPs from any security checks, or indeed lighten any of them, without compromising security.

The possibility of reducing random checks for RPs was examined, and this met with mixed reaction from stakeholders. Most Control Authorities were against such an idea although some were in favour. Airlines and airports would like to see a reduction in random checks for RPs. However, the inability to accurately define a lower risk passenger makes this option questionable and the creation of a lower security level has several impacts. The most serious of these is the creation of a weak link in the aviation security chain, which could have severe consequences.

One area where there is more scope for feasible change without compromising security is in accelerating checks. This acceleration is most likely to be realised through a combination of improved technology and processes and the increased capacity of security screening areas and personnel.

The potential impact of such developments will depend on the airport in question. One issue raised with stakeholders on such improvements related to how they would be funded. There are several business models that can be considered. The most feasible of these entails the RPs paying membership fees.

Central to a number of business propositions around RP schemes is the eventual benefit all passengers will gain from the advances and improvements that they expedite. This is difficult to assess in existing RP schemes given the commercially sensitive nature of the relationships between suppliers, airports, airlines and Control Authorities.

.

5 (Question 5) Would either existing or proposed Community legislation on aviation security allow such changes in procedures? What changes in Community law might be required to permit them?

5.1 Introduction

The analysis of legislation in this section is based on the interpretation of – "such changes in procedures" – as being changes that would allow exemptions to security checks for RPs, or a lighter security check process for them. This section examines both existing and proposed legislation.

5.2 Existing legislation

Existing legislation focuses on Regulation 2320/2002, which is based upon ECAC Doc 30, and from hereon referred to as *'the Regulation'*, which applies to airports located in the territories of the EC Member States.

The objective of the Regulation is that the security measures listed in the Annex to the Regulation must be implemented at EC airports (with the possible exception of small airports), for which implementation EC Member States are responsible. The security measures drawn up in the Regulation must be considered as *minimum* requirements, as "Member States may apply, in compliance with Community law, more stringent measures."[28] These form part of the National Aviation Security Plan (NASP) that each state must have in place.

The passenger and cabin baggage related measures listed in the Annex to the Regulation pertain to their search or screening by various methods (refer to Section 4.2) and the condition regarding the separation of departing and arriving passengers.[29] They do not concern the examination of passenger data. The question is whether RPs may be exempted from the provisions relating to screening laid down in Chapter 4.1 of the Annex to the Regulation.

The Regulation contains one provision pursuant to which "*categories of persons*" (italics added) may be exempted from screening (see Chapter 4.3 of the Annex). However, since other provisions (especially those laid down in Chapter 4.1) dictate that all passengers must be screened, it would seem that the exemption envisaged in Chapter 4.3 concerns security staff and Heads of State or other very important people as designated by the local country and held on locally controlled lists. This may vary from country to country and one of the aims of the proposed regulation is to help standardise the use of such local lists. In practice, it might be that the Heads of State (for instance, the Queen of the Netherlands) are exempted from security checks but Ministers are in fact screened, and so are diplomats. Non-European Ministers have protested against their submission to security checks.

Hence, exceptions for the benefit of RPs may only be made in accordance with an amendment of the Regulation, unless the list of nominated persons coming under Chapter 4.3 of the Annex of the Regulation includes an EU designated RP scheme and associated passengers, which, as stated above, is unlikely.

---

[28] See Article 6 of the Regulation
[29] See Section 4.1 and 4.2 of the Appendix to the Regulation

In terms of smaller airports, Member States are responsible for the provision of an "adequate level of protection" at the smaller airports as defined by the Regulation, which may be exempted from the security measures listed in the Annex. The Commission must examine whether such national measures applied to smaller airports are justified for (1) objective practical reasons, and (2) provide an adequate level of protection. Consequently, these two conditions must be met if a Member State wants to create a special position for RPs at smaller airports on its territory.

The Regulation is currently being revised, as briefly explained below.

5.3 Proposed legislation

The Commission has proposed a new regulation to replace Regulation 2320/2002, which presently is before the European Parliament and the Council for adoption. In order to be enacted, both must approve the new regulation but, just for the sake of simplicity, the common position taken by the Council on 11th December 2006 is taken as the point of reference for this discussion. The proposed Regulation has been laid down in the Common Position (EC) No 3/2007, adopted by the Council of Ministers on 11th December 2006, with a view of adopting a Regulation on common rules in the field of civil aviation security. It is referred to hereunder as *'the Proposed Regulation'*.

The Proposed Regulation is designed to provide flexibility to adapt implementing measures meeting evolving risk assessments, and to allow for the introduction of new technologies. The aim of the revision is to improve simplification, harmonisation and clarification of existing rules and the improvement of the levels of security.

Part of this revision relates to the laying down of basic principles without going into technical and procedural details on how they are to be implemented.

As with the existing Regulation 2320/2002, the Proposed Regulation provides for the implementation of detailed measures, to be adopted by the Commission with the consent of the Member States (pursuant to the co called '*comitology procedure*'). Amongst other things such detailed measures concern 'categories of persons… that for objective reasons shall be exempt to special security procedures, or shall be exempted from screening, access control or other security controls.' Objective reasons in this instance, as with the existing Regulation, are assumed to refer to officials of the security services and VIPs, and not RPs.

However, unlike the existing regulation, Chapter 4 of the Annex (to the Proposed Regulation) does not give room for exempted categories of originating passengers. Consequently, the margin for the application of alternative security measures for RPs appears to have narrowed down in the current text of the Proposed Regulation.

5.4 Conclusion

At the time of writing the existing and proposed legislation does not contain special procedures for the benefit of RPs. They are thus subject to the same security measures as all other passengers. If required, procedures for the benefit of RPs might be achieved by amending the above regulations.

Since the proposal for a regulation which is designed to repeal Regulation 2320/2002 is at an advanced stage of adoption, the position of RPs must be considered under the implementing measures provided for the text of the Proposed Regulation (repealing Regulation 2320/2002) as agreed upon between the Community institutions. Special

procedures for the benefit of RPs are difficult to construe under the current text of the Proposed Regulation.

6   (Question 6) Would the revised version of Appendix 17 to the Chicago Convention allow such changes to procedures?

6.1 Introduction

ICAO is the principal legislator for worldwide civil aviation, especially so in the areas of safety and security. Its rules are laid down in so called Standards and Recommended Practices which are included with the 18 Annexes to the Convention on international civil aviation of 1944, henceforth also referred to as the Chicago Convention. The Chicago Convention and ICAO (which is established by the Chicago Convention) have 190 contracting states, including the 27 EC Member States. The EC is not a party to the Chicago Convention but has observer status.

This section considers whether the revised version of Annex 17 to the Chicago Convention would allow changes to procedures that would enable RP scheme members to be exempted from certain security checks or experience a lighter security checking process.

6.2 The Binding Force of ICAO Standards

ICAO's Standards are not binding *per se*. States must implement them in their national legislation in order to give them legal force. ICAO states are responsible for their application and enforcement. ICAO states must notify ICAO if they cannot implement and apply a particular Standard. However, practice shows that ICAO states are not compliant with such reporting (regarding their non-compliance with ICAO Standards). ICAO does not have the (supranational) powers to take corrective action against such states.

The binding force of ICAO Standards cannot be determined in a general fashion for all EC Member States. EC Member States apply different legislative systems for the implementation of such Standards. The binding force can only be determined by examining the legal systems of the EC Member States on this point. Recommended Practices which are written in italics in the ICAO Annexes are recommendations only. They do not have binding force unless ICAO states choose to give them binding force under their national law. They have not been considered in the context of this study.

Depending on the formulation of the measure, ICAO Standards may be considered as minimum or generally formulated standards. In such instances, contracting states of ICAO, including EC Member States, may adopt stricter or more specific norms. An example of this is Standard 4.4.1 in Appendix 17:

> 'Each Contracting State shall establish measures to ensure that originating passengers of commercial air transport operations and their cabin baggage are screened prior to boarding an aircraft departing from a security restricted area.'

The minimum rule is that ICAO states are under an obligation (as they 'shall establish') to introduce security measures prior to boarding. States must decide which security measures they apply. This obligation is not enforceable by ICAO but may be enforced on a national level or through bilateral or multilateral aviation arrangements. Under such arrangements States may agree not to give permission to airlines to fly through their airspace or land in their territory if it has not screened passengers and baggage before boarding. The US is a prime example of enforcing such an obligation.

6.3 Appendix 17

The version of Annex 17 used for the purpose of this Study incorporates all amendments adopted by the ICAO Council prior to 1st December 2006. The relevant text is the Eighth Edition dated April 2006. Appendix 17 does not have any classified parts. Annex 17 refers at several instances to the Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference (Doc 8973). Access to this document is fully classified and is available only to ICAO contracting states.

Relevant Standards of Annex 17 are:

- Standard 2.1.1, dictating that ICAO states must have as their primary objective the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation. This standard is therefore not only concerned with the security of international, but also of domestic, civil aviation. The Chicago Convention governs *international* civil aviation.

- Standard 4.4.1 provides that ICAO states must establish measures to ensure that originating passengers of commercial air transport operations and their cabin baggage are screened prior to boarding an aircraft departing from a security restricted area.

- Standard 4.4.2 lays down rules for security checks of transferred passengers, and for ensuring that all passengers are screened before boarding.

- Section 4.7 draws up measures for special categories of passengers. This section foresees the development of requirements for so-called disruptive passengers and passengers who have been subject to judicial or administrative proceedings. Such measures must guarantee the safety on board an aircraft on which disruptive and other identified passengers are carried.

6.4 Conclusion

The ICAO measures – apart from those pertaining to disruptive passengers and passengers who have been subject to legal proceedings – apply without exception to RP schemes. As such there are no exemption procedures for RPs under Annex 17 of the Chicago Convention.

7 (Question 7) What would be the impact on operations at airports of a two-tier system of passenger screening?

7.1 Introduction

There several approaches to the implementation of a two-tier system of passenger screening. This section examines the impact of these approaches at airports.

7.2 Existing Landscape

Some airports already have a two-tier system of passenger access to screening. In addition to the ordinary passenger screening lanes, they have dedicated lanes for premium ticket types. The same level of security checks are administered regardless of ticket type. In addition, some airports also have dedicated staff and crew access points - again, the same checks are undertaken, as per Regulation 2320/2002.

The introduction of an RP scheme would potentially result in the creation of a new tier of passenger screening and the impact on operations would focus on the two key process steps:

• Identification and verification of the RP

• Security screening of the RP

7.3 Implementation Approach

The impact of a second tier of screening would differ depending on the method chosen to implement the RP scheme. This relates back to the purpose of the scheme and the benefits that an RP could expect to receive in comparison to the normal traveler. The methods that could be implemented are:

• A dedicated channel for RP at both authentication and screening

• A dedicated channel for RP authentication with passengers then entering the normal security screening area

• A shared staff search/RP channel with re-use of existing equipment and resources

7.3.1   Dedicated Lane for RP Authentication and Screening.

Authentication of RPs

To explore the impact on operations, the Study Team assumed that biometric technology is being used to conduct identity and membership status checks at the airport. Various options exist to conduct this check – 3 examples are detailed below:

• An automated gate where the passenger is verified as they pass through

• A self-serve or supervised kiosk where the passenger must stop and be verified

- A manned booth where an official rather than the passenger interacts with the system

For these options, implementing an RP scheme would require additional training of personnel to help welcome the passenger and to ensure that issues that arise with the identification and authentication processes or automated gates are resolved. In the case of the automated gate, the need for the 'helper' should be reduced after the initial implementation period – however, there will need to be someone available to assist should there be an issue with the gate or kiosk (e.g. power, technology, network access, etc).

There will also need to be a support network in place for staff in case the technology fails. This includes support teams, a help desk and a reliable system that meets stringent Service Level Agreements for system availability and business continuity. There is a cost associated with this support organisation, which would have to be included in any business case.

In addition to issues with authentication, practical consideration must be given to the training and knowledge new staff working in this area will need to support understanding of what type of passenger they are checking and also the customer expectations of the RP. Staff will need to be aware that it is a dedicated lane and to ensure that only RPs can enter.

Dedicated Screening of Passengers

In theory, the wait time for non-RPs will be reduced as a result of fewer passengers joining the regular security-screening queue, based on the assumption that an RP scheme has new channels and has not simply replaced existing channels.

Management of resources becomes a consideration – would there be a team dedicated solely to the RP lane or would there be a mixed team? This could present personnel, management and union issues and represents an additional area for management attention.

A re-configuration of the departure area to cater for a dedicated RP lane and new technology may be required. This may result in lost retail space as well as the associated income and would require capital expenditure to reconfigure the layout.

Depending on the uptake by RPs and the physical location of the lane, normal passengers could be directed on occasion to the x-ray machines and benefit from less time spent queuing. This is currently what happens in some airports for the 'fast track' facility that is designed to help as an overflow mechanism.

7.3.2   Mixed Approach – Dedicated Authentication and Common Screening

Dedicated RP authentication has been addressed in 7.3.1.

Common Screening

The use of a common screening area for RPs and other passengers would have an impact on the practical operation of the search area. Whilst better technology could lead to improved time for all, there are major implications with mixing RPs with other passengers. A common approach may well lead to an increase in complaints by non-RPs, as RPs would enter the standard security screening area after authentication. In effect, this system would enable RPs to jump to the top of the queue and cause a perceived increase in wait times for non-RPs.

Depending on the volume of RPs this may not be an issue and could be a way to pilot such a scheme. The combination of the types of passenger could also be a benefit to the non-RP if there is new and better technology being made available. This could help throughput for those in the RP lane and help to create greater benefit for all.

7.3.3 Shared Staff/RP lane

Consultation with airports has highlighted the potential to use the staff or crew access point as a way to help introduce the RP scheme. Furthermore, many believe that a Registered Crew/Staff scheme should take priority over and above an RP scheme. The use of the existing staff access points has been highlighted as a way to better utilise existing resources. An example of how this is being turned into a reality is the APEC Business Card traveler, where a cardholder uses the crew/staff route at the border control point.

In addition, by moving staff to a biometric identity and access mechanism, this could prove beneficial with regard to other issues faced by the airport industry around staff security. One issue to consider in the implementation of this option is if differing levels of security are required for RP and staff then confusion would be created for screeners.

The use of such access points for staff members needs to be balanced against the usage of the access control points for transporting stock and other items. Staff often carry stock or other items that take a long time to clear security which add to delays and frustrations for the travelers.

7.4 Other issues for consideration

- **Space;** the need for advanced planning to change the layout at airports should not be underestimated. The timeline from decision to implementation could be lengthy, leading to additional issues and complicated decision making processes. As one airport representative advised, *"The issue at airports is capacity and timelines for development. Change is continuous but plans are set in place years in advance."*[30]. The utilisation of space within an airport is also likely to have quite complex business models associated with it; space is typically at a premium and any move to install new lanes or security checkpoints will have an opportunity cost (e.g. what impact does this have on the non RP experience or lost revenues from retail outlets, etc).

- **Passenger Acceptability;** in France a scheme[31] in Lyon airport to implement security fast track which involves paying 120 euros per annum for shorter queue time was delayed due to the risk of passenger conflict, suggesting that lanes need to be clearly separated. As with business class and premium class lanes, these are often separated although at Brussels airport the fast path there is only separated by retractable pedestrian guideline barriers.

- **Legal Challenges**; in addition to the logistical challenges and impacts at an airport, the legality of implementing such a scheme must be reviewed in each Member State. The ability to offer a differentiated service following a risk assessment (and payment) may not be possible in some countries. One airport is facing legal action for implementing a fast-track scheme based on ticket type i.e. premium passengers only.

---

[30] Interview with Polish Airport Authority, 12th April 2007.

[31] Interview with French Ministry of Interior, 26th April 2007

7.5 Conclusion

Options for the implementation of a two-tier system of passenger screening include:

- A dedicated channel for RP at both authentication and screening

- A dedicated channel for RP authentication with passengers then entering the normal security screening area

- A shared staff search/RP channel with re-use of existing equipment and resources

The impacts of such implementations include:

- Accelerated processing for normal passengers as well as RPs

- Possible loss of retail space and associated revenues in some airports

- Additional capital expenditure to set up the additional facilities

- Potential confusion and conflict between normal passengers and RP's if shared security screening lanes are used

- Additional training for staff to manage both types of passengers and the associated process differences

The extent of these impacts will vary according to the airport and the type of RP implementation used.

Identification of RPs (Questions 8 to 9)

Questions 8 and 9 relate to Identification of Registered Passengers.

(Question 8) How best should data on "Registered Passengers" be stored so that national authorities could access it when controlling departing passengers at airports? How could authorities of one Member State be given rapid and easy access to lists of passengers registered by other Member States, when it recognised their registration? The contractor should analyse whether other data bases (existing or planned) would serve this purpose.

(Question 9) As for the identification of "Registered Passengers" when presenting themselves at airports, what system(s) for identifying travelers for border control purposes (existing or planned) might serve this purpose?

8 (Question 8) How best should data on 'Registered Passengers' be stored so that national authorities could access it when controlling departing passengers at airports? How could authorities of one Member State be given rapid and easy access to lists of passengers registered by other Member States, when it recognised their registration? The contractor should analyse whether other databases (existing or planned) would serve this purpose.

8.1 Introduction

There are a number of options for storing the data of RPs that would allow access by national authorities to enable the control of passengers at departing airports, and also facilitate rapid and easy access to lists of passengers registered by other Member States. This section considers the criteria against which these options might be judged and then applies them to a number of approaches to data storage: centralised, federated and distributed. It then considers the most effective way to facilitate rapid and easy access to passengers registered by other Member States.

8.2 Criteria for assessing data storage approaches to enable passenger control at departure

When storing data and controlling outbound passengers, Member States will require rapid access to RPs' information. A number of approaches can achieve this. Key factors for consideration are shown in the diagram below:[32]
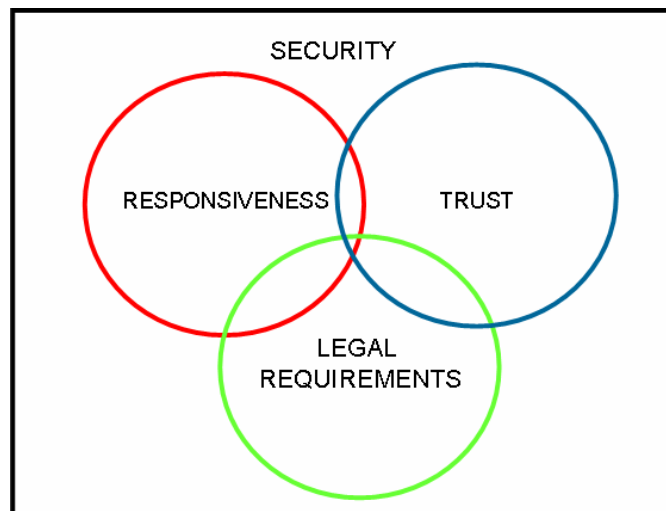

Figure 1. Key Factors for Consideration

- **Responsiveness** – the data necessary to determine the credentials of the passenger must be available quickly at the time the decision needs to be made

- **Trust** – the passengers' personal data and membership entitlement must be trusted by the Member States

---

[32] Other architectural factors such as security, resilience, scalability, and data integrity are critical to any system, but their implementation is not as dependent on the distribution approach adopted.

- **Legal requirements** – compliance with EU-wide and national law, such as the legality of storing RP's personal (including biometric) data, transmitting it abroad, and restricting access to it

8.3 Assessing possible approaches to data storage

At a high level, there are three broad approaches to data storage and access that are outlined in the following subsections:

- **Centralised -** In a centralised approach, the status of RPs and the information needed to authenticate their identities is stored in a central system managed by a single organisation. This is the storage model currently used by a number of European information systems such as SIS, VIS (planned for 2009) and EURODAC.

- **Federated** - In a federated approach, the information on a passenger is stored in the originating Member State's own system. Access to each database would have to be provided and real-time, secure communications would have to be implemented between the Member States' systems. Technically, this is a more challenging solution.

- **Distributed** - In distributed data storage architecture, RP data would be held by the individual RPs, on a membership card or other token (such as an ePassport or mobile phone) that would be presented and read each time the RP wished to use the scheme. This will probably be the most feasible approach, both from technical, legal and scalability point of view. Privium, PEGASE and miSense are good examples of a distributed approach.

The table on the following page assesses each of these approaches against the criteria detailed in 8.2. A more detailed assessment can be found in Appendix G.

	Centralised	Federated	Distributed
Responsiveness	• A single central system might present challenges around response times. • A single central system would be expected to process queries relatively efficiently, the sending and return of these queries internationally could add considerable latency, especially if large volumes of data were to be exchanged. • This risk could be mitigated by implementing national replicas of the central system, similar to the model used by the Schengen Information System (SIS).	• Like a centralised system, a federated system might present challenges around response times, and these challenges might be addressed in part by an appropriate replication strategy. • The data query process is complicated further by the need to ask, "Who holds this data?" to determine the appropriate database before the actual query can be made. Conversely, a Member State's own records will be available locally (intra-state) without the need for replication.	• Although a system using distributed storage will, as a minimum, still require connectivity to a central (or nationally replicated) database for validity checking, the bulk of data retrieval will be performed locally against the user token. • A distributed storage approach is expected to yield the best responsiveness of the three models under discussion.
Trust	• A centralised system could satisfy the trust requirements • Once the data stored on the system is trusted, accurate transmission to National Authority offices can be achieved by ensuring the implementation of secure interfaces and communication links using strong authentication between the central system and the National Authority systems.	• A federated system presents the same type of trust challenges as for a centralised system, with the added complexity that there are many more interfaces to be secured and other security access issues to be resolved.	• A distributed system will have to maintain the integrity of potentially millions of tokens in public circulation. • The existing standards around ePassports have been defined by ICAO with this specific purpose in mind, and include digital signing of the passenger's identity data during the enrollment process, to assure that it cannot subsequently be tampered with without detection. These same standards could be implemented in an RP token.
Legal Regulations	• Each country has individual laws concerning the storage of biometrics in centralised systems that need to be considered. Issues relating to accessing the centralised database from other Member States would need to be addressed.	• This could be mitigated in part if local replication of other Member States' databases was foregone and each state only offered query-response access to their data.	• This approach may run into fewer legal issues than a centralised or federated system since the individual RPs will store their own data, which they have the option to present (or not) at each airport.

8.4 Rapid and Easy access to RP lists

If Member States need rapid and easy access to up-to-date lists of all RPs (including those from other Member States), the data storage model adopted will in part dictate the appropriate method of sharing the current RP data between Member States. Before reviewing the access and ease relating to each approach, the need for accessing full lists of all RPs must be questioned and understood. The reason for challenging this need is that a full (or positive) check does not exist currently when using passports i.e. there is not a list of all passports issued that is checked when crossing the border. Instead, a central revocation list or negative list is checked against e.g. a lost or stolen passport list.

If there is no identification or membership card and a government issued ePassport is used as the membership token, there has to be a quick and easy way to confirm the person is an RP and that their membership status is valid. Otherwise everyone with an ePassport could enter the fast path and think they can use the RP scheme. This has happened with many of the operational schemes that do not include a token. Signage can help this situation but still does not help the RP scheme representative at the airport confirm that the RP membership is valid.

The need for a check against a full list could be to add an extra layer of certainty to the RP and provide comfort for the authorities around the fact that a membership has not been created without the correct authority. The table below details how authorities of one Member State could be given rapid and easy access to lists of passengers registered by other Member States.

	Centralised and Federated *(same for each)*	Distributed
Rapid access	• These storage models mean all Member States can be immediately appraised of new (and revoked) RPs, since they will be checking against a single logical database. Time taken to obtain the data from the central database can be expected to range from a few seconds response for simple queries through to a few minutes for a complex biometric matching query – subject to network connectivity. • If biometric authentication of RPs is required at airports, it is preferable that one-to-one queries are routinely used. One-to-many queries will still need to run in order to de-duplicate RPs at registration, but these can be performed as background tasks. Travelers will need to carry a token that holds at least an ID number that can be used as a reference to the central database.	• The distributed storage model differs from the centralised / federated one in that most of the data required at the airport will be held on the RP token, which can be read locally. This data does not have to be retrieved from another Member State. Such a system can be quick depending on the encryption technologies and computing hardware used • For example, the miSense Trial at Heathrow airport demonstrated the reading and decryption of a traveler's fingerprint from their smartcard in around five seconds. The central database requests that are necessary tend to be restricted to simple queries, such as permission to use the RP lane checks, aiding the responsiveness of the system.
Easy access	• In order to facilitate the exchange of RP data, the query and data formats, interface standards, and security policies should be defined. • Where appropriate, existing standards can be leveraged for this purpose (such as ICAO's guidance on encryption keys contained within 'PKI for Machine Readable Travel Documents'). • Where no standards currently exist, the central system should make available a single set of interfaces for Member State access.	• To ensure recognition between Member States, the data on the token itself should adhere to an agreed standard such as ICAO's Document 9303 for storage of personal data on machine-readable travel documents. As previously discussed for the centralised system, a standardised approach should be adopted to facilitate queries against the central database. • It should be noted that the ability to obtain passenger data locally from a token could help in situations where connectivity to a central system is not consistently available. This reason was a contributing factor to the design of the US Registered Traveler programme - airports in the US cannot guarantee continuous online connectivity to a central system.

8.5 Conclusion

Three approaches to the storage and access to RP data were considered:

- Centralised

- Federated

- Distributed

These approaches were analysed under several headings:

- Responsiveness

- Trust

- Legal Requirements

- Rapid & Easy Access

The conclusion is that a Distributed approach best satisfies the requirements through the utilisation of RP tokens or the use of ePassports.

9 (Question 9) As for the identification of 'Registered Passengers' when presenting themselves at airports, what system(s) for identifying travelers for border control purposes (existing or planned) might serve this purpose?

9.1 Introduction

There are a range of systems for identifying travelers for border control purposes that could be used in the identification of RPs when presenting themselves at airports. Existing systems such as EURODAC and those in development including SIS II, VIS and BMS could be leveraged to help perform key aspects of enrollment and identity checking for an EU-wide system. These systems will be of paramount importance if there is a need for initial checks and continual risk assessments to ensure that once an RP has joined the scheme, their status remains approved.

However, the question is focused on the identification of the RP at the airport and it is assumed to relate to 'point of use' after enrollment and approval to join the scheme. This section examines the options available and identifies the most promising way forward.

9.2 Key stages of identification and authentication

It is important to note that, unless departing from a Schengen area[33], identification of the traveler does not currently occur at the Security checkpoint. The defining check is that the passenger has the correct paperwork to allow them to move into the Security Restricted Area. Therefore, the addition of an identity check (to confirm the passenger is an RP) would be new to the Security checkpoint and represent an additional step. This must be stated as part of the Terms and Conditions at enrollment and made clear to the passenger. This response is based on the assumption that a distributed approach infrastructure is in place, supported by a token scheme

At the security checkpoint, identification and authentication of the RP will be broken down into three key parts:
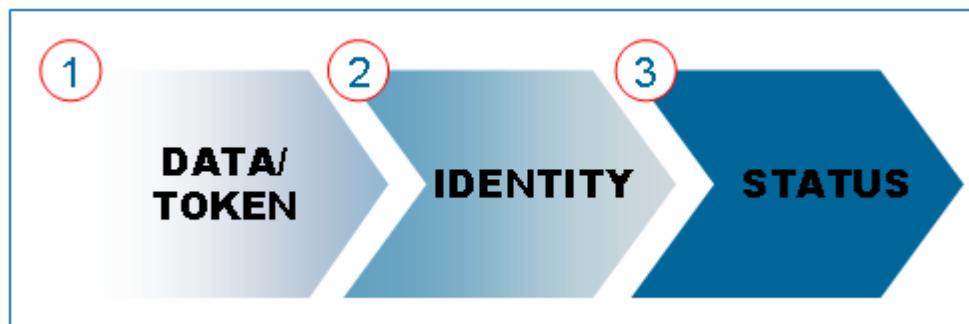
Figure 2. Key Stages at the Security Checkpoint

---

[33] On entry into the restricted area at airports if departing the Schengen area, passenger passports are checked to confirm identify and to ensure the passport is valid and not fraudulent. See Schengen Borders Code Article 7 regarding exit checks. Nonetheless there are no passport checks if taking an intra-Schengen flight, but a check of the eTicket or boarding pass is made to ensure the passenger has a valid pass for the flight, etc.

1. **Data/token Authentication** – is the data on the token still authentic and does it contain the original information?

2. **Identity Authentication** – does the identity on the card match the traveler?

3. **Status Authentication** – is the passenger still registered and allowed to use the automated fast path or has their membership been revoked?

When RPs present themselves at airports, the manner in which they are identified is extremely important. The identification must use something unique to the passenger to ensure that the correct individual is being dealt with. In industries such as financial services, retail and travel, the use of biometric documents is becoming more commonplace. The advent of ePassports, eVisas and biometric entry/exit checks shows clearly that in the travel industry this is the future way to confirm identity. It is this system that is put forward as the most promising method of identifying RPs when presenting themselves at airports.

Other systems (such as use of signatures, Personal Identification Numbers or Passwords) suffer from a lower level of non-repudiation (for example, if a PIN is used to assert identity of person X, person X can simply share it with person Y and they will appear to assert themselves as person X).

9.3 Biometrics

Biometrics is the automated recognition of individuals based on their physiological and/or behavioural characteristics and provides a binding link to the person whose identity was determined at enrollment. Biometric identification technologies can ensure a complete 'chain of trust' throughout the identity lifecycle, binding the process to the correct individual at all times and helping to confirm the uniqueness of that identity.

There are significant benefits to the use of biometric technology to identify passengers in airports in a highly automated way. This is evident from the success of many of the schemes around the world, although there are some practical issues to be considered when using biometrics, which are discussed in the next section. Stakeholders generally supported the use of biometrics to authenticate the identity of the individual. However, some have also noted that other means such as a manual identity verification using a check of the photograph should not automatically be overlooked in favour of more sophisticated biometrics and technologies like iris, facial and fingerprint matching.

9.3.1 Practical considerations when using Biometrics and the adopting a multi-modal approach

In using biometrics, it must be understood that there is no 'ideal' biometric (one that works 100% of the time for 100% of the population). Consideration must be given to a number of factors when analysing the applicability of biometrics:

- **Inclusion** - The ability to include a bigger percent of the population. One of the issues with choosing a single biometric is that for any given biometric there will be a proportion of the target population that will be unable to enroll. For fingerprints there will be people with either missing fingers or poor quality prints. For iris, there will be people who cannot enroll through disability or who have issues using the system following enrollment (see below). If enrollees are given the choice of which biometrics they give, then a bigger proportion of the target population will be catered for.

- **Usability** - In addition to the capture of biometrics at enrollment, the ability to use the biometric equipment at the airport (e.g. in conjunction with an automated gate or a kiosk) needs to be reviewed at the analysis stage of an RP scheme. For example, how would a child reach the height of a fingerprint device or how would a wheel chair user manage to use an iris capture device? As with other self-service devices (e.g. an ATM) there needs to be careful analysis to ensure users can actually use the device(s) with ease.

- **Cultural issues** - There are a number of cultural and religious issues with biometrics. Fingerprints can be associated in people's minds with criminal activity but this view is changing as they become more openly used e.g. with credit cards or payment systems, and by moving away from the traditional use of ink capture to smarter and quicker electronic machines. Iris usage can also be unacceptable to some religions.

- **Perceived hygiene issues** - There are some cultures that have issues with touching objects. In these situations, Iris, face and palm vein may be more suitable as they are biometrics that do not involve touching anything. There is also the operational issue regarding the need to have the biometric devices cleaned on a regular basis.

- **Perceived health issues** - The public needs to be reassured that using something like an iris scan or other biometrics will not impact on their health.

An important and practical consideration when using biometrics is the varying performance levels across modes (industry standards for various modes including face, finger and iris are provided in Appendix F). Consequently, the utilisation of a multi-modal solution is recommended to mitigate the limitations of single mode systems. They are used to overcome the limitations of single mode systems to help:

- Enhance matching performance

- Increase population coverage by reducing failure to enroll rate

- Combat spoofing – it is difficult to spoof multiple traits simultaneously

A multi-modal approach helps to solve the non-universality issue – ensuring that everyone can use the system. There is the additional cost of having more than one type of biometric capture device but with advances in technology and 'Moore's Law'[34] in play, this should increasingly become a marginal debate.

9.4 What systems can be used?

Research has shown there to be a variety of systems available at airports to help with the identification of individuals. In Europe, immigration departments have a key requirement to accurately identify and verify passenger's identity. Many immigration departments are currently using ID cards or passports (and visas) to check identities and confirm the person's right to enter the country or Schengen Area. In general, the review is conducted in three ways:

---

[34] http://www.webopedia.com/TERM/M/Moores_Law.html

- Manual review of the travel document

- Swipe of the passport to check against various national watch lists and European databases e.g. SIS

- Scan of the passport to check the contents of the first generation ePassport chips – to ensure the printed photo on the passport matches the one contained in the chip implanted in the passport – and a check against a watch list at the same time

The USA has introduced the US-VISIT programme for non-US passport holders, which entails capturing biometrics on arrival to help check and verify the identity of the passport holder. The capture process includes capture of two fingerprints and a facial image. In the near future, passengers will be expected to provide 10 fingerprints to help reduce error rates and increase accuracy and compatibility with other systems such as the FBI criminal fingerprints database.

Current RP schemes that exist in Europe and around the world also point to how easily a person's identity can be recorded and used for an RP scheme. The miSense Trial demonstrated the ease of capturing all 13 biometrics for use in risk assessment processes and then for use at the airport. Once approved, biometric information is placed on a token for secure usage at airports. It also allows the customer to chose a preferred biometric and a back-up, in case this preferred biometric is not working or the scheme being used does not have all the biometric capture devices available.

9.5 Using a token

A common data structure and security mechanism needs to be in place and schemes around the world are using tokens in different ways – either containing a reference number to help look up data on the database or to carry all the data within the card itself. In a distributed system, the need for a token containing biometric and biographic information is clear and should be based on ICAO 9303 Machine Readable Travel Documents standards. This approach enables direct compliance with data privacy standards by removing the need for biometrics data exchange: the traveler will be carrying his/her biometrics on the token, and can share it with destination border control agencies.

The use of the second-generation ePassport[35] as the token for carrying biometrics should be assessed as part of the development. This will be rolled out in Europe from 2009 - however, only in 2019 will all nationals from Member States have ePassports. This removes the need to carry membership cards and also uses a standard format that will be the international norm. The security and cost issues related to the issuance of RP cards also means that stakeholders are keen to take advantage of 'trusted documents' and remove the need for any additional token or membership card. From a user perspective, it also saves the user from having several different membership cards to carry.

The use of a token other than the government-issued ePassport or ID card also has certain benefits that appeal to the commercial sector, including the use of the card for other services (at the airport or beyond) for example, as a credit card or loyalty card. As the second generation ePassport is still in its infancy and will take time to rollout it may be that

---

[35] Second generation ePassports contain fingerprints as well as the photo in a microchip inside the passport page.

the membership card is used as an interim token. In addition, by having a membership card, a valid RP can easily be identified. There is less likelihood of passengers believing they have a right to use the RP scheme just because they have a passport, and see other passengers using theirs to gain entry to a faster security process. This can, of course, be mitigated by signage and advertising.

If third country nationals were to participate in RP schemes, then a separate token may have to be issued if their passport is incompatible or if they desire to opt for a membership card. Indeed it could be that any RP (regardless of nationality) is offered the choice of a membership card with additional benefits for which they pay more than if they were to join a scheme and become a member using their ePassport.

In addition to traditional tokens the mass appeal of mobile telephones and other contact or contact-less technology (e.g. credit cards) should be considered to act as the token. This may further complicate the requirements and costs of an RP scheme but should not be ruled out without due consideration.

9.6 Conclusion

Accurate and fast identification and authentication of the RP when presenting themselves at airports is essential to the success of the scheme.

The use of a multi-modal biometrics system (i.e. with the capability to operate on several different biometric types) along with an identity token is strongly recommended as the means to achieve this. This will reduce human error and increase the integrity and credibility of the scheme.

There are many practical considerations to consider when using biometrics, but advances in technology, use of the multi-modal approach and the increased use of biometrics by the public in other aspects of their lives is helping to overcome the issues that may have been faced in the past.

Potential benefits to passengers, airlines and airports (Questions 10 to 12)

Questions 10 to 12 relate to potential benefits to passengers, airlines and airports:

(Question 10) To what extent would the introduction of a "Registered Passenger" scheme at Community level facilitate air transport? In particular, what reductions in delays might typically be expected, and at which types of airports and at what periods of time?

(Question 11) To what extent would the introduction of a "Registered Passenger scheme" at Community level benefit the operations of air carriers and airports and what might the impact on their costs?

(Question 12) How far might common approaches lessen the costs of identifying passengers and maintaining their databases?

10 (Question 10) To what extent would the introduction of a "Registered Passenger" scheme at Community level facilitate air transport? In particular, what reductions in delays might typically be expected, and at which types of airports and at what periods of time?

10.1 Introduction

The aviation industry is under increasing competition from other forms of transport. Rail travel has evolved into a real competitor – with Eurostar services from London to Paris and Brussels and the recent news of the Bullet train from Paris to Strasbourg being examples of this. In the US, road transport is becoming an attractive option with high-yield business travelers now willing to drive five or more hours rather than risk the unpredictability of the airport security experience.[36] Many stakeholders interviewed believed the increase in demand for air travel, combined with the resource constraints in place at airports has transformed air travel from an enjoyable leisure experience to one characterised by continuous checkpoints, queues and delays. One industry representative described this as 'everyone being made to feel like a terrorist'.[37]

This section first looks at current innovations to facilitate air transport and then examines where and when the introduction of RP schemes might have the greatest impact on delays.

In answering this question the definition of an RP scheme is used which deviates from that laid down in the Terms of Reference. Here it is a commercial scheme that offers RPs better customer service (e.g. accelerated checks) rather than exemptions to or lightening of security checks.

10.2 Current innovations to facilitate air transport

To counter increased competition and to help drive demand, airlines, airports and Control Authorities are continually updating and innovating their products and services. Airports are implementing new technology to help move passengers faster through the airport and into the lounges and shopping areas. Some airports also have fast path entrances to security based on ticket type; Brussels Airport and Nice Airport have dedicated lanes, whilst some major airports have dedicated manual fast paths for business and premium class passengers.

Airlines are moving towards online and self-service check-in, with time and convenience becoming the unique selling points. An example of this is a new service called SilverJet[38] from London Luton which advertises a 30 minute check-in before departure time. Some airlines are also moving to charging for priority boarding of the plane, creating additional revenue streams at little extra cost whilst at the same time meeting the differentiation in customer demand.

Control Authorities are putting in place pilots or operational systems to help speed the journey without increasing risk. These are mostly focused on immigration checkpoints and

---

[36] http://businesstravelcoalition.com

[37] Interview with Bruno Marcedo, March 2007

[38] http://www.flysilverjet.com

not security facilitation, as immigration status (in comparison to security status) is seen to be easier to verify. Examples of this include various registered travel programs including P.E.G.A.S.E [39] in France, Sapphire[40] in Asia and eGate[41] in UAE.

In most instances the pilots or programmes involve a partnership approach with key stakeholders coming together to enhance the overall travel experience. IATA's Simplifying Passenger Travel Interest Group is an example of a forum that helps to facilitate this, with the coming together of airlines, airports, Control Authorities and industry suppliers. Other organisations are uniting to help review and improve security – one example of this is ACI and AEA creating the European Strategic Partnership for Aviation Security (ESPAS) where the focus on risk-based security is a key part of their strategy.

RP schemes have the potential to facilitate air transport by increasing customer satisfaction without reducing security or border controls. As one airline representative explained,

"An RP programme will help stimulate tourism and travel and assist Europe as a place to travel to, through and from." [42]

However, it should be noted that an RP scheme will not be suitable for all airports – for example, airports where passenger throughput is relatively light or where waiting times are short. In Europe there are examples of RP schemes that have been piloted or implemented at major airports; for example Privium at Schiphol and the miSense scheme at London Heathrow. Both schemes aim to create a unique customer service offering and help to improve the attractiveness of air travel for frequent users. For example the Privium scheme has 35,000 members with a 94% renewal rate. MiSense results show the most important benefit of an RP scheme would be speed - 86% of passengers stating that a faster journey was their number one priority.

10.3 Reduction in Delays

In the context of this study delays typically occur for the passenger in two key areas:

- Delay during the passenger journey before boarding

- Delay to flights caused by security queues

10.3.1 Delays during the passenger journey before boarding

The key part of this question is related to delays for the passenger in their journey before boarding. Where applicable, an aim of the scheme would be to reduce time spent at security for both the RPs and ordinary passengers. The P.E.G.A.S.E scheme in France has had a very positive impact on the users, confirmed by surveys that Air France has

---

[39] http://www.ier.fr/~/uk/market/access-control/~/uk/focus_on_air-france-is-testing-the-pegase-project/

[40] http://www.saphire.co.id

[41] http://www.dnrd.gov.ae/dnrd/E-Services/E-Gate/Default.htm

[42] Interview with British Airways, 13th March 2007

completed. Air France stated; 'A huge majority of passengers are clearly awaiting such initiatives from airlines, airports and authorities.'[43]

This is of interest to all stakeholders for a number of reasons:

• Travelers do not like queues, inconvenience and uncertainty

• Airports want travelers to spend money in retail outlets and not select other less crowded airports or other forms of travel

• Airlines and airports do not want people moving from air travel to other forms of travel as a result of delays or the increased inconvenience and frustration levels

• Governments want to increase security and also to be seen to be helping the passenger journey despite introducing new regulations. Recently, it has been identified that queues at security screening areas are themselves a security risk due to the high volume of passengers in a single place

RP schemes throughout the world have appealed primarily to frequent travelers who would therefore make up the largest group of RPs. As the majority of these people take flights that depart either early in the morning or late in the evening, it could be argued that the greatest reduction in delays would coincide with those time periods. In addition, as business travel tends to take place between airports in major cities, it could equally be argued that the greatest reduction in delays would be experienced at those locations.

For popular holiday destinations and tourist resorts, there is also an argument for use of automation to help facilitate travel during the seasonal peaks. However, the real issue with this is the practicality of enrollment and associated costs for people that do not travel frequently. This issue could be resolved by using ePassports as the token and remove the need for a secondary enrollment process for a separate membership token. The rollout of 2nd generation ePassports is planned from 2009 onwards.

---

[43] Interview with Air France, 26th April 2007.

US Insights

Bill Connors[44], executive director and chief operating officer of the National Business Travel Association in Washington, D.C., stated 'proper queue management' would prevent security delays among unregistered travelers. At Orlando International, he said that 10% to 12% of flyers belong to Registered Traveler which uses 6% of the airport's checkpoint lanes. *"There are a lot more people going through the Registered Traveler lanes without impacting other lanes,"* Connors said. *"They're disproportionately going through. It's taking more people out of the mix, so non-registered travelers are getting through faster as well. It's easing the burden on everyone else."*

Industry estimates are that once the US RT is rolled out nationally, RT members could represent as much as 30% to 55% of the travelers moving through an airport. This is in part because the programme is expected to be popular among frequent flyers and in part because those frequent flyers make up a disproportionate share of air travelers on any given day. It is not assumed that the figures will be same in Europe. However, it does suggest that such schemes would appeal to a significant portion of travelers.

10.3.2 Delays to flights caused by security screening

Delays to flight departures can be caused by passengers waiting to clear security screening. These can be reduced by the implementation of an RP scheme, which could accelerate security screening for RPs and non RPs. (i.e. through use of advanced RP lane technology as an overflow, or the eventual 'trickle down' of technology to the mainstream security checks).

A challenge for airlines is the move to online check-in, which can occur up to 24 hours before flying. Unlike traditional check-in where it is known that the passenger is in the airport, online check-in means that passengers with only cabin luggage can fail to turn up for a flight and yet the airline has to wait until 10 minutes before departure for the traveler to appear.

Therefore a means to link the journey and the identity at the security checkpoint would also enable airlines to have advance notice of travelers who will make the flight.

10.3.3 Where and when would a Registered Passenger scheme have the greatest impact?

Where an RP scheme should be introduced, and at what operational times, are heavily influenced by the airport operators and customer expectations of the service being offered. The level of reduction in delays will also be dependent on the current performance of the

---

[44] http://www.tmcnet.com/usubmit/2006/04/24/1601728.htm

airport e.g. it could be expected that an effective RP system would have a greater impact on a poor performing airport than a high performing one.

During the consultation, a consistent theme emerged about the type of airport best suited to an RP scheme; namely large hub airports where the volume of passengers is high and the crowding at security has negatively affected the traveler experience. In addition, there appears to be demand for such a scheme from regular business travelers from regional airports or regular travelers for other reasons e.g. the amount of people that have second homes and often travel between locations.

This does not rule out other airports from participating in an RP scheme – for example, there may be small airports that have limited space for security screening areas and at peak times this results in a huge bottleneck of passengers. However, careful consideration would need to be given to the potential costs and benefits for all interested parties (e.g. airports, Control Authorities) prior to proceeding.

In order to meet customer expectations, the operational hours and dates of an RP scheme should, as agreed in consultation with other travelers, match that of the airport. If passengers are paying a fee for fast access then the expectation is set at enrollment. It may be that the airport can introduce manual workarounds should there be the need to reduce the operational hours as a result of funding constraints or technical issues. However, the initial aim should be to match the operational hours that the airport and existing security screening areas support.

As with the US RT programme, a pilot of any future EC RP scheme should include a variety of airports which would allow lessons to be drawn from a range of experiences. A pilot project structured in this way would allow hypotheses to be tested on the most appropriate type and time to introduce and use RP schemes, as well as the scale of improvement that can be expected. During these pilots it might also be useful to check the 'bedding in' time for such schemes if new technology or processes are involved.

Insights from other industries

Insights can be gained from other industries – for example traffic management on toll roads. Automated toll collection lanes process vehicles faster and absorb a higher number of vehicles than standard lanes, as a result all traffic moves through tolls faster because their lines are shorter (even those that are not automated) than before the system was introduced.

This is the same concept used at some supermarkets and retail organisations where different types and locations for check-outs have allowed people that make small purchases to move faster and those doing a large purchase to have assistance and other benefits. The same could be said for the travel industry with a new focus on how to create a positive customer experience at security with helpers for people that need assistance and streamlined lines for people that have little or no luggage and know the process very well.

10.4   Conclusion

An RP scheme could be one of the ways to improve the passenger experience in the face of challenges from increased security levels, growing demand and limited resources. The potential exists for RP schemes to facilitate air transport by creating a more convenient and faster experience at the security checkpoint. Other industries and organisations are

continually looking to improve the customer experience through advances in technology and process; the RP scheme could be a vehicle for such changes in the aviation industry.

RP schemes could facilitate air transport for all passengers, not just RPs – particularly if the infrastructure (including staff, lanes and equipment) is in addition to that provided for normal passengers. As to the type of airport to which the RP scheme is best suited, the consultation with stakeholders suggests that large hub airports with high volumes of passengers and possibly some regional airports with a high percentage of frequent fliers are the most likely candidates.

The key time of day when air transport could be facilitated most effectively by an RP system would be during the peak hours for business and holiday flights – this is typically when most congestion occurs.

The reduction in delays is difficult to estimate as it will vary from airport to airport depending on a number of factors including; type of scheme, quality of implementation, and the scope for improvement.

11 (Question 11) To what extent would the introduction of a "Registered Passenger scheme" at Community level benefit the operations of air carriers and airports and what might be the impact on their costs?

11.1 Introduction

Depending on the type of RP scheme implemented and the business model that underpins it there is the potential for a scheme to have a real impact on the cost base and revenue streams of airlines, airports, and Control Authorities. There are various examples of free, low cost and high cost schemes and schemes that also offer additional incentives alongside speed and convenience.

The impact of an RP scheme on the operational benefits and cost base of the industry depends on how the scheme is funded. The feasibility of various funding streams for RP schemes is discussed earlier in this report (Question 4). Consistent with the conclusion that the most feasible business models are those with RP fees as a key revenue stream, it is assumed for the purposes of the question, that the scheme is funded directly by passengers who pay a fee that covers the cost of enrollment, risk assessment, enhanced technology and the operation of the scheme. In addition, the fee could do more than cover the cost and offer a financial return to those involved in creating and running the scheme. Depending on the business model and aims of the scheme, such a scheme could be profit making – however this needs to be balanced against pricing pressure from consumers.

This section identifies the possible benefits of RP schemes to air carriers, airports and Control Authorities. It examines the cost bases typically associated with RP schemes and provides a case study of the US RT to draw out some of the lessons learned from the introduction of such schemes.

11.2 Airline industry – Airports and Carriers

11.2.1 Airports

There are a number of operational benefits that an RP scheme can realise in an airport:

- **Passenger satisfaction and retention** - Increased passenger satisfaction due to a reduction in queue waiting times and better technology, process and use of staff. RP schemes would also provide quicker and more convenient security screening and more predictable and punctual journeys for their customers.

- **Revenue generation** - Additional throughput of passengers could lead to increased retail income at the airport. The more time the passenger spends waiting for security the less time they are in the retail outlets spending money.

- **Revenue protection** - The introduction of an RP scheme could help to reduce fines for the length of the security queues. It could also enhance the ability of the airport to meet targets and become a more attractive place to fly through.

- **Public Relations -** The implementation of an RP scheme could be seen as a pro-active measure to deal with existing issues at Security. This could lead to positive press and media coverage.

- **Other Benefits -** An RP scheme could be tied to a frequent flyer scheme or help with the verification and de-duplication of boarding passes.

The research has also shown that some airports have good queue times for security and so see little value in investing in an RP scheme. This has been the case in some US airports and reflects the variations in challenges that exist across airports.

11.2.2 Carriers

Feedback on the potential operational benefit for airlines was mixed – however, as can be seen by the involvement of Air France, British Airways, Virgin Atlantic, Cathay Pacific and Emirates in various schemes around the world, there are some benefits. The airlines consulted acknowledged the benefits of RP schemes, but the type of benefit acknowledged varied by interviewee.

Benefits include:

- **Better service** - The frequent flyers (and not necessarily premium class passengers) that are at the heart of the airline industry are the key target customers of any RP scheme. Following enrollment into an RP scheme they would spend less time and suffer less inconvenience at the checkpoints. Theoretically, this would help maintain or increase demand for air travel and go some way to help boost the attractiveness of air travel again. The introduction of an RP scheme could also lead to the continued development of the business flyers and frequent flyers who, given the increased focus on controllable cost and expenditure, will opt to fly using low cost carriers wherever possible. The introduction of a card that gives them a fast-path through security (and maybe immigration and other services) could help to drive competition amongst airlines.

- **Unique selling point** - An airline-sponsored RP scheme could become a unique selling point for the airline and attract business travelers to them. Airlines could, for example, become the marketing front end of the scheme and offer this as a unique benefit for their flyers. This is especially the case where the airline has control or single use of a terminal building and examples of this can be seen in Europe and in the USA.

- **Cost Reduction** - The ability to reduce costs by removing the need for an airline funded fast path for their premium passengers. Some fast path facilities are run on a cost recovery basis where airlines are charged by airports for use of the fast path.

- **Public Relations** - The implementation of an RP scheme could be seen as a pro-active measure to deal with existing delays at Security. This could lead to positive press and media coverage.

Some regarded RP schemes as benefiting only the frequent flyer and premium market. Possible negative effects were also discussed. For example, some airlines may lose customers if the trip is short haul and one of the only reasons passengers buy premium tickets is to use the fast track and avoid a lengthy security delay. As with the variation in airports across Europe, an RP scheme will not be an attractive proposition for all airlines.

11.2.3 Control Authorities

An RP scheme could realise benefits for the Control Authorities; these include:

- **Increased security** – An RP scheme can help provide better technology combined with the certainty that the RPs are not on watch lists at the point of use. In addition, it can enable the more effective use of resources, including the ability to target limited resources at potentially higher risk passengers. A strong identity check could be added to the security checkpoint using biometric features that are significantly more difficult to forge than paper documentation. Increased benefits would also be created if the RP scheme helped to accelerate the way in which the security checks were completed.

- **Rapid and low cost advancement** - It could be agreed that a percentage of the profits from the RP programme be allocated to a central organisation, which is responsible for testing new security screening developments for all.

- **Proactive enhancement of the customer experience** – There are leadership and reputation benefits for Control Authorities, governments and the EC through being seen to be leading the way. This would also show the media that the government and Control Authority were being proactive and assisting passengers.

- **Facilitating the movement of people and goods** - If security processes and infrastructure improve this leads to benefit for the economy overall.

11.3   Costs associated with an RP scheme

The costs incurred by air carriers, airports or Control Authorities will depend on the business model applied. In developing this model two sets of costs will need to be considered:

- Home country costs

- International scheme costs

11.3.1 Home country costs

Home country costs will vary according to the national set-up and infrastructure for the RP scheme in a particular country. For example, it may be that an RP scheme is already in place or alternatively that government capacity for swift security checks is limited.

Cost centres that would need to be considered include (but are not limited to):

- Scheme set-up and legal costs

- Marketing and customer management costs

- Enrollment costs – location, equipment, staff

- Security checking – the ability to complete and approve membership and deal with customer issues such as denial of entry

- Card issuance (note this could also be completed at scheme level but potentially removes the flexibility of having different cards issued by different airlines, airports, etc and adds to difficulties regarding delivery management)

- On the ground - operation of the authentication point and dedicated security search

- Additional services – for example car-parking

- Management of the scheme

- Technology development and support costs

11.3.2 International scheme costs

Additional costs relate to managing and maintaining the international aspects of the scheme:

- Scheme set-up and legal costs

- Design and run of the central card status list and other IT systems needed at international level

- Management of the member states

11.4   Summary of costs

Regardless of the funding mechanism, a clear cost-benefit analysis needs to be completed by organisations that are interested in the introduction of an RP scheme. These could be airports, airlines, government or private industry. It is important to note that some of the financial benefits may be less tangible; for example the ability to estimate the impact of reduced wait time on passengers' willingness to re-use the airport or indeed the increased security that an RP scheme may bring with it.

Alongside the funding of the scheme in terms of set-up and operation, a more complex issue is that of cross-charging. One Control Authority official[45] focused on this by using the following example – hypothetically what happens if only a few RPs signed up for the service (and paid the required fee) in the home country, but RP membership in other Member States is much higher (thousands or hundreds of thousands). In order to provide a full system in both directions, the home country would have to resource the system according to this demand. However, in this case, the fee revenue received by the home country authorities would be disproportionately low.

It is clear that the costs of such a scheme and the method of funding will need to be reviewed in detail. The ability to charge for a premium service and avoid any legal challenges must be assessed early in the planning and assessment phase for each of the participating Member States.

11.5   Learning from existing schemes

11.5.1 Demand

Due to the varied nature of schemes in operation it is difficult to draw conclusions on the costs and benefits that have been realised so far. This is in part due to the variation in the purpose of the schemes and in part due to the commercially sensitive nature of such information. Instead, the growth of schemes around the world shows that demand does exist for RP schemes and their associated services.

---

[45] Interview with OMAS Malta, 18th April 2007

Various schemes around the world show passengers are willing to pay for a quicker and better service. For example, there are 400,000 people registered in the Dubai eGate scheme and passengers pay $40 per year. Over 40,000 people are enrolled in the Privium Scheme paying between €80 to €120 Euros per annum. In the UK there is clear demand for a service that helps reduce queuing time (albeit at border control) with approximately 100,000 people enrolled in the IRIS scheme. There is no direct charge for this service and the government funds it.

11.5.2 The US Registered Traveler Programme

"*Essentially, the RT programme is a system based on privileges that, if fully operational, would offer a streamlined security experience for applicants who pay a fee and meet both TSA and the Service Provider's eligibility requirements*" [46] *Kip Hawley, Assistant Secretary, United States Transportation Security Administration*

The US RT Programme started in 2004 to explore technology, customer reaction, and collaboration in the development of a comprehensive, nationwide RT programme. A brief history of the scheme is detailed below, together with a summary of the benefits, challenges and lessons learned.

Brief History

Following the successful piloting of the scheme at five airports throughout the US, the US RT programme is growing rapidly. It is the result of a public-private partnership, where industry and government came together through a RT Interoperability Consortium (RTIC). It is the only security-focused scheme in the world and so merits further analysis.

Initially, the scheme acted as part of a layered approach to US aviation security. However, it has swiftly moved towards a commercially led enterprise without any reduction in security levels.

"Given the extraordinary public interest in the programme, and the appealing logic behind it, TSA was willing to give wide latitude to private sector entrepreneurs, airlines and airports if they were able to construct an RT (Registered Traveler) programme that did not increase risk to the system." Kip Hawley

The benefits of the scheme

It is funded by the applicant and managed at a local level by the airport. In return for payment of $100 per annum, the US Registered Traveler receives a membership card that entitles them to use a dedicated security screening lane. They receive the same level of security but will normally have less time to wait for the actual search to commence and typically have more staff available to assist the checking process. In some cases, new technology is already being introduced to screen shoes at the time of entering the RT lane.[47]

---

[46] Statement of Kip Hawley before the United States House of Representatives Committee on Homeland Security, 31st July 2007

[47] For more information on the US RT programme go to http://www.tsa.gov/what_we_do/rt/index.shtm

The airport may outsource the scheme operations to a private company, but they remain at the heart of the decision, which is critical, as they own the infrastructure. The TSA is the approving body and also responsible for the background checking/approval mechanism and associated liabilities. They receive part of the application fee to cover their costs

In terms of facilitation, the level of security has not been reduced but the wait times for going through security have been reduced and this is considered to be the main advantage.

Challenges to the scheme

It should be noted that in some quarters the benefits of the US RT scheme are being questioned and challenged. A key question raised concerns how an RP scheme enhances security. This is a potential legacy from the initial aims and expectations that were set at the outset of the American scheme. Indeed one airline industry representative noted,

"We should simply focus on making sure that no passengers, whatever their profile, bring weapons or explosives onto our jetliners." [48]

The US Air Transport Association, the primary trade association for U.S. air carriers, asked the airports not to participate in this programme as it perceives the scheme to be a waste of resources that would not bring a level of benefit commensurate with the cost.[49] There are varied views on the scheme - initially the carriers were strong advocates of the RT idea, but since then the ATA has moved to argue against the scheme as the initial benefits (e.g. less security for 'trusted' passengers) have not materialised.

Lack of awareness is also a problem for the RT programme. This is backed up by a survey[50] conducted in the US where almost two-thirds (61%) of surveyed passengers were unaware of the programme. However, even after reading a description of the programme, 83% were not interested in enrolling, despite the programme's goal of enabling passengers to move quickly through security checkpoints. At the same time, survey respondents said their biggest airport security-related complaint - by a wide margin - was long queues at airports, with more than half (54%) citing it as their top concern. Cost appeared to be only a minor issue. However, if their employers paid the fee, 36% said they would enroll, or would consider enrolling in the programme, and 70% of frequent travelers (those who travel once a month or more) would enroll or consider enrolling.

Lessons learned

There are many valuable lessons that can be learned from the US model, not least of which is the importance of creating a forum to agree interoperability standards. The RT programme used pilots to test the attractiveness and viability of such a scheme. There are some notable and obvious differences between the American scheme and any proposed European scheme. As the answer to Question 2 explained, each of the 27 European countries has differing security, cultures, politics, legal and decision-making apparatus.

---

[48] http://www.aclu.org/privacy/gen/26500res20060817.html

[49] [4] Matthew L. Wald, "Airline Group Asks Airports to Boycott Tests of a Way to Speed Security," *New York Times*, June 8, 2006, online at http://select.nytimes.com/gst/abstract.html?res=FB0E17FD3E550C7B8CDDAF0894DE404482

[50] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemId=973

There are also many different government rules regarding equality and privacy compared to the US. Finally, unlike European airports, there are very few American airports that have separate lines for different types of ticket e.g. first and business class.

In summary, the US RT programme may be a useful reference for a European scheme, but it should not be the only reference point used – there are many European RP schemes currently in operation that should also be referenced and involved as and when a pan-European RP scheme is initiated.

11.6   Conclusion

Benefits to airports include:

- Passenger satisfaction and retention

- Revenue generation

- Revenue protection

- Positive PR

- Other Benefits including frequent flier programme tie-in

Benefits to carriers include

- Better service

- Unique selling point

- Cost reduction

- Positive PR

However, it should be noted that RP schemes will not be applicable to every passenger, air carrier, airport or Control Authority. Amongst some of the Control Authorities and airports interviewed there was a lack of appetite for change and innovation, and a lack of demand to alter security screening processes. Equally, the US RT programme has experienced a mixed reaction in the US, from organisations and passengers alike.

The costs associated with an RP scheme for air carriers, airports and Control Authorities vary according to the business model used. There is a range of cost centres that need to be considered in the development of such a model that include home country costs and international costs.

12 (Question 12) How far might common approaches lessen the costs of identifying passengers and maintaining their databases?

12.1 Introduction

The costs associated with identifying RPs and managing their data can be attributed to two distinct groups of business processes:

- **Identity Assurance -** which includes the initial enrollment of the RP, subsequent verifications and renewals

- **Status Management** - which maintains the permissions each RP has to use the scheme in each country

Within each business process, varying degrees of commonality could be pursued, from independent, country-by-country standalone operations to a shared-service RP scheme. The diagram below illustrates this:
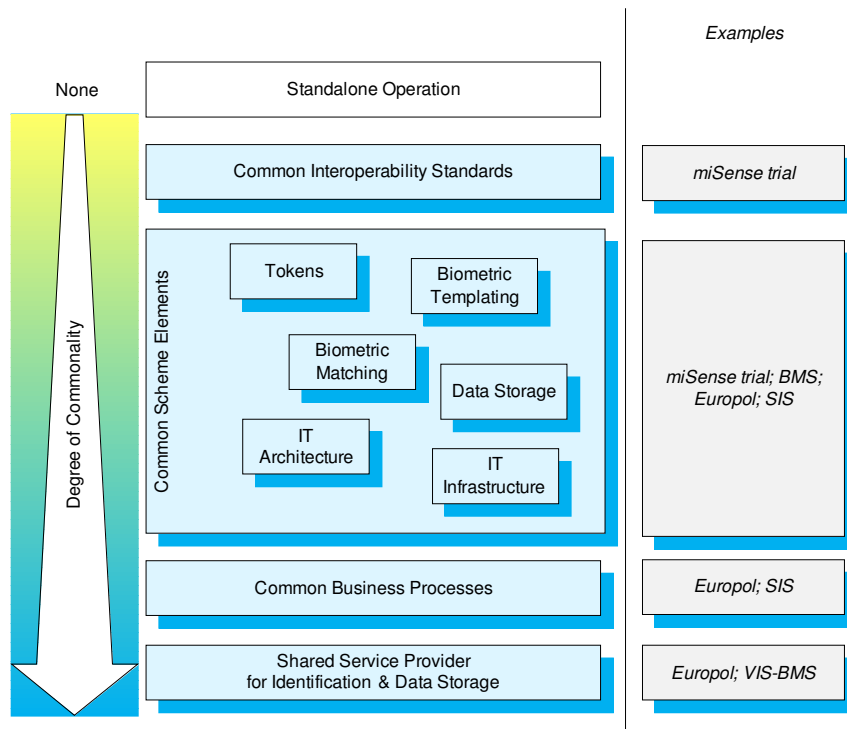
Figure 3. Adopting a Common Approach to Identifying RPs and Maintaining their Data

There are a number of obvious challenges to commonality, such as National Security protocols, confidentiality and data protection laws.

The various stages of commonality introduced in Figure 3 are described below.

12.1.1 Common Standards

Common standards are critical to reducing the costs of operation of a European RP scheme. For instance, the data captured (and its format, structure and quality) at initial

enrollment is key to the simplicity of subsequent interactions with the system. Consider the inverse case, in which no common standards were implemented. RPs enrolled in Spain might have their biographic data stored in a different structure to that of RPs enrolled in the Netherlands, which would thus necessitate translation between the two formats whenever the records had to be compared.

12.1.2 Common Scheme Elements

There are also ways to combine elements to cut costs. For instance:

It is likely that some kind of token (as simple as a reference number, or as complex as a biometric smartcard) will be required to enable an RP scheme. Standardising these tokens (at least their functional and technical capabilities, if not their visual design) can be expected to bring significant cost savings through simplicity of development, implementation, and support. For example, ICAO's standard for machine-readable travel documents could be used to create a common biographic and biometric RP token, as implemented in the 2007 miSense trial at Heathrow airport. A standard token will be available internationally in the form of an ePassport carrying biometrics, but this will not be widely distributed for the next five to ten years.

If biometrics are implemented, common biometric templates and matching algorithms will simplify development work and may result in reduced license fees from the vendor(s). It is worth noting that capturing the 'core 13' biometrics (face image, 10 fingerprints, 2 iris images) would aid the compatibility of an RP scheme with external schemes and systems, and help future-proof the enrollments to some extent.

The enrollment process will generate a (relatively small) quantity of data per passenger; the scheme will also generate small amounts of data that need to be stored whenever an RP interacts with it. Despite the relatively small size of the data to be stored, the total storage capacity required is likely to be significant across the EU due to the anticipated volumes of RPs. Cost efficiencies could clearly be made by offering a common data store to all participating Member States, although it is recognised there may be data privacy and security issues.

A common IT architecture could simplify development and operation of a European RP scheme. Such architecture could include shared applications (e.g. a shared enrollment tool that could be customised for each Member State), common services for tasks such as data insertion and modification, or shared security architecture. Given that the IT architecture is likely to be complex for such an RP scheme, this area has great potential to reduce costs.

A common IT Infrastructure could be implemented across different Member States, providing facilities such as a shared Virtual Private Network, or shared application server hosting. The impact of this on the cost of a European RP scheme is difficult to ascertain at this stage; however, it is an area worth investigating further.

In addition to the above, a common RP status list could also be included as a standard service that is signed-up to by schemes – in a similar way to the financial service model for VISA or MasterCard. This could be provided by a single organisation and help to gain more efficiency as more schemes opt to join.

12.1.3 Standardising Business Processes

The need for consistent business processes across Member States could help reduce both system development and operational costs. Since the majority of business processes are likely to be common within an RP scheme, such as 'token issue and distribution', and 'biometrics capture', they can be designed once, customised for each country if required, and then potentially supported centrally.

12.1.4 Shared Service

At the far end of the scale is the option of a Shared Service Provider; this would see a single organisation taking care of (for example) all ID verification for the RP scheme, working in conjunction with the relevant local authorities.

This function could include not only the development and running of IT systems but also management of the business, for example HR and finance, and customer related activities such as help-desk, single customer account and the web site.

12.2   Analysis of efficiency

The next logical step is to consider each high-level business process in turn, highlighting where each stage of commonality might yield the best improvements.

The tables below include some of the key business processes within Identity Assurance and Status management. These are not intended to be exhaustive, but rather to encompass the main areas. Areas with significant opportunity for cost reductions through commonality are indicated by tick-marks (✓); areas that could be made common if desired but where the cost reductions are less immediately obvious are marked with tildes (~).

	Common Interoperability Standards	Common Scheme Elements						Common Business Processes	Shared Service Provider
		Tokens	Biometric Templates	Biometric Matching	Data Storage	IT Architecture	IT Infrastructure		
Initial ID Enrolment	✓	✓	✓	✓	✓	✓	~	✓	~
Token Issue, Reissue & Renewal	✓	✓				✓	~	✓	~
ID Verification (Home & Host Country)	✓	✓	✓	✓		✓	~	✓	✓

Figure 4. Identity Management

	Common Interoperability Standards	Common Scheme Elements						Common Business Processes	Shared Service Provider
		Tokens	Biometric Templates	Biometric Matching	Data Storage	IT Architecture	IT Infrastructure		
Initial Background Checking (Home & Host Country)	✓				✓	✓	~	✓	
Subsequent Background Checking (Home & Host Country)	✓				✓	✓	~	✓	
Exceptional Changes	✓				✓	✓	~	✓	

Figure 5. Status Management

12.3 Cost Savings by Leveraging Other EC Systems

It is the European Commission's IT strategy to use Services Oriented Architectures (SOA) for large scale IT systems. This enables the Commission to provide centrally re-usable business functionality to the Member States in all possible domains according to the latest IT standards.

This allows for greater efficiency by re-using existing functionality and systems for Member States. Examples of systems that could be utilised include BMS/VIS and SIS

As part of any future RP scheme, the central card status list could also be leveraged or re-used to help create an international watch list system that has more than a card status and more than existing watch lists entries such as alerts and arrest warrants. However, this would need to be reviewed in detail and the scope carefully managed – especially with the fact that an RP scheme may not be European-wide initially and that other systems may be planned for this purpose.

12.4 Conclusion

Common approaches can lessen the costs of RP schemes through the adoption of:

- Common standards

- Common scheme elements such as:

    o Standard tokens

    o Common biometric templates and matching algorithms

    o Shared data storage

    o Common IT architecture and infrastructure

- Standard business processes including shared services

- Leverage of existing EC systems

Appendices

- Appendix A – List of Stakeholders

- Appendix B – Biometric Standards

- Appendix C – RP Schemes around the World

- Appendix D – Glossary

- Appendix E – Examples of New Technology

- Appendix F – Biometric Modes

- Appendix G – Approaches to data storage

- Appendix H – Report methodology

Appendix A – List of Stakeholders

The table below shows the stakeholders that were consulted as part of the Study:

#	Stakeholder	Name
1	IATA	Georgina Graham
2	IACA	Luc Geens
3	AEA	Nathalie Herbelles
4	ACI	Bruno Macedo
5	ERAA	Nick Mowers
6	Poland – LOT	LOT Polish Airlines
7	Poland – Government	Maciej Urbanski, Adam Borkowski
8	Poland – Warsaw Airport	Zbigniew Orlowski, Robert Moscicki
9	Germany – Lufthansa	Peter Andres, Iris Leinhart, Christian Leininger
10	Germany – Ministry of Interior	Dr. Jessica Daebritz, Dr. Steffen Richter
11	Germany – Fraport	Martin Bulow, P. Kriegbaum, D. Naumann, K. Wendler
12	Malta – Airline	Mario Bugeja
13	Malta – Gov	Mario Bugeja (OMAS), Davina Spiteri (OMAS), Alphonse Cauchi (Air Malta)
14	Malta – Airport	Mario Cuomo
15	UK – BA	Michael Cavanagh, Jim Forster
16	UK – VAA	Nina Mitchell, Andy Blackwell, Liz Brackley
17	UK – Gov (DfT)	John Parkinson, Richard Orrin
18	UK – Gov (Home Office CT)	David Barofka
19	UK – BAA	Tom Hardimann, Ian Hutchinson
20	Belgium – Gov	Frank Durinkcx
21	Belgium – Airport	Kathleen Vereecken, Dirk Hoornaert, Luc Heynderickx
22	Spain – Government contractor	Esther Nistal Cabañas
23	Spain – Madrid Airport	Ignacio Lopez
24	Ireland – Ministry of Transport	Ethna Brogan & Kevin Doyle
25	Ireland – DAA	Eleanor Travers, Rowan Fogarty, John Reidy (SAA)
26	Ireland – Aer Lingus	Mark Dunphy
27	Ireland – Ryanair	David O'Brien, Carol Sharkey
28	UK Border & Immigration Agency	Graeme Kyle, Alan Craig, John Muir, Glen Wimbury
29	EC DG JLS	Elfa Kere
30	French Airport (ADP)	Baudouin delescluse
31	French Government	Renaud BERNARD, Bernard DELIAS
32	Privium - Dartagnan Biometric Solutions (full subsidiary of Schiphol Airport)	Frits Bosch (CEO) Nanne Onland (Dir. Aviation)

Appendix B – Biometric Standards

Biometrics are heavily governed by standards. Appendix B details some of the key standards that exist within the industry.

BioAPI

The BioAPI specification is one of a set of International Standards produced jointly by the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC) under their Joint Technical Committee 1 (JTC1), Subcommittee SC37 Biometrics. The Standard was based on work done by the BioAPI Consortium, which was called BioAPI 1.0 and BioAPI 1.1. The first international version was therefore called BioAPI 2.0. A subsequent international version of BioAPI containing extensions of the user interface-related features and other enhancements is BioAPI 2.1.

The purpose of the BioAPI specification is to define an architecture and all necessary interfaces (using C programming language specifications) to allow biometric applications (perhaps distributed across a network) to be integrated from modules provided by different vendors.

The ability for system integrators to produce complete systems using components from multiple vendors is essential in the rapidly changing technology of biometrics. It gives flexibility in the provision of modules, avoids vendor lock-in, and provides a degree of future-proofing as the best available biometrics technologies change. The modules being integrated may be software components containing capture devices, such as fingerprint readers, cameras for face recognition, iris scanners, signature recognition devices, vascular imaging systems, etc. or modules that provide support for image processing of biometric data, feature extraction (a form of compression that is specific to a given biometric technology and allows direct matching of the compressed formats - for example, the relative distances on the face between eyes, nose, mouth, or the number of ridges between identifiable ridge endings or ridge bifurcations on a fingerprint).

In addition, modules that provide archiving and retrieval of biometric records to support matching or searching for a match are also a recognised part of the BioAPI architecture.

CBEFF

BioAPI-compliant devices produce biometric data that is embedded in the biometric data block within a CBEFF record.

Image Formats

For face and fingerprint images the ANSI INCITS-385 and INCITS-381 standards are relevant. These allow for a range of compression algorithms including JPEG and JPEG2000 for face, and WSQ, JPEG, JPEG2000, and PNG for fingerprint images. While all of these compression alternatives are supported, accuracy testing has shown better results when WSQ is used for finger, and JPEG2000 for face, and these are the compression algorithms used by default.

INCITS-379 is the relevant standard format for iris images.

The ISO image interchange standards, standardised by JTC1/SC37 in 2005 and 2006 are very similar to the earlier INCITS standards.

The International Civil Aviation Organisation (ICAO) has taken early versions of the SC37 interchange formats and incorporated them into its own Logical Data Structure (LDS) format for use in travel documents. Support for these ICAO specific formats is being built in 1H05 as part of its ePassport offering set.

In addition, the ANSI-NIST ITL-2000 format is supported, and EFTS and Interpol implementations of it. These also allow WSQ-compressed fingers and JPEG-compressed images to be stored within a record. EFTS and ITL-2000 are discussed further in the section below.

There is also support for traditional 'lossless' image formats such as raw images and Windows bitmap (BMP) image formats. These may be needed where image archives exist before the standards were agreed, or where legacy device interfaces provide images as output.

EFTS

In order to exchange biometric data between different systems, biometric data interchange formats are required. A well-established standard for the interchange of forensic quality biometrics is the ANSI/NIST data format standard for the interchange of fingerprint, facial, and scar mark and tattoo information (ANSI/NIST-ITL 1-2000). The specification is open and flexible, providing many optional fields and allowing for user-defined records.

The U.S. Department of Justice has defined an implementation of this standard, for use by law-enforcement agencies. This implementation, the Electronic Fingerprint Transmission Specification (EFTS), is used worldwide for exchanging and storing rolled and flat fingerprint images. It is used not only by law-enforcement agencies, but also in many civilian identity systems.

With EFTS, images can be compressed and decompressed using the Wavelet Scalar Quantisation Specification (WSQ) or JPEG2000 formats. The default compression ratio is 15:1, but other compression ratios can be configured as required. Images may also be stored in WSQ compressed format. When using fingerprint images captured from sensors not based on optical sensing technology, alternative compression ratios may be recommended, in order to maintain image quality and matching accuracy. Facial images and other non-fingerprint images are compressed using the JPEG standard.

Template Formats

Standardised template formats allow the exchange of biometric data in a non-proprietary format. Existing ANSI-INCITS standardised template formats are supported, and will add support for the corresponding ISO formats as they are finalised in 2005 and 2006. Where a specific vendor does not currently support a standardised template format, legacy proprietary formats are used.

These template formats define the structure, content, and semantics of a data format for a number of specific biometric technologies.

Additional template formats are being defined by the INCITS and SC37 bodies, and these include finger pattern skeletal data, signature/sign time series data, signature/sign processed dynamic data, and hand geometry silhouette.

ANSI INCITS 378

This is the ANSI INCITS 378 minutiae-based interchange format. A number of different vendor-proprietary algorithms are supported by the system to create and match records in this format. This includes leading algorithms, as benchmarked by the Fingerprint Vendor Technology Evaluation (FpVTE03).

Recent performance testing of the ANSI INCITS 378 implementations has shown that the best results were achieved when the same algorithm that is used for enrollment record creation is used for verification record creation and matching. Where different algorithms are used for record creation and matching, accuracy needs to be derived through testing and appropriate matching thresholds applied dependent on the combination used.

ANSI INCITS 377

The ANSI INCITS 377 pattern-based interchange format is also present. The preferred algorithm is from Bioscrypt, the leading pattern-based vendor, as independently benchmarked in the Fingerprint Vendor Competition 2004 (FVC2004). A consortium of biometric experts led by the University of Bologna, Italy conducted this accuracy test.

ANSI INCITS 377 defines how a raw image is cropped and down-sampled, before being further transformed to produce the pattern interchange format. This down-sampling makes it suitable for use with a wide range of different fingerprint sensors with resolutions as low as 250DPI. The system supports a selection of additional single-finger readers that are suitable for use in conjunction with this standard and pattern-based matching.

The pros and cons of images vs. templates

Biometric matching algorithms come in two flavours: those that operate directly on images and those that operate on templates generated from the images. The majority of algorithms operate on templates.

Biometric templates are generated from enrollment images. The choice between open interoperable template formats or closed proprietary formats is dependent on the later uses of these templates. This applies mainly to fingerprints. Open templates allow compatibility with other systems and algorithms, without re-generating new templates, but some accuracy is lost due to the lack of proprietary representations. The images may be archived, while the templates should be entered into a live comparison system, used for watch-list and background searching.

ISO/IEC 19794

ISO/IEC 19794 is an international multi-part standard for all mainstream biometrics. The ISO/IEC 19794 series of standards cover the science of using biological properties to identify individuals (for example, the recording of fingerprints, iris scans and facial recognition that is set to become a part of everyday life). ISO/IEC 19794 applies to access control and identification systems, (e.g. information stored on smart cards or other recognition tools, as well as the storage of biometric identification data in corporate databases). The ISO/IEC 19794 standards are applicable to all identity management systems including:

- Identity document delivery and access management systems – such as border controls, corporate identity and access cards

- Forensic identification – to identify casualties or suspects at the scene of a crime

- Citizens' rights – including voting, national health, unemployment benefits, driving licences

- Privileges associated with a particular employment category – including access to highly secure areas such as ports, airports, military establishments, company buildings, information systems

- Access to services – including banking services, financial services, and online purchases

The issue with these standards is that they are by definition lowest common denominator. Proprietary formats and their associated algorithms give superior performance, but at the costs of vendor lock-in. It is usually not possible to convert from one format to the other. This is why it is important to keep the original images even when dealing with templates

Appendix C – RP/Traveler schemes

Name	Location	Enrollment	Cost	Method	Purpose	Available to
NEXUS	USA/Canada	US and Canada government check	$80	Card and Iris	Pre-arrival processing for USA / Canada - Air, Land and Sea	Canadian/US Citizens and permanent residents only
APEC Business Travel Card (ABTC)	Asia – Pacific Economic Council	Each country has to review and approve usage	$100 for 3 years	Manual inspection against card photo and person	Dedicated Entry and exit	APEC citizens
International Registered Traveler	USA/ Holland	Little information is publicly available about this scheme apart from a press announcement in early 2005.But it is believed to involve a common enrollment location for American and Dutch officials but two separate systems and schemes.				
IACS – Immigration Automated Clearance System	Singapore	Biometrics captured at passport enrollment	Free with Passport	Passport/ fingerprint on a central DB	Arrival	Singapore citizens
Express Entry	Israel	Card/hand Geometry	$25	Hand geometry and card	Arrival	Israeli Nationals only
Automated Passenger Clearance System (eChannel)	Hong Kong	Use National ID cards	Free with National ID card	Check against thumbprint (on the card)	Arrivals and departures	National ID card holders
SmartGate	Australia	Part of passport process	Free	ePassport/ Facial match	Arrival	Australian ePassport holders
eGate	Dubai	Government checks conducted at enrollment	AED150 (£20)	Smart card/RFID issued, Data held centrally	Entry and Exit Credit card use	Anyone Who has legal right to enter the country
Privium	Holland	Government	€99 - €119	Check against Iris (on the card)	End to end immigration and other perks	EEA and Swiss
Saphire	Indonesia	Government	$200	Check against Iris (on the card)	End to end immigration & other perks	Citizens of Indonesia
CanPASS	Canada	CBSA	CAN$50 pa	1:many check against Iris	Canadian Immigration and customs on arrival	Canadian/US Citizens and permanent residents only
IRIS	UK	UK Immigration Service	Free	1: many check against Iris	Arrival	EEA nationals and frequent travelers
miSense Trial	UK	UK Immigration Service	Free for Trial	Check against fingerprint and card, and central card list	End to end and international	EEA nationals and frequent travelers
Pegase Trial	France	Air France and PAF	Free for Trial	Card/fingerprint	Immigration	EU members and Switzerland
Registered Traveler	USA	TSA but delegate to approved local service providers	$100 pa	Match v card And central card list	Entry to security only	US citizens only

Appendix D – Glossary

Glossary	
ABTC	APEC Business Travel Card
ACI	Airports Council International
AEA	Association of European Airlines
ATS	Automated Targeting System
APEC	Asia-Pacific Economic Co-operation
DG TREN	Directorate-General Transport and Energy
ECAC	European Civil Aviation Conference
ERAA	European Regions Airlines Association
ICAO	International Civilian Aviation Authority
ID	Identity
ITT	Invitation to Tender
EC	European Commission
EEA	European Economic Area
FAR	False Accept Rate
FAST	Future Attribute Screening Technology
FRR	False Reject Rate
FTE	Failure to Enroll/Failure to Acquire
IATA	International Air Transport Association
IACA	International Air Carrier Association
LPR	Lawful (also known as Legal) Permanent Residents
NASP	National Aviation Security Plan
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PNC	Police National Computer
RP	RP
RT	Registered Traveler
SIS / SIS II	Schengen Information System / version II
SPOT	Screening of Passengers by Observation Technique
STA	Security Threat Assessment
TSA	Transportation Security Administration
UK	United Kingdom
US/USA	United States/United States of America
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
VIS	Visa Information System

Glossary	
WTMD	Walk Through Metal Detector

Appendix E – Examples of New technology

Backscatter Technology

In the USA, operational testing of backscatter technology is now underway at Phoenix Sky Harbor International Airport. This will be used in random screening and on a voluntary basis as an alternative to a random search. TSA plans to expand the backscatter pilot later this year to two other airports (John F. Kennedy airport and Los Angeles).

Backscatter will be able to detect non-metallic devices and objects, as well as weapons or other harmful objects that a passenger may be carrying on his or her person. The Backscatter is a voluntary option for passengers undergoing random screening as an alternative to the physical pat down procedures currently conducted by Transportation Security Officers at the security screening checkpoint. This technology has also been tested at BAA London Heathrow in 2003.

Millimeter Wave Technology

Millimeter Wave Technology, a form of body-imaging technology, uses non-ionising electromagnetic waves to generate an image based on the energy reflected from the body. This technology changes the way searches are conducted and potentially will remove the need for a WTMD <u>and</u> a random search. To use this technology, the passenger stands still and the scan revolves around them – giving the ability to reduce the need for random searches by integrating this in the primary search. The actual scan time may take longer for passengers when compared to the current process but also this technology allows for the passenger to retain jacket and coat. The images generated through millimetre wave are lower-resolution than that of x-ray backscatter, and as a result, privacy may be less of a concern for the travelling public.

In the US, the TSA plans to partner with the U.S Coast Guard and a major city ferry to use tripod-mounted passive millimetre-wave sensor systems, which are designed to detect explosives, including IEDs, concealed on individuals. During the pilot, passengers will move through terminal turnstiles at their normal pace while being screened. Passengers will not be asked to stand in place, nor will they even need to break stride.

Explosive Trace Detection Portals

Explosive trace detection portals are machines that blow puffs of air on a traveler, which it then analyses for trace amounts of explosives. These are now being trialled in airports and in some cases included as an additional part of the US RT scheme before going through traditional security devices such as WTMD.

Other Technologies

Other innovations include shoe scanning technology, baggage checking and walk-through detectors.

The ability to carry out shoe security checks whilst the passenger is still wearing them has been approved by the TSA for use in the USA and is in operation in some of the US RT schemes. This has the obvious advantage that the RPs do not need to remove their shoes and also that the security lane is not slowed by people removing shoes or putting them back on again. In addition, some airports have now staggered the process by installing additional shoe checking machines after the WTMD and cabin baggage search area.

The ShoeScanner portion of the GE Secure Registered Traveler kiosk has TSA approval to detect explosives but not metal weapons. RT members with metal in their shoes still had to remove them to go through security but this highlights how advances in technology will continue to evolve to help the traveler and security.

To avoid laptops and other items being taken out of bags, which is an inconvenience faced by travelers, another innovation is to bring versions of the EDS (hold baggage checking technology) to also check cabin luggage. BAA are trialling this technology in Glasgow Airport through the use of a Smiths HI-SCAN 6040 aTiX system.[51] This is an x-ray inspection system that automatically detects explosives in cabin baggage. In addition to keeping laptops in the bag it will also alert security officers to the presence of liquids in a bag.

To help increase the efficiency of the required random search and reduce the management of, and stress on, the security staff, new Walk-Through Metal Detectors are also being trailed. BAA are trialing Ceia[52] detectors that help the screener by highlighting the part of the body that needs to be searched in order to minimise the effort and time required for the random check. This also helps the security personnel by automatically counting the required percentage of people that need random checks – helping to focus the resource on the security check rather than on the statistics to ensure they meet regulatory targets.

The need to advance and combine technologies to help security is on-going and one example of this is a trial that attempted to combine the questions used in the human profiling technique with biometric sensing. Tested at airport security checkpoints in Knoxville, Tenn., passengers were selected to be subjected to a sensor that monitors physical responses while answering questions on a computer touch screen about their travel plans and other matters.

---

[51] http://www.smiths-group.com/page.aspx?pointerid=E0E038A5CAA74EBD98DC54036E66B33C

[52] http://www.ceia.net

Appendix F – Biometric modes

Different biometric types have very different performance characteristics. This is evidenced in the table below, which shows the 'State-of-the-art' error rates that are possible for various biometric types.

Biometric	Test	Test Parameter	FRR	FAR
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
Face	FRVT [2002]	Outdoor/Indoor	10%	1%
Iris	ICE [2006]	Single-eye camera	1.3%	0.01%

Figure 6. Error Rates

The pros and cons of finger, face and iris as biometrics

In the following sections, the biometric modalities of face, finger, and iris are examined. All biometrics have varying levels of security, acceptability and cost. Selection of a biometric technology must take into account the requirements of the specific application. The table below provides a summary of the characteristics of biometric technologies currently in use.

	Security	Acceptability[1]	Cost	Suitable applications
Face	Medium low	Medium high	Medium	Watch-list scanning, verification
Fingerprint	Medium High	Medium	Medium low	Verification, medium- to large-scale identification
Iris	High	Medium	High	High security access, large-scale identification
Voice	Medium Low	High	Low	Telephone authentication, low security verification
Signature	Medium low	High	Medium	Applications with traditional signature
Hand	Medium high	Medium high	Medium	Verification for access control
Multimodal	Very High	Medium	High	Potentially all, cost related issues
Pin/Password	Medium low	Medium low	Low	Default implementation

[1] *Acceptability* encompasses the user-related aspects such as Intrusiveness, Cultural Concerns, User Acceptance, Effort and Universality

Source: Accenture secondary research

Figure 7. Comparisons of Biometric Technologies

One of the predominant issues in the use of biometrics has been the lack of usability of the biometric systems for everyday users. The move from laboratory research, as well as human assisted law-enforcement uses of biometrics, to "self-service" installations has been slow to materialise due to the additional challenges such an environment poses. Part of the enrollment process must be to train users and make them comfortable with the process.

Users will benefit from both assisted and unassisted training. This has been shown to reduce error rates in a number of biometric trials involving pedestrian traffic.

Face

Facial recognition, unlike fingerprint, is a non-contact biometric that can be acquired at a distance. Various camera types may be used to capture facial images and these are processed and compared against enrolled images of the user (verification) or against persons on a watch list (identification). Comparison techniques are generally based on the geometry of the face, where up to fourteen features are used as landmarks, or on a global pattern representation of the face and its similarity to different generic faces in a gallery. More recently, skin texture analysis has been employed, in particular as a method of differentiating between twins. Technology employing three dimensional (3D) modelling of the face, using stereo cameras or structured light, is also maturing.

In theory, the person being authenticated only needs to be within the field of view of the camera to be subject to facial recognition. Factors such as lighting, movement, face positioning, differences in appearance over time, and many other factors make successful face verification less reliable. When the verification time must be minimised for both user acceptance and throughput reasons the difficulty is further increased, but this can also be said of other biometrics.

For over a decade, vendors and universities have been demonstrating facial recognition products, often quoting laboratory-tested biometric error rates. However, the level of performance observed in the laboratory is typically unachievable in the real world, due to the lower degree of control over the factors that affect performance (e.g. lighting conditions, which greatly affect accuracy). This degradation hinders the acceptance of the underlying products as building blocks for highly usable automated identity verification systems. Automated face recognition can be used as an automated identity verification mechanism (e.g. Australia Smartgate), as an input to a manual inspection process, or for 'watch list' purposes; it can also be used in combination with other biometrics to provide higher levels of security and accuracy.

Two of the key performance issues in deploying facial recognition are:

- Variations of environmental and user factors, including facial lighting, user pose, expressions, and eyewear.

- Difficulty to process moving users, due to the difficulty in locating and correctly segmenting face images from pedestrian users who are walking towards a video camera.

However, progress continues to be made in improving this technology as evidenced in Portugal's RAPID system.

Finger

From a usability perspective, all biometrics have both strong and weak points. Often the biometrics that are the most easy to use (e.g. requiring no physical contact), can be the weakest in terms of accuracy.

Fingerprint analysis has been the predominant method of identity verification for over 100 years. Thus, fingerprint technology, in its original ink-based form and more recently in 'live capture' electronic forms, has had tremendous resources applied to enhancing automated capabilities.

Evaluation of vendor algorithms for large-scale government programmes is carried out regularly. In particular, this is performed in the US by the National Institute of Standards and Technology (NIST). The results are often published, sometimes without releasing the names of the participating technology vendors. As with facial recognition evaluations, much of the emphasis has been on testing algorithm accuracy and more recently compatibility. Almost all of the data used in these tests is from supervised or human assisted acquisition techniques. Of late, there have been deployments of systems that provide automated capture, without this supervision, such as the miSense trial in London Heathrow airport.

Fingerprint capture is generally contact based and the user has to correctly place their finger(s) on a sensor for capture. This can be a process with a high degree of variability, especially when significant amounts of time are not spent training and re-training the users. With some devices the process can be tedious, depending on the acquisition time, however, new devices are now coming onto the market which can be used with confidence e.g. at Disneyworld.

When high quality fingerprint images are obtained, state-of-the-art comparison algorithms can perform a strong verification of identity. As might be expected, the more fingers that are captured, the greater is the achievable accuracy.

Potential issues with fingerprint technology include:

- Achieving adequate acquisition, match and non-match performance within the time constraints of the airport environment.

- The tolerance of individual technologies and products to environmental conditions and contamination, such as heat, humidity and dust, which may be present at a location, and the related operational challenges (e.g. regular cleaning).

- It is possible to build multi-biometric systems in which finger imaging can be used to securely strengthen the verification abilities of facial recognition. However, it is important to note that fingerprint (and thumbprint) is becoming the norm for biometric use on a mass scale and has been for many years in countries such as Hong Kong.[53]

Iris

The human iris is a biometric that is widely acknowledged within the biometrics industry to be one of the most accurate and stable human authentication systems in existence. However, it has some issues in terms of the ability to conduct background checks and also from a practicality perspective.

Although the area of the iris is small it has enormous pattern variability, which makes it unique for every person and hence leads to high reliability. The fact that an individual's right and left eyes are different and that patterns are easy to capture, establishes iris-scan technology as one of the biometrics that is very resistant to false matching and fraud. The only widely deployed iris recognition algorithm can offer a false accept rate (FAR) of ~0.0001% (1 in a million).

---

[53] eChannel scheme for HKSAR ID Card holders.

The iris pattern does not change or deteriorate over time under normal conditions, unlike other physical characteristics such as face, hands or fingers. During the first year of life a blanket of chromatophore cells may change the colour of the iris, but the iris pattern itself is stable throughout a person's life.

Of course, an iris may be altered by actual physical damage to the eye, such as might occur from an extreme accident. The same could be said for finger and face. Iris geometry may also change slightly over time, but the impact on matching accuracy is limited, and usually does not affect system performance.

Issues with iris technology include:

- It is important to note that unlike fingerprint and face, there are limited legacy systems or data that can be used for potential searches.

- Cost and risk of vendor lock-in (although the market, which was locked down for many years, has started opening with the expiry of some key patents).

- Iris recognition is very difficult to perform at a distance further than a few meters or if the subject is non-cooperative. Current iris recognition technology requires the subject to be still and directly looking into the camera during the image acquisition process – which can lead to user issues, inconvenience and time delays. As with other biometric technologies, iris recognition is also highly susceptible to poor image quality, with associated failure to enroll rates.

- Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made in fingerprint recognition. In addition, the only proven technology is controlled, through patents, by a single vendor, which imposes some additional risk on any deployment.

- One recent research development is the ability to capture iris while a subject is walking towards the security checkpoint. This 'iris on the move' technology appears highly promising, but is still in the research stages and not yet available to the market.

Appendix G - Approaches to data storage

At a high level, there are three broad approaches to data storage and access that are outlined in the following subsections:

- Centralised

- Federated

- Distributed

Centralised Approach

In a centralised approach, the status of RPs and the information needed to authenticate their identities is stored in a central system managed by a single organisation.

This is the storage model currently used by a number of European information systems such as SIS II (planned for 2008), VIS (planned for 2009) and EURODAC.

A centralised system might be assessed against the three key factors as follows:

- Responsiveness – A single central system might present challenges around response times. Whist a single central system would be expected to process queries relatively efficiently, the sending and return of these queries internationally could add considerable latency, especially if large volumes of data were to be exchanged. This risk could be mitigated by implementing national replicas of the central system, similar to the model used by the Schengen Information System (SIS), so that queries would be performed against local copies of the central database.

- Trust – Data stored in and retrieved from a central system must be trusted by individual Member States and by the RP who provides his data in good faith, assuming close controls of access on the central system to avoid the possibility of tampering, coupled with trusted data input from the various Member States. Once the data stored on the system is trusted, accurate transmission to National Authority offices can be achieved by ensuring the implementation of secure interfaces and communication links using strong authentication between the central system (and the national replicas, if appropriate) and the National Authority systems. Since each of these challenges has been solved in the past (as demonstrated by the successful implementation and operation of SIS), a centralised system could satisfy the trust requirements placed upon it.

- Legal requirements – Each country has individual laws concerning the storage of biometrics in centralised systems, which would have to be considered. In addition, issues relating to accessing (or replicating) the centralised database from other Member States would need to be addressed.

Federated Approach

In a federated approach, the information on a passenger is stored in the originating Member State's own system. Access to each database would have to be provided and real-time, secure communications would have to be implemented between the Member States' systems. This is a more technically challenging solution.

A federated system might be assessed against the three key factors as follows:

- **Responsiveness** – Like a centralised system, a federated system might present challenges around response times, and these challenges might be addressed in part by an appropriate replication strategy. The data query process is complicated further by the need to ask "who holds this data?" to determine the appropriate database before the actual query can be made. Conversely, a Member State's own records will be available locally (intra-state) without the need for replication.

- **Trust** – A federated system presents the same type of trust challenges as previously described for a centralised system, with the added complexity that there are many more interfaces to be secured and other security and access issues to be resolved.

- **Legal requirements** – A federated system is likely to raise the same legal queries as previously outlined for implementation of a centralised system. This could be mitigated in part if local replication of other Member States' databases was foregone and each state only offered query-response access to their data.

An alternative federated approach is one where within each Member State there are numerous data sources that exist. It could be envisaged that RPs' data is to be held on one of a number of systems within each Member State (for example, by the various airport operating companies, should they be involved in enrolling RPs). This is a more complex variant of the federated approach and might present particular challenges if the storage and exchange of RPs' biometric data between private firms is required.

Distributed Approach

In distributed data storage architecture, RP data would be held by the individual RPs, on a membership card or other token (such as an ePassport or mobile phone) that would be presented and read each time the RP wished to use the scheme. This will probably be the most feasible approach, from a technical, legal and scalability point of view. Privium, PEGASE and miSense are good examples of a distributed approach.

Whilst centralised and federated systems could opt to have RPs carrying tokens to aid their identification, a distributed architecture would require it.

As well as the token-based storage, a centralised list would be required to maintain a record of invalid (e.g. lost or stolen) tokens, as a minimum. This model is similar to the 'credit card' model where all relevant user data is stored on the card, and a 'blacklist' is held centrally which can block usage via a central system. In reality, it is likely that a number of other centralised lists might be required, depending on the type of RP scheme implemented (for example, to confirm that the token holder has permission to travel to Country A).

The management of RP status would require on-line or frequent database searches in order to ensure that there has not been a change in the traveler's situation and eligibility. There would need to be clear lines of responsibility between who is the data owner and processor and also clarity around access management to the centralised list or access to RP level data. It may be that there is one overall RP system owner (who maintains the central list, but the list only contains basic data relating to the membership number and RP status) and each RP scheme owner – who records, transmits and stores RP biographic and biometric data. During the analysis phase of any RP scheme, the US RT model should be looked at carefully to see how the data privacy and processing issues are handled.

If the RP scheme implemented a common vetting process and clearance procedure then biometric and biographic information of applicants would also have to be held at a central level, to enable the de-duplication process at enrollment, as well as to support initial security checking. The information could also be used on a perpetual basis to carry out on-going status checks to ensure that the traveler is allowed to retain their RP status, or to re-issue lost or damaged membership tokens.

A version of this approach was developed for the TSA and is being adopted by the US Registered Traveler programme. In this example, a central system (known as the CIMS or Central Identity Management System) provides the interfaces to support vetting of passengers (a common method for agreeing the bona fides of an RP). Once complete, the information necessary to authenticate the passenger (including their biometric data) is stored securely on a smart card carried by the RP.

A distributed system might be assessed against the three key factors as follows:

- **Responsiveness** – Although a system using distributed storage will, as a minimum, still require connectivity to a central (or nationally replicated) database for validity checking, the bulk of data retrieval will be performed locally against the user token. Therefore a distributed storage approach can be expected to yield the best responsiveness of the three models under discussion.

- **Trust** – A distributed system will have to maintain the integrity of potentially millions of tokens which are in public circulation. The existing standards around ePassports have been defined by ICAO with this specific purpose in mind, and include digital signing of the passenger's identity data during the enrollment process, to assure that it cannot subsequently be tampered with without detection. These same standards could be implemented to safeguard an RP token (as in the miSense Trial at London Heathrow airport in 2007). In this data storage model, RPs will have to trust that their data is secure on their own token, as well as on the central system. Again, as per the standard for ePassports, this can be assured through the use of mutual authentication protocols ('keys') between a token and the system it is presented to, ensuring that the token's data is obscured unless that system is trusted and authorised to receive it. The responsibility for ownership and management of these encryption keys is of prime importance and could be a role that the EC or another centralised body could play.

- **Legal requirements** – A system following a distributed storage approach may run into fewer legal issues than a centralised or federated system since the individual RPs will store their own data, which they have the option to present (or not) at each airport. For example, the Privium registered traveler scheme operating at Schiphol airport has used a membership card to avoid the need to retain biometric data on a central system. With a distributed approach, biometric data belonging to RP scheme members does not necessarily have to be held centrally (though it may be desirable to do so for operational reasons).

Rapid and Easy access to RP lists

If Member States need rapid and easy access to up-to-date lists of all RPs (including those from other Member States), the data storage model adopted will in part dictate the appropriate method of sharing the current RP data between Member States.

Before reviewing the access and ease relating to each approach, the need for accessing full lists of all RPs must be questioned and understood. The reason for challenging this need is that a positive check does not exist for passport holders, instead a central revocation list or negative list is used.

If there is no clear identification or membership card and a government issued ePassport is used, then there needs to be a quick and easy way to confirm the identity and status of the RP at the point of use. Otherwise everyone with a Passport could witness the fast path and think they can use the RP scheme. This has happened with many of the operational schemes that do not have a token.

The need for a positive list could be to add an extra layer of certainty to the RP and provide comfort for the authorities around the fact that a membership has not been created without the correct authority.

Centralised Approach

Rapid Access

A centralised storage model will mean that all Member States can be immediately appraised of new (and revoked) RPs, since they will be checking against a single logical database. The update may be delayed if local replicas are used. Estimates of the actual time taken to obtain the data from the central database should be made during a technical investigation, but these can be expected to range from a few seconds response for simple queries (such as the current validity of an RP's membership card) through to tens of seconds or even a few minutes for a complex biometric matching query – subject to network connectivity.

If biometric authentication of RPs is required at the airports, given the anticipated numbers of RPs, and understanding the relative performance of the different types of biometric query, it is preferable that one-to-one queries are routinely used ("Is this traveler Mr X?") rather than one-to-many queries ("Who is this traveler?"). One-to-many queries will still need to run in order to de-duplicate RPs at registration, but these can be performed as background tasks. To facilitate this, travelers will need to carry a token that holds at least an ID number (perhaps a membership card, or a passport, as used in both the Germany ABG and UAE eGate schemes) that can be used as a reference to the central database to find the RP's record and match against it.

Easy Access

In order to facilitate the exchange of RP data, the query and data formats, interface standards, and security policies should be carefully defined. Where appropriate, existing standards can be leveraged for this purpose (such as ICAO's guidance on encryption keys contained within 'PKI for Machine Readable Travel Documents'). Where no standards currently exist, the central system should make available a single set of interfaces for Member State access (including, continuing the example given above, an interface that returns the current validity of an RP's membership in response to a query from a National Authority).

Federated Approach

The approach outlined for the centralised model applies equally to the federated approach; indeed, with the proliferation of systems amongst Member States, it is even more important to have one central body defining the standards for data exchange.

Distributed Approach

Rapid Access

The distributed storage model differs from the centralised one in that most of the data required at the airport will be held on the RP token, which can be read locally. Because this data does not have to be retrieved from another Member State, such a system can be effective epending on the encryption technologies and computing hardware used – for example, the miSense Trial at Heathrow airport demonstrated the reading and decryption of a traveler's fingerprint from their smartcard in around five seconds. The central database requests that are necessary tend to be restricted to simple queries, such as permission to use the RP lane checks, aiding the responsiveness of the system.

Easy Access

To ensure compatibility between Member States, the data on the token itself should adhere to an agreed standard such as ICAO's Document 9303 for storage of personal data on machine readable travel documents. As previously discussed for the centralised system, a standardised approach should be adopted to facilitate queries against the central database.

It should be noted that the ability to obtain passenger data locally from a token can help in situations where connectivity to a central system is not consistently available. This reason was a contributing factor to the design of the US Registered Traveler programme - airports in the US cannot guarantee continuous online connectivity to a central system, and airport authorities felt the costs of putting continuous connectivity in place to be prohibitive.

Appendix H – Report methodology

Stakeholder Consultation

A consultation exercise was completed with over 30 representatives with an interest in passenger aviation security and air travel. These sub-sections detail the selection process and the methodology used when completing interviews.

Stakeholder Selection

The Study Team identified a list of key stakeholders who could provide professional opinions on the questions put forward by DG TREN and around the concept of an RP programme. The EC DG TREN recommended the Study Team consult with the following representative organisations:

• International Air Transport Association (IATA)

• European Regions Airlines Association (ERAA)

• Association of European Airlines (AEA)

• International Air Carrier Association (IACA)

• Airports Council International (ACI)

In addition to the representation organisations recommended by EC DG TREN, five Member States were selected as 'primary' stakeholders by the Study Team to get a good range and understanding of the Member States. As such a combination of the size of the country (large and small), geographical position in Europe (East and West, North and South), and membership length (new and old Member States) were selected.

The primary countries were:

• Belgium

• Germany

• Malta

• Poland

• Spain

In addition to the primary list of stakeholders, the following countries were also added:

• France

• Ireland

• UK

The full list of stakeholders and contacts is detailed in Appendix A.

Consultation Objective and Process

The objectives of the consultation exercise were to get an understanding of the opinions of key stakeholders in the industry in response to the concept of an RP programme and to consult on 12 questions documented in the ITT.

The aim of the interviews was to gain a further understanding of the issues and questions surrounding an RP programme. In conducting the interview process, a standard series of summary questions was developed and sent to the stakeholders in advance. The questions then formed the basis of the stakeholder interviews and the outcomes from the meetings were documented and sent back to the stakeholder to confirm. Wherever possible, meetings were conducted face to face. In some instances, however, some meetings were conducted by telephone.

Desk Research

In addition to the consultation exercise, extensive desk-based research was undertaken to ensure that published reports and statistics were reflected in the Report.

This included a review of existing schemes around the world and includes Privium (Schiphol airport), the miSense Trial (London Heathrow) and the Registered Traveler Programme in the USA.

Legal Review

The two questions that focus on the legal aspects of feasibility (in terms of Aviation Security regulations that may need to be amended) have been reviewed by the University of Leiden International Institute of Air and Space Law and additionally reviewed with Marion Knoben (EC DG TREN) in a meeting dated 6th June 2007.

Attendance at Events and Forums

The European Registered Traveler forum was held in Paris on 28th Feb and 1st March 2007. This event was attended by members of the Study Team and insights were recorded for use in the Report.

In addition to the Registered Traveler Forum, the following events were attended by the Study Team:

- IATA Simplified Passenger Travel Interest Group (held in Copenhagen from March 20-22nd 2007)

- Global Passenger Summit (held in London from 26-27th April 2007)

RP schemes around the world

Whilst the focus of the Study is primarily on aviation security, there are a number of different schemes around the world that focus on parts or the whole of the passenger journey for air and land travel. Schemes can also be free of charge or fee based and can be run by airports, airlines or Control Authorities.

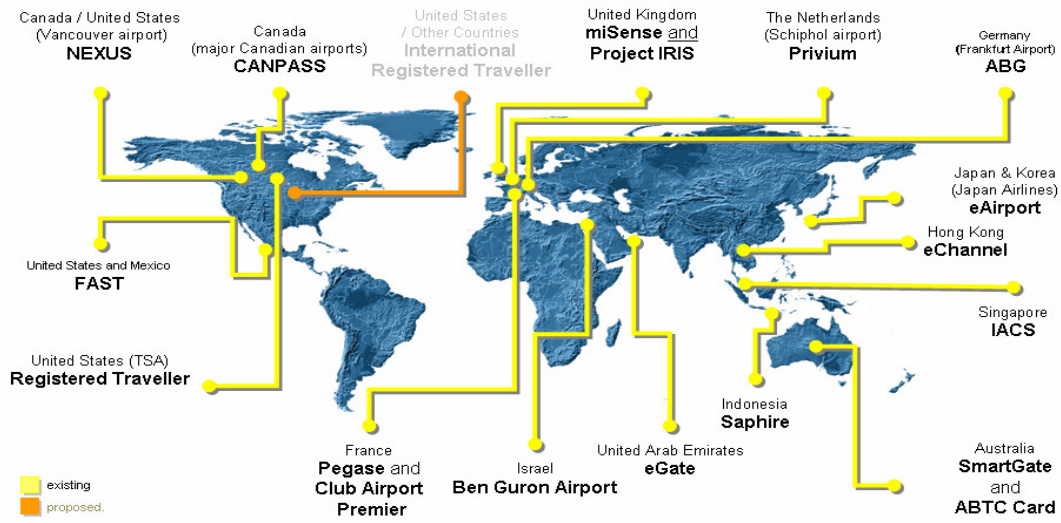Appendix C details some of the schemes that exist around the world and Figure 8 shows a summary of these below.

Figure 8. Schemes around the world