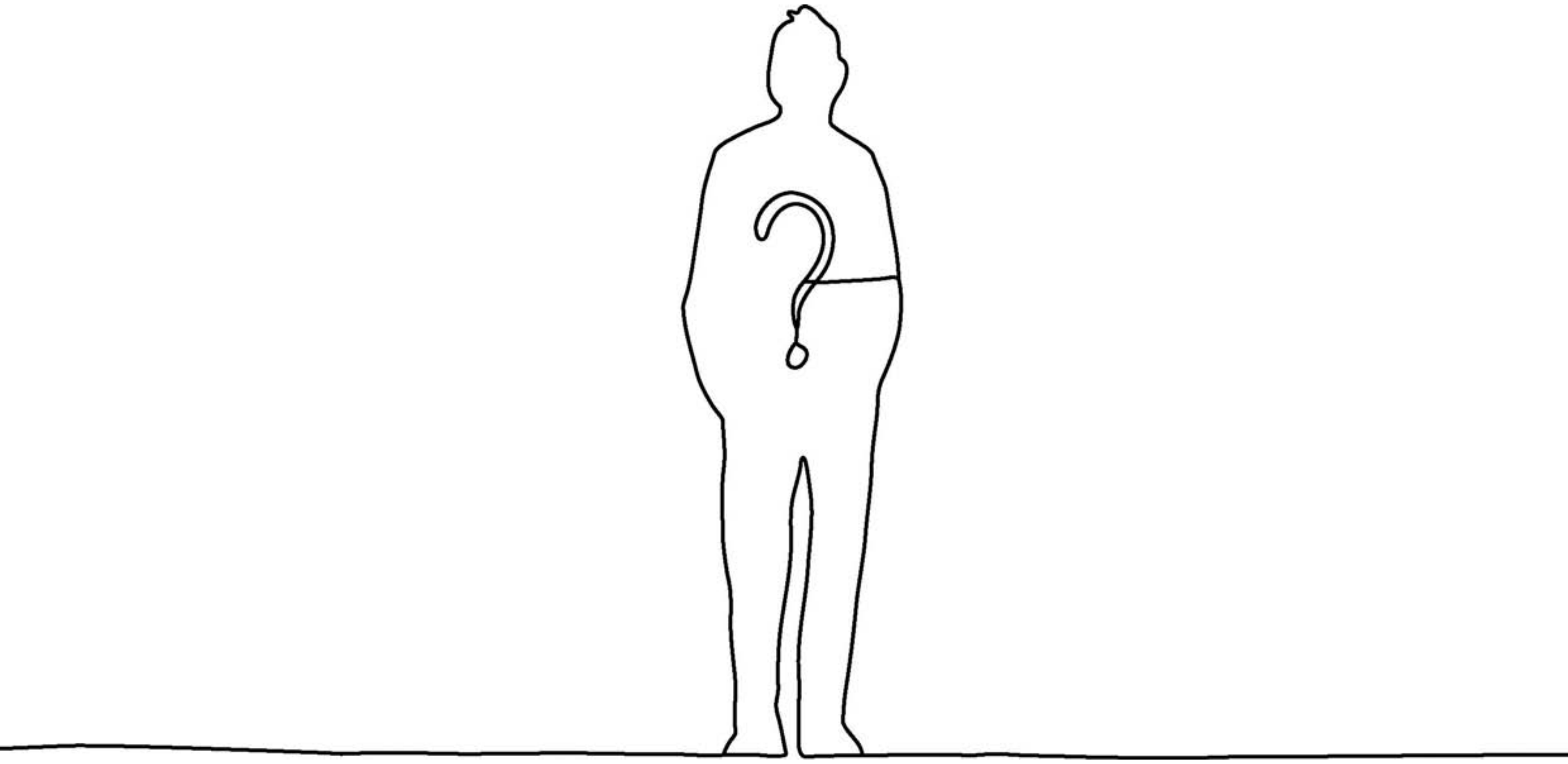


The future of transportation security

Passenger screening

SITA

Transportation security is a vital priority for governments, airlines and airports alike. Huge improvements have been made over the past five years, but an enormous amount remains to be done – not just in making transportation safer and more secure, but also to simplify passenger travel.

This year, some two billion passengers will take to the skies. Of these, only a small fraction will arrive without proper documentation (passport, visa etc.). Even fewer will be illegal immigrants, drug traffickers, terrorists or other criminals. The challenge for our industry remains a veritable balancing act: to strike the right balance between security and facilitation. Not an easy task. The principal challenge is to properly identify these very few 'persons of interest' among the multitudes of business and leisure travellers, and intervene before they can cause trouble.

Since 9/11, tens of billions of dollars have been invested in trying to ensure that a similar tragedy never happens again. Yet there is still much more to be done in further minimizing risks, while at the same time making passenger travel simpler and more straightforward – goals which the industry must achieve in the face of ever growing passenger numbers.

This will not come cheap – what price can be put on public safety and confidence? – so it's all the more important that stakeholders invest wisely in creating the safe, secure, travel and transportation industry of the future.

Where the industry is today

Security is a seriously expensive business. In the US alone, the government's 2007 budget provides a staggering US$ 58.3 billion – a US$ 3.4 billion, six percent increase over 2006 – to support the homeland security activities of 32 government agencies.[1]

Nearly US$ 5 billion of that is allocated to the Department of Homeland Security's aviation security work, including:

- US$ 3.2 billion for aviation screening operations;
- US$ 440 million for baggage screening devices;
- US$ 80 million for emerging technology at passenger checkpoints;
- US$ 700 million for the Federal Air Marshals programme; and
- US$ 40 million for Secure Flight, a passenger pre-screening programme.

Investments over the past few years have greatly improved transportation security around the world – from the introduction of reinforced cockpit doors, to enhanced passenger and baggage screening, to the effective implementation of new, tougher, security rules and regulations.

[1] Source: US President's 2007 budget, www.whitehouse.gov/omb/pdf/Homeland-07.pdf

Early efforts are also underway to make travel easier for passengers who are willing to undergo pre-screening through registered traveller programmes, and to introduce biometric technology into the travel process.

But in the face of a number of serious problems with security today, a great deal more needs to be done.

What challenges?

There are several main problem areas:

- Not enough global coordination or standards.
- Self-service deployment impacts on transportation security processes and responsibilities
- Biometric technology isn't yet standardized or widely available.
- Passenger screening is becoming a major cause of airport congestion.
- Security at the airport landside.

Global co-ordination

Throughout the industry, security requirements are increasing and regulatory requirements are changing rapidly, with more governments wanting more information about arriving and departing passengers from airlines. The problem today, however, is that many new developments are not being globally co-ordinated or supported by global standards or practices.

Self-service

Passengers who check-in online and print their own 2D bar-coded boarding passes also face new security issues. How can the authorities verify passengers' identities? With self-service, who's checking the validity of travel documents? Efficient deployment of off-airport check-in options will require coordination and approval from the local border control, security and airport authorities – and they will need to be able to inter-connect with airline systems to be able to check the validity of boarding passes.

Throughout the industry, security requirements are increasing and regulatory requirements are changing rapidly, with more governments wanting more information about arriving and departing passengers from airlines.

How can the authorities verify passengers' identities?

Biometrics

New technologies, such as biometric identification, offer the potential to not only improve security but also speed up passenger movement through airports. With the aid of biometric verification, passengers could also take advantage of other benefits, such as gaining rapid access to airline lounges, car parks etc.

Passenger screening

Passenger screening, while much improved, is also becoming a major cause of congestion at airports, with long lines now the norm both at immigration and security checkpoints. As passenger numbers grow, such problems can only get worse.

Landside security

Another problem is that while security airside at the airport, and on planes, has been greatly enhanced, there is still relatively little security landside. For the great majority, this is not a problem – we all like to be met or seen off by friends or family, and increasingly airports offer great retail space, even for non-travellers. But with increasing numbers of people landside, airports now present a major security risk in their own right: the combined volume of passengers checking in for four full-capacity flights aboard the new A380 (and modern airports have room for many more than that) would be larger than the number of people who died in New York on 9/11.

Where the industry needs to go

Increased security shouldn't need to mean longer queues and a less pleasant passenger experience. This is in all the stakeholders' interest:

- Governments, who might not worry about long queues per se, certainly want to present a good image of their country, and promote tourism;
- Airlines are constantly in search of faster aircraft turnaround, and hence quicker boarding processes;
- Airports would much prefer passengers to be shopping, eating or drinking, than standing in queues;
- Passengers want to avoid queuing wherever possible.

Indeed, the best security of all is the kind which passengers barely notice or don't even notice at all. What's needed, therefore, is a combination of smarter technology, more automation, better data processing, improved integration and more effective collaboration.

Almost anyone can get into an airport, and many people do, even if they're not intending to fly.

In terms of mitigating risk, the best way of finding these very few ‘persons of interest’ is to progressively make the target population smaller.

Airports shouldn’t look or feel like prisons; instead they should encourage the free flow of people, and make passengers feel that flying is once again an enjoyable experience. Passengers’ main priority is to be able to move effortlessly through the airport and onto the aircraft, and while everyone accepts the need for increased security and screening, nobody wants to wait in line if they can possibly avoid it.

Where possible, and within the constraints of security needs, the industry should therefore be working towards achieving simplified passenger travel at every step of the journey.

In terms of mitigating risk, the best way of finding these very few ‘persons of interest’ is to progressively make the target population smaller. By using a layered approach to security, with each layer further reducing the risks, the transportation industry can become ever-more secure.

Enhanced security can be achieved with less impact on passengers, rather than more. A good example is explosive detection in shoes. With the smart application of modern technology – for example under-floor detection systems – passengers really shouldn’t need to take their shoes off. Detection should happen automatically and transparently to the passenger, while checking-in at a kiosk, walking down a jetway to the aircraft or as an integral part of the security screening process.

Airports shouldn’t look or feel like prisons.

In the same way, passengers shouldn’t really need boarding passes. Instead, governments, airports and airlines should be able to ‘recognize’ valid travellers, since the right to fly depends ultimately not on a piece of paper, but on data in airline and airport systems and on the passenger’s eligibility and physical presence in the right place at the right time. Once a reservation has been made, the passenger should simply be able to show up at the airport, prove his or her identity, and be granted access to the plane – assuming he or she has the right to fly that day; and assuming that he or she can be constantly updated with key information such as flight number, boarding gate, seat allocation, departure time, etc.

Among other things, this is likely to mean:

- Smarter technology, systems and processes than we have in place today;
- Robust, reliable, machine-readable travel documents;
- More stealth screening – for example by closed-circuit television (CCTV), through sensors built into turnstile doors, gates and checkpoints, and through the use of measuring /detection systems underfoot.

This will help security know, at every stage, for each and every person, who they are and where they’re going; landside, airside and onto the aircraft.

Security processes will also need to become performance-based, rather than prescriptive. Screening, for example, needs to be defined not by the screening process itself but by the desired passenger throughput. If today’s systems lead to unacceptably long queues, they will need to be rethought, and if necessary replaced by smarter, more efficient systems.

So how can we create a more secure, safer, travel and transportation industry?

How are we going to get there?

The simple answer to the question is by investing time and resources effectively. Governments, airports and airlines will need to work together to implement smaller, smarter technology, and to use time and space at the airport intelligently.

That’s already a challenging task, but they will have to do all of this while respecting individuals’ privacy as well as taking into account local constraints, requirements, obligations and regulations.

The longer answer is that a multi-layered response will be needed to drive process change, mitigating risk further with each security ‘layer’. Each of the following steps will make the target population smaller, and the few persons of interest easier to find:

- Regulation and legislation
- Technology and systems
- Processes
- People

Governments, airports and airlines will need to work together to implement smaller, smarter technology, and to use time and space at the airport intelligently.

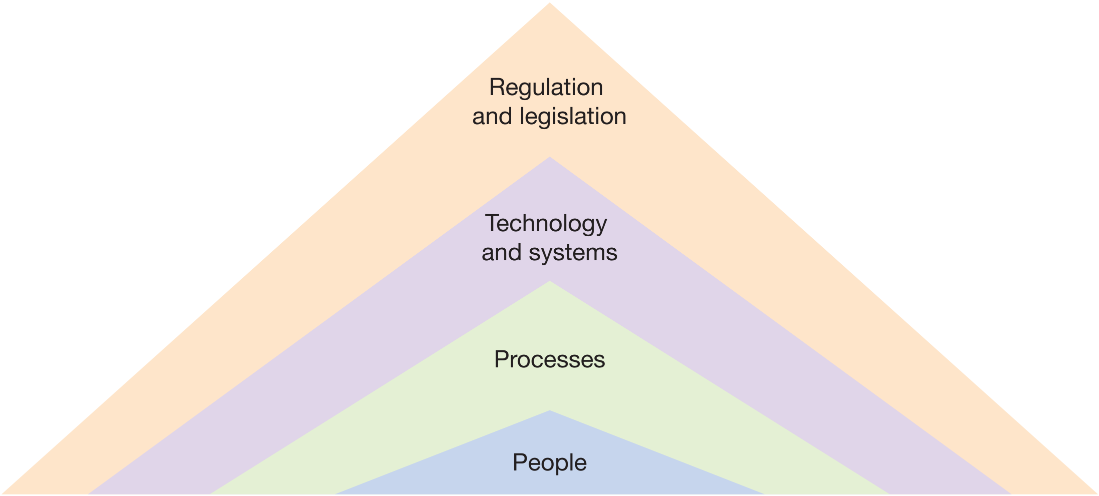


Diagram: A multi-layered approach to risk management

Regulation and legislation

For security to be most effective, governments will need to coordinate their transportation security regulation and legislation closely with one another – and with international bodies such as ICAO, IATA, Interpol and the World Customs Organization (WCO). They will also need to collaborate in order to achieve national and international harmonization and avoid costly duplication of effort and/or incompatibilities between systems and processes.

A good example of effective coordination is the work carried out under ICAO's leadership in helping to specify internationally-agreed standards for machine readable passports. These will be issued across all 188 ICAO member states by 2010,[2] and will pave the way for the next generation of fully secure biometric passports.

The strong interdependence between transportation industry stakeholders also means that close collaboration is needed between airlines, airports, ground handlers, immigration, security, intelligence, customs and quarantine, as well as with technology companies and security contractors, all of whom have a strong interest in 'passenger identity'.

Co-ordination between document-issuing authorities and between government authorities and Interpol is also essential, in order to ensure access is available to the most up-to-date watch-lists and prevent undesirables from crossing borders wherever possible. The passenger's 'right-to-fly' and the airline's 'authority-to-carry' both need to be well-established before the passenger actually boards the plane.

To be genuinely useful, policies and practices will need to be flexible and modifiable. As circumstances evolve, they will also need to be adaptive.

[2] For more information on ICAO and machine-readable travel documents see www.icao.int/mrtd.

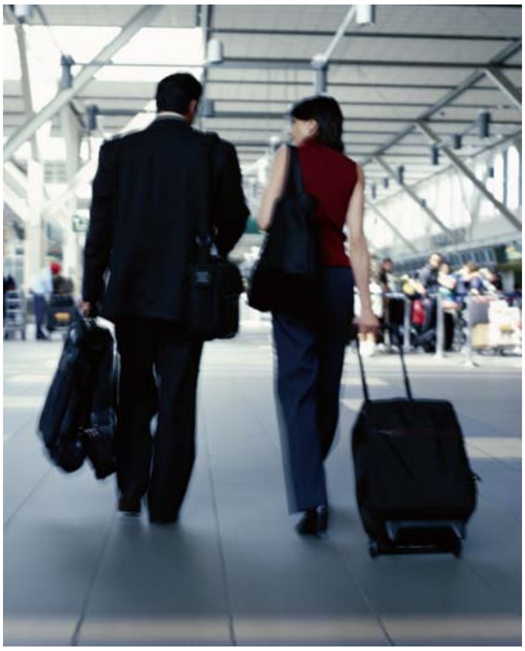
Technology and systems

Moving forwards over the coming years, technology – already a powerful enabler in security systems – will play an ever-increasing role. In particular, new advances in scanning and detection technology will help protect not just aircraft and the airside part of the airport, but the landside area as well, making the airport as a whole more secure.

A good example is passive millimetre wave (PMMW) systems, which have the ability to penetrate clothing and can therefore be used to detect concealed objects such as guns or knives – which means you won't have to take off your coat, let alone your shoes.

We can already consider that PMMW systems could be installed as part of the revolving doors at an airport's entrance, with the option of immobilizing the door if a weapon-carrying person is detected, thus arresting the suspect and protecting other airport users.

The same revolving door could also be used to implement the latest explosive-detection systems, which use an upwards puff of air over a moving body and detectors in the ceiling to register the presence of even tiny amounts – just 20 nanogrammes – of Group A (TNT, TNB, etc.) or Group B (Semtex H, RDX, C4, etc.) explosive, as well as many improvised explosives, in a matter of two or three seconds.



It's important to remember, however, that safeguards must be built into these systems to ensure that cleared personnel (military, police or security, for example) don't get caught in revolving doors – when it may be quite legitimate for them to be carrying arms, and who may be bearing traces of explosive as part of the normal course of their work.

Such new scanning and detection technologies have the advantage that not only do they greatly enhance security, but they do so without inconveniencing travellers: the scanning and detection process can now be entirely transparent to them – which is great for the innocent majority, yet helps to catch the guilty few. They also mean that the landside area of airports can now benefit from the same or even better levels of security as airside areas.

New technologies not only enhance security but do so without inconveniencing travellers. Scanning technology within the airport also needs to get a good deal smarter than today's X-ray machines, which only detect dense objects in baggage, such as metal and improvised explosive devices.

New machines also need to be able to 'see' plastics, as well as biological, chemical and radiological hazards, and materials such as fuel that have the potential to explode or catch fire. Today, a bottle of petrol in hand baggage looks much the same to an X-ray machine as a bottle of water. PMMW systems and new explosive detection technologies are at least part of the answer.

Another useful technology will be under-floor detection systems (placed at the end of escalators, for example, or in front of screening machines) which can be used to perform an explosive check on shoes – and again, without the traveller necessarily being aware of the process.

Automation will speed up the progress of passengers through the airport. It will also, however, require technologies such as 'single-person detection' (ie did only one person go through at a time?) and 'no left object' detection (to prevent dangerous or hazardous objects being left behind) at gates, turnstiles and rotating doors.

Transportation security will also be greatly improved when fully-biometric enabled travel documents (comprising iris, finger or 3D face scans) become ubiquitous, though for this to be the case, scanners and readers will need to become much more accurate than they are today.

Finally, airport facilities will have to get smarter, too, with built-in security. Panels, or cisterns, for example, should be wired, to ensure nobody tampers with them, or uses them as a place to conceal illicit or dangerous items – such as components of an explosive device, or a gun.

Processes

With regulation and legislation harmonized, and the right technology and systems in place, the next logical step in mitigating security risks is to establish the right security processes.

A simple example for airports which do not operate 24/7, would be to establish a daily clean sweep policy. This can be performed at night, while the airport is closed for business, and ensures that the environment is completely sterile at the beginning of each new day.

More complex processes are needed not just to gather all the data coming through an airport but also to validate, analyze and interpret it. A good example is each traveller's 'personal authority to fly', which needs to be validated at each of the following points:

- Check-in
- Border control
- Security
- Departure gate

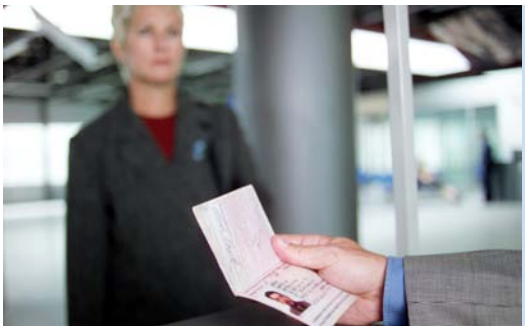
This is not a simple task, as each step can require multiple verification and feedback loops. Imagine a British woman with a biometric passport leaving the UK to go to Hong Kong via Dubai. She may be cleared by British immigration and security to leave the country, and by the airline to board the plane, but what if Dubai isn't happy for her to transit because she's on a watch-list or previously had a visa overstay? Or what if Dubai is happy for her to transit, but she has been refused a visa for Hong Kong?

Information needs to be passed not just forwards but backwards, in real-time, so the passenger can be denied boarding in spite of being cleared by local immigration, customs and the airline.

This already happens when you fly to countries like Australia, Bahrain and New Zealand, and the practice will become a great deal more widespread in the coming years.

Once fully-biometric enabled travel documents are commonplace – some time after 2010 – it will become possible to know, on a passenger by passenger basis, who is arriving, departing, or transiting through an airport. Being certain about people's identity will also enable faster throughput for specific groups of recognized passengers – such as nationals, frequent flyers or registered travellers – who will be able to benefit from separate channels at immigration, for example, or self-boarding through automatic turnstiles at the departure gate.

The departure gate, in fact, is the ideal place for final screening, as the jet way is a contained area, through which passengers must transit, and it allows for the detection of any weapon, explosive or chemical device which might have been assembled after other security checks have taken place.



Information needs to be passed not just forwards but backwards, in real-time, so the passenger can be denied boarding in spite of being cleared by local immigration, customs and the airline.

Scanners and readers will need to become much more accurate than they are today.

This is an important issue. It's relatively easy to detect an explosive device or a gun through the use of normal scanning and detection systems, but how do you detect the 35 separate pieces of a bomb being carried by 35 separate people which can then be assembled pre-flight? Controls of individuals on their own are not enough – the whole picture needs to be examined.

Closed Circuit Television (CCTV) has already done a great deal to improve security. The suspected bombers from the failed attack in London on 21 July 2005, for example, managed to escape from the scenes, but were later arrested with the help of CCTV footage and archived images. It would have been much better still, of course, if they had not been able to bring bombs onto the public transport system in the first place.

Real-time analysis

What would be needed therefore – though it will be a big, complex task to implement – is not just CCTV, but smart, real-time analysis of the situation at each control and checkpoint. This should be linked closely to databases and should draw on powerful data coordination and data mining applications able to quickly trawl through broad data sets looking for patterns, commonality and anomalies.

The ability to perform this kind of real-time analysis would be a huge step forward for transportation security. Everything about a passenger might seem in order, for example, but what if the credit card used to make the booking was the same card used to book a flight for someone with a visa overstay? What if their ticket was issued by a travel agent with links to known smugglers? What if they are in some way connected with a person previously denied boarding – through the same car rental, hotel, or conference participation? Smart analysis of the whole data set can help assign different risk levels to different passengers, and improve overall transportation security. And any such practice would need to be fully compliant with data protection laws and an individual's privacy rights.

Staff and aircraft crews matter too

It's also important that security processes take airport staff and aircraft crews into account. As with passengers, the overwhelming majority of personnel are absolutely no cause for concern, but with special access privileges, staff also need special security processes.

One obvious precaution is to ensure that everything related to staff movements is automatically logged in un-editable records. Another is to check all anomalies. If a staff member shows up for work three hours early it may be entirely innocent, but you still want to know the reason why.

No matter how smart technology is, or how automated processes become, humans will still be not only involved but essential in detecting suspicious behaviour and persons of interest.

Different clearance levels also need to be applied to different areas of the airport, too – access to the baggage handling area may require different security checks to access to the apron, the control tower or the fuel supply.

People

The last – and perhaps most important – element in improving transportation security is the human factor.

No matter how smart technology is, or how automated processes become, humans will still be not only involved but essential in detecting suspicious behaviour and persons of interest. By their very nature, humans are particularly good at spotting anomalous or suspicious behaviour in other people.

It makes sense, for example, to question a passenger who changes queue three times at immigration, or someone who seems to be spending an unusual amount of time in a car park.

Equally, you would want staff to pull aside anyone travelling with a gas mask in their hand baggage, even if it wasn't on the list of prohibited items.

Key to security in the industry is therefore ensuring that staff are highly-trained – preferably intelligence-trained – and properly rewarded. Indeed, if transportation is to become safer and more secure then the whole security function needs to become more professionalized. If security staff are poorly-trained or lowly-paid then it's hardly surprising on the one hand if they're open to corruption, abuse or disaffection, and on the other if they're not very good at their job.

Human factors also need to be applied to staff in and around the airport. Should three people with access to the fuel supply all be allowed to fly from the same airport on the same day, for example? Even if they're only going on holiday?

Staff need to be highly-trained and properly rewarded.

Security will also be enhanced by a more standardized approach to background checks and screening of airport staff – if data capture about staff members were harmonized, then it would be much easier to check and verify individuals at the national level.

Conclusion

To sum up, a safer, more secure transportation industry will depend on a multi-layered approach to progressively mitigate risk. As we have discussed, the crucial elements here are coordinated regulation and legislation; smaller, smarter technology and systems; improved processes; and capitalizing on skilled human resources.

Improved security will also depend on all the available data in airline and airport systems being coordinated in real-time, so that passengers' individual 'personal authority to fly' can be validated. At the same time, concerns about privacy and data sharing must be respected, with inappropriate data – such as political, medical or religious information – remaining confidential.

If these elements can be brought successfully together, then we can look forward to a travel and transportation environment where passengers not only feel more secure but also regain some of the sense of fun and adventure which used to be associated with air travel.

SITA and transportation security

With our unique knowledge and experience we help government and industry work together to enhance transportation security. We actively participate in the industry forums that define how nations' borders will be managed in the future. We deliver the applications, infrastructure and networking capabilities which make it all possible. It's as straightforward as that.

SITA

SITA is the world's leading service provider of IT business solutions and communications services to the air transport industry. SITA manages complex communication solutions for its air transport, government and GDS customers over the world's most extensive communication network, complemented by consultancy in the design, deployment and integration of communication services. SITA also provides market-leading common use services to airports and air-to-ground communications to airlines. We deliver a comprehensive portfolio of e-commerce solutions for airlines and are pioneering new technologies in areas such as in-flight passenger communications and transportation security. Motivated by industry concern for lower costs, asset optimization and an improved passenger experience, we aim to simplify travel and transportation removing complexity and improving our customers' operational performance.

SITA has two main subsidiaries: OnAir, which is leading the race to bring in-flight mobile telephony to the market, and CHAMP Cargosystems, the world's only IT company solely dedicated to air cargo. SITA also operates two joint ventures providing services to the air transport community: Aviareto for aircraft asset management and CertiPath for secure electronic identity management and the company sponsors the Internet's top level domain reserved exclusively for aviation – .aero.

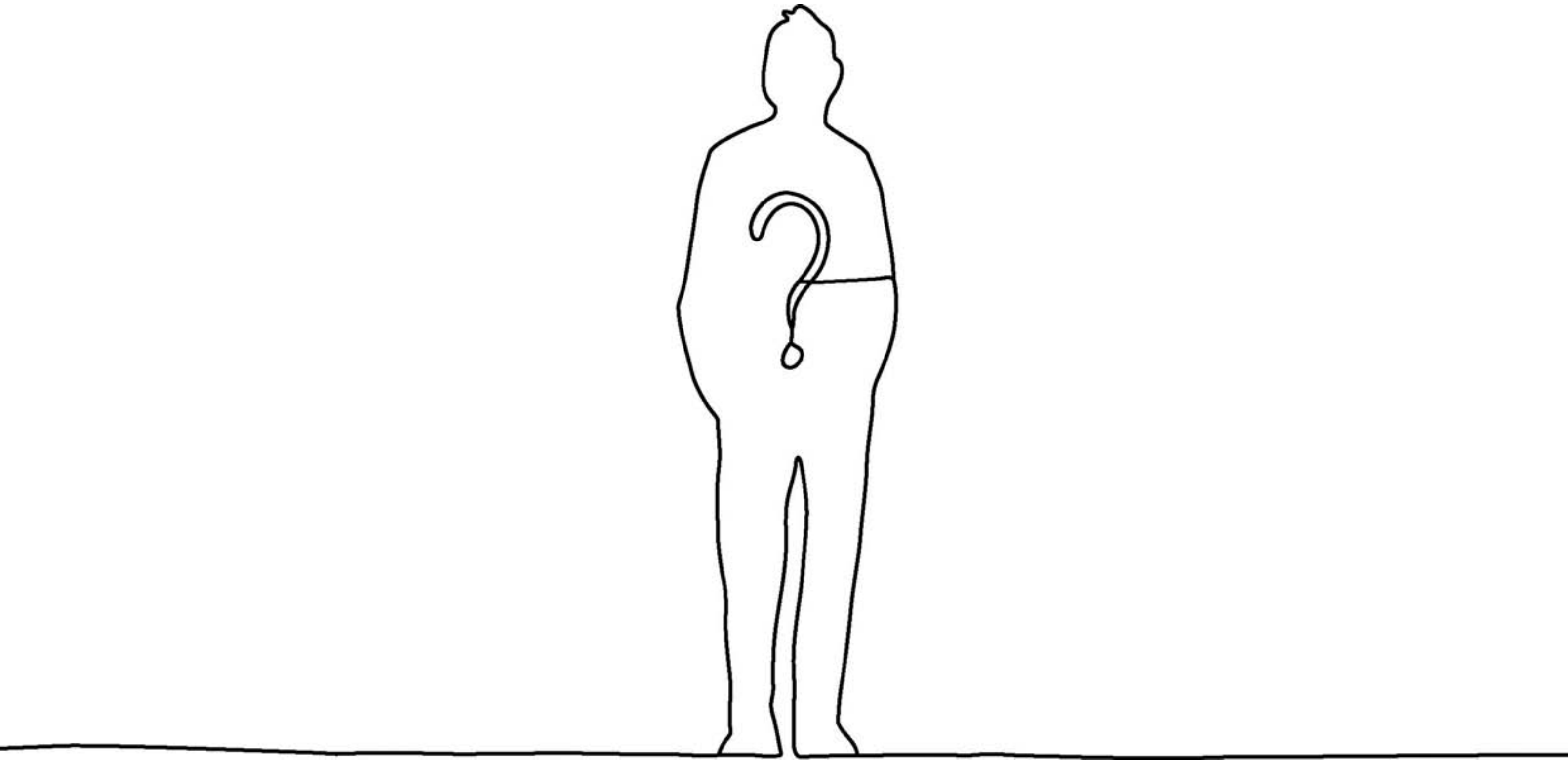
Across the globe, SITA employs people of more than 140 nationalities, proficient in over 70 languages, and covers 220 countries and territories. With its main office in Geneva, Switzerland, SITA had aggregated revenues of US$ 1.554 billion in 2005 (€1.295 billion).

To find out how SITA is helping to enhance transportation security, visit us at www.sita.aero/security or send e-mail to transportation.security@sita.aero.

Notes

Notes

Notes



For further information, please contact SITA:

Americas
3100 Cumberland Boulevard,
Suite 200, Atlanta, GA 30339,
USA
tel: +1 770 850 4500
fax: +1 770 612 2265
e-mail: info.americas@sita.aero

Asia Pacific
11 Loyang Way, Singapore
508723, Republic of Singapore
tel: +65 6545 3711
fax: +65 6548 2730
e-mail: info.asiapacific@sita.aero

Europe
Capital Place, 120 Bath Road,
Hayes, Middlesex UB3 5AN,
United Kingdom
tel: +44 (0)20 8476 4500
fax: +44 (0)20 8730 1337
e-mail: info.eumea@sita.aero

Middle East and Africa
Bachoura, Khandak El-Ghamik,
Daoud Ammoun Street, SITA
building, P.O. Box 11-6524,
Beirut, Lebanon
tel: +961 (1) 657200
fax: +961 (1) 655951
e-mail: info.mea@sita.aero

www.sita.aero

This literature provides outline information only and (unless specifically agreed to the contrary by SITA in writing) is not part of any order or contract.