BORDER MANAGEMENT: KEEPING PASSENGERS MOVING
Contents

Foreword..............................................................................................................................................................................3
Part I – Joining the dots ......................................................................................................................................................4
  Identity management....................................................................................................................................................4
  Moving data collection upstream..................................................................................................................................4
  End-to-end border management .................................................................................................................................5
  Integrated communication infrastructure.......................................................................................................................6
Part II – How will it improve facilitation? .............................................................................................................................7
  Speeding up manual checking......................................................................................................................................7
  Automated entry checkpoints.......................................................................................................................................7
  The early adopters........................................................................................................................................................8
  Separation of passenger flows......................................................................................................................................8
  Integration of self-service processes ............................................................................................................................9
Part III – What are the challenges?....................................................................................................................................10
  Greater stakeholder collaboration...............................................................................................................................10
  Closer inter-State cooperation....................................................................................................................................10
  Balancing privacy with security...................................................................................................................................10
  Deploying standards...................................................................................................................................................11
Part IV – Conclusion ..........................................................................................................................................................12
Notes and references ........................................................................................................................................................14
Foreword

One of the great conundrums facing the air transport industry has been establishing the right balance between facilitation and security. How much should the vast majority of legitimate air travellers be inconvenienced to deter the few?

There is of course no definitive answer, but the scale of the 9/11 devastation redefined the threat and showed us that the balance was not right. Since that time governments and the air transport industry have worked to build a more secure global air transport system. But long lines of frustrated travellers snaking through airports worldwide and a series of high profile security failures are a testament to the bluntness of many border management techniques. It is no surprise that the 2009 SITA/Air Transport World Passenger Self-Service Survey found security screening as the step of the journey air passengers would most like to change.

However, the next decade should see a radical improvement with tighter security and faster facilitation going hand-in-hand. Overlapping developments in technology and increasing growth in passenger numbers are driving the change. This New Frontiers paper takes a look 5-10 years into the future when billions of low-risk passengers will be quickly, conveniently and cost-effectively processed, while focusing valuable resources and attention on high-risk travellers.

To get there, border management agencies worldwide are implementing an intelligence-led approach to drive new integrated strategies. Information gleaned from government and industry databases will be the lifeblood for data-driven systems to provide advance risk assessments on every passenger. Their use will be sharpened by harnessing the power of networked technologies and intelligent applications to improve both targeting and throughput. A systematic risk analysis will be the key element in determining every passenger’s right to fly.

The speed of progress will vary from country to country, so system-wide improvement will take time. Countries such as Australia, Canada, the United States, as well as the EU-bloc, are laying the groundwork with respect to passenger data driven solutions, while the countries of South East Asia and the Middle East are leading with respect to biometric solutions. Indeed, much of the progress to date has been achieved at a national rather than international level. Nevertheless, it is a necessary stepping stone and in five to ten years a more cohesive picture will have emerged with a far greater number of countries adopting the best practices of the early leaders.

Tom Marten
Vice President,
Business Development Government and Security Solutions
SITA
Part I – Joining the dots

In the eight years since the September 2001 attacks on the World Trade Centre fresh security threats have targeted air travel, including the shoe bomb plot aboard an American Airlines flight\(^1\) and the 2006 conspiracy to detonate liquid explosives on ten transatlantic aircraft\(^2\). Each one has brought incremental responses, both to the frontline screening of passengers and the background intelligence gathering. But this has resulted in disconnected processes applied inconsistently across the global breadth of air transport.

It was a problem alluded to by US President Barack Obama, following the Christmas Day 2009 attempt to detonate an explosive onboard a Northwest Airlines flight bound for Detroit. A young man with suspected terrorist links travelling on a long-haul flight with no checked-in luggage, who purchased his ticket at the last minute for cash, should have raised red flags, both on arrival in the US and on departure from Europe. The fact that it did not was a result of “systemic failures”\(^3\) to use the words of the US President. The information to uncover the plot had been available, but authorities “failed to connect the dots”\(^4\). There had been a shortcoming in international cooperation, as well as a failure of outbound checks from Europe.

It is clear the business of border management needs to transform significantly to cope with the increasing frequency and sophistication of attacks on or using the aviation system. But with over seven billion passenger movements through airports expected each year by 2020\(^5\), this transformation will require a much deeper focus on a risk-based approach – “finding bad people, not just bad objects” as Giovanni Bisignani, CEO of IATA, put it. Collecting and using information will be the lifeblood of the transformation.

How are the dots going to be joined?

- Better identity management
- Moving data collection and control tasks upstream
- End-to-end border management
- Integrated communications infrastructure

Identity management

A key tenet of risk-based profiling is being able to correctly identify each person. In the future all passengers will be locked into a secure biometric identity, allowing governments to reliably track movements across borders. This will reinforce border management strategies by providing more information to improve targeting.

The most common identifier will be a biometric passport or e-passport as they are known. These contain a digital image of the face and in some cases another biometric identifier. E-passports make it possible for the first time to establish a unique connection between the document and its owner. Biometric verification at airport checkpoints will ensure the person travelling is the same one to whom the travel document was issued (and on whom passenger data checks are performed).

Identity management will also be strengthened by including biometric data collection as part of the visa application process. The biometrics will be checked against those held in databases and combined with other data sources to provide a better risk assessment. A three month UK trial in 2007 uncovered over 300 applicants making a visa application in a second identity\(^6\).

Moving data collection upstream

While stronger identity management improves the quality of risk assessment, so too will having more time to assess the risk level. In essence, the earlier the risk is identified and acted upon, the greater the chance of it being mitigated – and the less costly to do so. It is therefore both more effective and more efficient to move data collection and analysis for air travel as far upstream as possible. By doing this, not only will the threat from high risk passengers be identified earlier, but equally low risk passengers – who make up the overwhelming majority of travellers – can be processed early on to facilitate their faster movement through border controls.

The initial step in many international journeys is the visa application. Therefore an important requirement in joining the dots will be to bring consular processes and border management closer so that visa issuance is fully integrated into border control. Biometric identifiers and passenger data of visa applicants captured at consular points will be stored on a shared database making it easier to detect, verify and track high risk travellers from their past visa applications.
The process will be further strengthened by linking to other security databases so that the visa application is assessed not in isolation but in conjunction with other relevant information known about the passenger. For many countries, much of that material today lies within siloed government agencies and often stored in systems that do not “talk” to each other.

The information will also be shared with applications and personnel downstream and enriched with new information as it becomes available, including data from the Passenger Name Record (PNR) held in the reservation system of the airline and Advanced Passenger Information (API) supplied by the passenger at check-in. Australia, Canada, South Africa and the US have already adopted solutions that follow this path.

The accelerating trend of off-airport check-in, via the web or mobile phone is making API information available much earlier from a larger proportion of the flying public. Currently, around 24% of passengers use off-airport check-in, but it is expected to double to 48% by the end of 2013. This provides more time for border agencies to cross-check it and develop a more accurate risk assessment by the time the passenger reaches the outbound border checkpoint. The increased threat to airlines in-flight has made it of paramount importance to stop and check high risk travellers before they board the aircraft.

The US, for instance, plans to use “intelligence-based” profiling for “surgically targeting” in-bound passenger from 14 countries, in the wake of the failed December 2009 attack. This replaces a blanket approach that saw all passengers on flights from the countries suffer the indignity of extra physical security screening before they could board the aircraft.

**End-to-end border management**

A major difficulty for border management has been determining whether someone who has entered the country is still there or has departed. For example, it has been estimated that around 40% of all visitors to the United States overstay their visas. The fact that it has to be an estimate highlights a serious problem for border agencies trying to join the dots – there are a large number of unaccounted travellers. While the vast majority will be low risk, it still leaves an intelligence gap that can be exploited, and a serious shortcoming in terms of border enforcement. In fact at least six of the 9/11 hijackers were reportedly overstaying their visa.

The border security of the future will see all travellers counted in and counted out. It is a mammoth task, particularly where there are extensive land crossings, and in countries such as the US which have not historically conducted outgoing border checks. Movements across the external borders of the EU underline the size of the undertaking. Each year, 160 million EU citizens and 140 million non-EU citizens move in and out of the EU-bloc. Nevertheless, it is a necessary step and the relative ease of implementation and the greater scale of threat compared to land and sea entry points is encouraging governments to make air transport the first place to close the gap.

Creating a closed aviation system will allow border management agencies to count in and count out each passenger.
As a result departure information will be collected from air carriers and matched against inbound data to verify that the person entering was the same as the one leaving. This will provide compliance data on passenger movements that will improve future decision making and risk assessment, both overseas and at the point of departure.

Risk assessment and watch list checks conducted on outgoing passengers by programmes such as the US Secure Flight initiative will help prevent suspected terrorists from fleeing their crimes, as in the recent Times Square bombing attempt, and will help identify potential terrorists such as the December 25 bomber before they start their missions. In particular, the end-to-end control over passenger movements should enable the compilation of improved watch lists as well as the development and roll out of trusted traveller schemes designed to allow legitimate travellers to pass quickly through controls.

Integrated communication infrastructure
If the dots are to be joined not just at the strategic and process level, but also at the technology level, then a secure, high performance IT infrastructure will be essential to deliver the level of automation and response times to keep passengers moving.

Today, most of the systems used can only handle text data, but in 5-10 years they will be required to transmit, process, and store biometric images, as well as the biographic data, relating to more than 20 million passenger movements through airports each day. API datasets requested by governments will need to include biometric identifiers for each passenger and crew on top of the biographic data already supplied.

Many governments may wish to check the biometric of incoming passengers against those of suspected criminals stored in biometric databases – a so called “one-to-many” check. This approach raises valid privacy concerns, but as was the case with supplying passenger data, IT systems can be designed and harnessed to protect the privacy of travellers at the same time as they protect their lives and safety.

Within the airport environment a real-time processing capability will be imperative. Passengers will interact with kiosks and control sensors at automated border points to scan passports and visas, as well as validate biometric identifiers. Border agents will need to interrogate ‘live’ security databases to determine go/no-go decisions for those passengers pre-selected from a risk assessment for manual processing.

Handheld devices used by control personnel will be linked directly into the communication infrastructure, so that information regarding the passenger is cross-checked with databases while the traveller is with the border agent. Currently, passenger information is often stored in the devices and not uploaded to databases until the end of the agent’s shift, undermining their usefulness for pre-emptive action.

The constant back-and-forth of information and synchronization of distributed databases will result in a massive increase in communication traffic, putting considerable demands on bandwidth availability. The criticality of the information will also require the communication to be secure. That implies the use of encryption using digital certificates, such as those provided by Certipath.
Part II – How will it improve facilitation?

While security threats are the most pressing driver for change, growing volumes of passengers and limited airport capacity are also forcing border management agencies to examine strategies to enhance convenience for passengers by reducing time spent at airport checkpoints. As the June 2007 attack at Glasgow Airport indicated, just having a large crowd of people queuing in the terminal building presents a potential target.

The greater focus on pre-emptive, risk-based assessments will improve facilitation in four ways:

- Speeding up manual checking
- Automated entry checkpoints
- Separating passenger flows
- Tighter integration with self-service developments

**Speeding up manual checking**

The checking of documents by border officials will remain a common occurrence at airports in many countries in the near future. Nevertheless, the process will become much faster for the vast majority of travellers as the use of e-passports and e-visas becomes prevalent. Running a passport through a document reader is quicker than visually inspecting it and eliminates the need for manual data entry. The collection and validation of data upstream means border agents on the frontline will immediately receive a go/no-go decision on the passenger. This will significantly enhance the ability to manage bottlenecks and improve the facilitation of legitimate travel.

Mobile devices will provide additional flexibility to deploy staff in response to changing priorities, for example surges in low risk traffic. Border agents using handheld devices will be able to scan e-passports and receive a real-time risk assessment from a security database, for each passenger.

**Automated entry checkpoints**

The widespread use of e-passports provides the two necessary components for border management to embrace fully automated entry systems. First, the data is recorded in a digital form making it machine-readable. That means e-passports can be linked to other digital systems and authenticated without a human interface. Second, they contain at least one biometric identifier that can be automatically matched to the person presenting the passport. These two components together provide the identity confirmation, which when cross-checked against a government database, give the level of confidence necessary to remove the human decision making process from the equation.
The first steps are being taken by some countries (see inset below).

**The early adopters**

- The UK operates a biometrically controlled automated entry system at four major airports. Scanners match the eye pattern of pre-registered passengers with those held on a database. A positive match allows passengers to proceed and avoid queuing to present their passport to an agent at the control. Official results indicate the machines take 13-15 seconds per passenger, compared to 20 seconds for an agent.

- Australia and New Zealand use face recognition technology to give some arriving international travellers with e-passports the option to self-process through passport control. The SmartGate system, as it is called, takes a photograph of the passenger and matches it to the digital image stored on the e-passport. The passenger is then free to go straight to the baggage hall.

- Pre-enrolled Israeli citizens can use a biometric smart card based system to enter Israel through Ben Gurion International Airport. The card stores a biometric of the hand geometry of the card owner which it then matches to the passenger. The system reportedly processes passengers three times faster than if going through the human inspection channel.

- Singapore residents use a biometric smart card for automated immigration clearance travel through Changi International Airport.

- Over 60,000 UAE citizens and residents are enrolled to use biometric e-Gates for automated border crossing at Dubai International Airport.

These examples are largely focused on expediting residents of only the host country and, in some cases, another country where there is a close tie. Expanding it to the next level so that a much wider group of travellers can benefit is going to take time and much will depend on the willingness of governments to share information on their nationals.

They also highlight a further impediment to creating a common system-wide automated entry system. The lack of consensus over the “best” biometric may make it difficult to harmonize on a global scale.

Further down the line, the promise is for much faster biometric verification technology. Some providers are already claiming rates as fast as 30 people a minute\(^1\), equivalent to one every two seconds. If this level of throughput proves realistic and sustainable in a live airport environment then it will significantly speed up airport border checks for legitimate travellers.

**Separation of passenger flows**

The improvement of risk assessments on each passenger will pave the way for much greater use of automation in the exit processes of passengers. The separation of travellers into flows that reflect their risk profile will allow border management agencies to tailor resources more effectively to combat the different threat levels. There are strong incentives for achieving it.

A number of countries, such as the Netherlands and US already operate trusted traveller schemes. These commonly pre-screen travellers in return for fast lane access and simplified security checks. Official reports indicate the majority of such schemes deliver faster processing, estimated to be one third of the time taken for manual immigration\(^1\).

Trusted travellers programmes can also be linked with automated border crossing gates so that the traveller not only has a simplified security check but can then proceed directly across the border.
Biometrics underpin the integrity of the process. Members of the scheme are issued a smart card encoded with a biometric identifier, such as an iris scan or fingerprint. It can then be inserted in kiosk style machines to match against the passenger at designated control points within the airport.

As with many automated entry systems, membership of these expedited security check and border crossing programmes is often limited to residents of the country in question, so members of one scheme do not have entitlement to benefit from similar schemes in other countries. Consequently, a system-wide scheme is still a long way off, but some countries are taking the initiative and expanding their programmes.

The US and Canada, for instance, jointly manage NEXUS, a scheme run for US and Canadian citizens, while the Netherlands and US have a memorandum of understanding to link their trusted traveller schemes at Schiphol and JFK airports. In the United Arab Emirates, the eGate scheme run at Dubai International Airport is now open to visa holders from 33 countries.

A more significant step is the discussion by Germany, Netherlands, the UK, and EU border agency Frontex to promote an ‘International Expedited Traveller (IET) Programme’ as a possible blueprint for a common Registered Traveller and Automated Border Crossing programme across all EU Member States. If successful, it would represent a major milestone in the vision of a system-wide programme.

Integration of self-service processes
To avoid a paralysis at control points in terminal buildings, governments, airlines and airports are starting to cooperate far more so that border management supports and works in tandem with existing and expected self-service developments.

The UK miSense trial, which ran from December 2006 to March 2007, successfully tested elements of IATA’s Simplifying Passenger Travel (SPT) initiative. The aim of this initiative is to improve the 14 separate steps of each passenger journey and enhance security by replacing repetitive checks of passengers and their documents. The system will collect the information once and then share it electronically with subsequent service providers to clear the passenger through their entire journey. The lynchpin for it is capturing biometrics for identity verification at key points in the departures and arrivals process.

There is a strong incentive for airlines in particular to strengthen the security of self-service processes. They have made large investments in technology to improve facilitation through the airport and cannot afford the perception – or the reality – that it may not be as secure as the human approach.

In particular, the use of 2D bar codes is set to become the primary mechanism for airlines to automatically “guide” passengers through the airport touch points from check-in kiosks through bag drop points to the gate and onto the aircraft. The barcodes will store the itinerary of the passenger replacing the magnetic stripe boarding pass. How fast and how widely that vision will be realized is largely down to getting governments to accept them at airport security checkpoints. Currently, over 20 countries out of the top 40 accept bar coded boarding passes. That equates to 234 airports representing 57% of passengers.

Airlines also have the responsibility to ensure that a passenger is properly authorized to travel. Failure to do so can be costly. IATA estimates the average fine for each of the 35,000 travellers turned back each year with improper documentation is US$ 5,000. With associated manpower costs, that adds up to a US$ 200 million problem for the industry.
Part III – What are the challenges?

There are some major bridges that need to be crossed to reach the end goal of a holistic passenger processing system that is both secure and convenient.

**Greater stakeholder collaboration**
The need for much greater cooperation and collaboration between governments and industry participants, both at the national and international level, is paramount.

**Closer inter-State cooperation**
The cordon of security around the air transport system will only be as good as the weakest link so a more structured and effective approach, based on global cooperation between governments, is vital. ICAO is the appropriate body to achieve it, but its assemblies are held only once every three years, making it difficult to develop a regulatory framework that is flexible and responsive enough to quickly accommodate new security situations.

That puts pressure on countries to act unilaterally or multilaterally with trusted partners. The result is security measures that are not applied uniformly and consistently across the whole air transport system. It also leads to passengers from some countries being treated en-bloc. In essence, the risk level of passengers is judged not by their individual risk, but a perceived risk based on their country of nationality.

At the heart of the issue is creating an environment that allows for the much wider sharing of data between governments in order to make quality risk assessments at an individual passenger level.

**Closer government-industry cooperation**
There is also the need for stronger relationships between the industry and border agencies. It is a position that is now increasingly accepted and recognized by both sides. The deep involvement of IATA CEO Giovanni Bisignani and US Secretary of Homeland Security Janet Napolitano at an IATA aviation security summit in January 2010 is a testament to this.

Nevertheless, there is still a degree of friction that threatens to slow progress. Since 9/11 a much greater burden has fallen on the airlines and airports to ensure compliance of new security regimes. According to IATA, security measures cost airlines US$ 5.9 billion in 2009\(^\text{16}\). There will be no let up. The collection of biometric identifiers from departing passengers to include with the current API datasets may well be next on the wish-list of many governments.

Greater cooperation between governments and the industry would lead to more efficient mechanisms for securing air transport, reducing the cost burden on the industry.

Part of the issue is a lack of harmonization of requirements for passenger data between countries and by different control agencies within the same country. It creates a hugely complex data matrix for individual airlines to satisfy when providing passenger information. A community hub approach for airlines, which centralizes the collection, filtering and communication of passenger data, has significantly improved the efficiency on the airlines’ side, but there is a growing call for governments to use a single window approach on their side to receive and distribute the data covering all their agencies.

**Balancing privacy with security**
The classification of passengers by risk will make protection of personal privacy an even greater challenge than it is today. The convergence of data-mining and information integration with biometric identifiers, as well as greater international cooperation between governments, will drive increased oversight by privacy authorities to place reasonable limits on what data is collected and how data is shared across borders. It is likely that in the future, EU leadership in this area will generate a much needed global standard for protecting the privacy of travellers while ensuring their security.

Adequate data stewardship and protection will not just be a serious issue for governments, but one for the air transport industry as well. Airlines could find themselves burdened by some governments with collecting biometric data of passengers leaving a country to send to border agencies of both the country of departure and with the other API requirements to destination countries. Those airlines with extensive international route networks could face legal uncertainties in some parts of the world, unless harmonization of data privacy regulations can be achieved.
Deploying standards
There is a strong consensus that security would be strengthened and facilitation enhanced if border management procedures and the technologies that underpin them were standardized system-wide. International measures, applied universally and systematically, would ensure passenger familiarity with requirements, in turn speeding the flow through controls and reducing border agent interventions.

For example, nearly four years after the foiling of the Heathrow plot there is still widespread confusion amongst international travellers about LAG (Liquids, Aerosol or Gels) regulations from one country to another. An Australian government report on aviation security\(^1\) indicated that a lack of knowledge or preparation for screening by passengers was a major contributor to delays and queuing at control points.

It applies equally to airline workers and border agency personnel. Familiarity with security measures makes it much easier for those tasked with applying them to do it to a consistently high standard.

Technology standards are also going to be an important factor in determining how quickly governments and the industry are able to mesh the global patchwork of border management systems together to eliminate duplicate and inconsistent checks. Currently there are no universally recognized standards for security equipment or even for exchanging passenger data. Even e-passports can use three types of biometric identifier – face, fingerprint or iris. Different countries are opting for different identifiers making it more complex to link national border security initiatives, such as registered traveller programmes, together.

Technology and process standards will be essential if governments and the industry are to mesh the global patchwork of border management systems together.
Part IV – Conclusion

The challenge over the next decade is to speed up airport processing for the vast majority, while ensuring effective, accurate and timely responses to those who pose a threat. Overly zealous controls applied to lower risk passengers add considerable delay to the passage through the airport, and at worst it can amount to a disincentive to fly. We must always remember that air transport is one of the key pillars of the global economy, and is vital for growth and employment in many, if not most, countries of the world.

At the heart of achieving this is determining accurate risk assessments for each passenger. The most effective – and efficient – way of addressing risks is to identify those passengers which present a threat as early as possible. That requires cohesive strategies and processes, supported by smart technologies and better quality information.

Innovative security technologies, such as 3D face recognition and multimodal biometrics, smart cards and Radio Frequency Identification (RFID), will enable new security applications and the optimization of complex processes in the airport. Processes that today are operated manually will be automated or semi-automated. The enhanced data capability delivered by combining government systems with industry data sources and the integrity of identity delivered by biometric identity, should provide richer, more accurate, information on each passenger. Human intervention and randomness will always be a vital part of effective security programs, but intelligence led solutions will make such intervention more effective, less costly, and more expeditious.

This intelligence-led approach changes the thinking from one of random inspection to one of selective targeting of passengers based on pre-emptive risk assessment. Border inspection at the airport is no longer the primary line for determining the right to travel. This has already been determined. Instead, inspection may be used simply to confirm what is already known and provide a convenient point of interception.

The approach will allow fully automated exit and entry systems to play a much bigger role in processing lower risk passengers through airports using a mix of biometric identifiers, e-passports and secure 2D bar codes. Governments and air transport industry stakeholders will cooperate far more so that the joined-up approach to border management becomes an integral part of the industry’s passenger processing, complementing self-service developments.

Turning the local or regional progress that is already materializing in some parts of the world into a harmonized, system-wide security apparatus for the industry will take time. There are any number of reasons, including poor IT infrastructure, lack of political will or even legal complexities. It will require dialogue, cooperation and hard work by all stakeholders to overcome. Passengers will also have to play their part by trading a degree of privacy for increased security of the air transport system.
About SITA

We are the world’s leading specialists in air transport communications and IT solutions. We deliver and manage business solutions for airline, airport, GDS, government and other customers over the world’s most extensive network, which forms the communications backbone of the global air transport industry.

Created and owned by the air transport community, SITA is the community’s dedicated partner for information and communications technology. As a team of industry experts, our know-how is based on working with customers across the global air transport community. Almost every airline and airport in the world does business with SITA.

SITA innovates collaboratively with the air transport industry, and the industry itself drives the company’s portfolio and strategic direction. Our portfolio includes managed global communications, infrastructure and outsourcing services, as well as services for airline commercial management, passenger operations, flight operations, aircraft operations, air-to-ground communications, airport management and operations, baggage operations, transportation security and border management, cargo operations and more.

With a customer service team of over 1,900 staff around the world, we invest significantly in achieving best-in-class customer service, providing integrated local and global support for both our communications and IT application services.

We have two main subsidiaries: OnAir, which is the leading provider of in-flight connectivity, and CHAMP Cargosystems, the world’s only IT company dedicated solely to air cargo. We also operate two joint ventures providing services to the air transport community: Aviareto for aircraft asset management and CertiPath for secure electronic identity management.

In addition, we sponsor .aero, the Internet top level domain reserved exclusively for aviation.

We are one of world’s most international companies. Our global reach is based on local presence, with services for over 550 air transport industry members and 3,200 customers in over 200 countries and territories. Set up in 1949 with 11 member airlines, today we employ people of more than 140 nationalities, speaking over 70 different languages. SITA had consolidated revenues of US$1.49 billion (€1.07 billion) in 2009.

For further information go to www.sita.aero
Notes and references

Note 1, Page 4:  http://en.wikipedia.org/wiki/Shoe_bomb
Note 5, Page 4:  ACI Global Traffic Forecast 2008-2027
Note 7, Page 5:  The Airline IT Trends Survey 2010, conducted annually by Airline Business and SITA.
Note 11, Page 6:  ACI Global Traffic Forecast 2008-2027
Note 12, Page 6: Certipath is a cross-industry organization providing digital certificates and a PKI bridge to authenticate parts and maintenance work within the air transport industry supply chain. More information is available at www.certipath.org
Note 13, Page 8:  http://www.sarnoff.com/files/iris_on_the_move_brochure_0.pdf
Note 15, Page 9:  http://www.iata.org/pressroom/pr/Pages/2007-12-12-02.aspx
Specialists in air transport communications and IT solutions

For further information, please contact SITA by telephone or e-mail:

**East & Central Europe**
+41 22 747 6000  
info.ece@sita.aero

**Latin America & Caribbean**
+55 21 2111 5800  
info.lac@sita.aero

**Middle East & North Africa**
+961 1 637300  
info.mena@sita.aero

**North America**
+1 770 850 4500  
info.nam@sita.aero

**North Asia & Pacific**
+65 6545 3711  
info.nap@sita.aero

**North Europe & Sub-Sahara Africa**
+44 (0)20 8756 8000  
+27 11 5177000  
info.nesa@sita.aero

**South Asia & India**
+65 6545 3711  
info.sai@sita.aero

**South Europe**
+39 06 96511500  
info.seu@sita.aero