

▶ A BUNDESDRUCKEREI  
POCKET GUIDE TO  
BORDER CONTROL

[www.bundesdruckerei.de](http://www.bundesdruckerei.de)



▶ A BUNESDRUCKEREI  
POCKET GUIDE TO  
BORDER CONTROL

**Published by**

Bundesdruckerei GmbH  
 Oranienstrasse 91,  
 10969 Berlin, Germany  
 www.bundesdruckerei.de

**Project Management**

Krowne Communications GmbH  
 Schlüterstrasse 37, 10629 Berlin, Germany  
 www.krowne.de

**Copyright**

© 2007 Bundesdruckerei GmbH  
 No reprinting of this document is allowed.

Introduction. ....	10
CHAPTER ONE – FRAMEWORK CONDITIONS FOR CONTROLLED BORDER CROSSING	
<hr/>	
1.1 Multi-tasking essential .....	11
1.1.i Facilitating entry. ....	11
1.1.ii Why are you here? .....	12
1.1.iii Exit barred – preventing entry. ....	13
1.1.iv Documentation of immigration. ....	13
1.1.v Beyond documents. ....	14
1.2 Conventions and agreements .....	15
1.2.i Schengen Convention. ....	15
1.2.ii Schengen Information System (SIS) .....	17
1.2.iii Visa Information System (VIS) .....	17
1.2.iv US Enhanced Border Security and Visa Entry Reform Act .....	18
1.2.v Bilateral agreements .....	19
1.3 Emerging trends .....	19
1.3.i Growing traveller numbers .....	19
1.3.ii Bigger aircraft. ....	20
1.3.iii ePassports .....	21
1.3.iv Flows of migrants .....	21
1.3.v Illegal immigration, human trafficking and ID document fraud .....	21
1.3.vi International terrorism. ....	22
1.4 Requirements for future border control .....	23
1.4.i System interoperability .....	23
1.4.ii Increasing throughput .....	23
1.4.iii Biometric verification and identification of travellers. ...	23
1.5 Action alternatives for border control .....	24
1.5.i Process automation .....	25
1.5.ii New strategies .....	26
1.5.iii Recycling data. ....	26
1.5.iv Simplifying immigration. ....	27
1.5.v New technologies. ....	27
1.5.vi Speed is essential .....	28

CHAPTER TWO – BUNDESDRUCKEREI: A SOLUTION FOR EVERY REQUIREMENT

---

2.1	Process management software .....	29
2.2	Document control .....	30
2.2.i	Optical authentication .....	30
2.2.ii	Electronic authentication .....	31
2.2.iii	BAC .....	31
2.2.iv	EAC .....	31
2.2.v	PKI .....	33
2.2.vi	Database queries .....	33
2.3	Control of individuals – a face to the future .....	34
2.3.i	Building on experience .....	35
2.3.ii	It's your choice .....	35
2.3.iii	Biometrics at border control .....	35
2.3.iv	Quality is the key .....	36
2.4	Integration of visa issuance into the border control chain .....	36
2.4.i	Visas come in many shapes and sizes .....	37
2.4.ii	Establishing a connection between the visa and its holder .....	39
2.4.iii	Joined-up thinking .....	39
2.4.iv	Optimising border control .....	40
2.5	Exit-entry system .....	40
2.6	Implementation scenarios at the point of entry .....	42
2.6.1	Staffed process .....	43
2.6.2	Separated process .....	45
2.6.3	Automated process .....	46
2.6.4	Mobile control .....	49

CHAPTER THREE – INTEGRATION

---

3.0	Choosing an integrator .....	50
3.1	Responsibilities .....	50
3.2	Defining the system .....	50
3.3	Supply and installation of the system .....	51
3.4	Project implementation .....	51
3.5	Fitting the project together .....	51
3.6	Establish realistic plans .....	52
3.7	Training and support .....	53

CHAPTER FOUR – GLOSSARY

---

**Move forward**

In our increasingly globalised world, the number of travellers is constantly expanding. Growing wealth, new markets and global connectedness are boosting business and private travel across international borders.

At the same time, there has been an increase in the incidence of security threats, such as illegal immigration, organised crime and international terrorism. Many recent incidents could have been prevented at borders in advance with the help of intelligent border control systems.

In the future many horizontal processes that are currently operated manually will be automated. Furthermore, the integration and cross-linkage of applications will enable efficient processes without disruptions. These developments are supported by innovative databases and self-service applications.

**Your documents, please**

This macro environment supports the market success story of innovative security technologies, such as biometrics, smart cards and Radio Frequency Identification (RFID), which enable new security applications and the optimisation of complex processes.

By 2010, more than 40 countries will have introduced the electronic passport (ePassport), covering around 50% of the world's population. Unsurprisingly, the first nations to adopt ePassports are those whose citizens travel the most.

Electronic travel documents facilitate innovative automation concepts and enable integrated security processes at borders that rely on machine-assisted control. Border authorities have already started to evaluate the potential of machine-assisted and automated self-service border control solutions. However, controlled border crossing is more than simply a case of implementing trusted self-service checkpoints for registered travellers.

This document focuses on the point of entry only. Border surveillance is not part of our consideration.

**1.1 MULTI-TASKING ESSENTIAL**

Today's border police have a surprisingly broad job description. In many countries it is now no longer a case of them having simply to permit travellers to cross the border – or prevent them from doing so. Instead, officials may need to examine a multitude of documents, compare a traveller's details against a watch-list of suspected criminals or terrorists, prevent the entry of certain individuals, document the entry of others, and carry out numerous security checks ranging from screening hand luggage and individuals to checking luggage security. And, although border police have a different function from customs officials, the two groups must often liaise to ensure that a joined-up approach to border management is achieved.

Primary border control includes three core activities: Document authentication, verification, and identification of data and the individual.

**1.1.i Facilitating entry**

One of the most obvious tasks border police have to carry out is enabling authorised travellers to enter a country. Although their methods may have changed from the days of writing out the names and contact details of passengers on a border entry list, the task is basically the same. Today's officials grant entry to travellers based on strict requirements set out in a country's national immigration law as well as any supranational regulations that it may be a signatory to. Moreover, officials increasingly have to use technology to facilitate immigration.

Permitting entry to a country may require either a manual or an automated examination of a traveller's documents. Officials need to be aware of the wide range of documents that are permitted for gaining entry to a country. The most obvious is the passport, which includes a traveller's personal information as well as data about the document's validity. Another type of document frequently used by citizens travelling across regional borders is the national ID card.

In addition to the national document issued by a traveller's home country, some individuals will only be permitted to enter a state if they also have a visa. A visa sets out certain rules for a traveller's stay in a country, including:

- ▶ The purpose of the visa holder's journey;
- ▶ How long the visa holder is permitted to stay in the country;
- ▶ The latest date the visa holder can enter the country.

Depending on a country's regulations – and the type of visa required – a visa may have to be obtained before reaching a border checkpoint, or it may be granted by an official at a border.

The US have already started to enhance visa procedures by enrolling, storing and querying biometric data of visa applicants. In the European Union, the introduction of biometric technologies to the visa issuance process will start soon. Both the US and the EU seek to enhance interagency cooperation by sharing information such as biometric or biographic data of applicants.

If a traveller is arriving at a country's land border by his or her own car, border officials may additionally need to see documentation related to the ownership of the vehicle.

Of course, requirements at land, air and sea borders may differ from each other.

#### **1.1.ii Why are you here?**

Travellers enter a country for a variety of reasons, so – assuming all documentation is in order – border officials need to facilitate a number of different types of entry. For example, some travellers may wish to enter a country for a limited period of a few days, weeks or months. Others may simply be entering for several hours because they are in transit to another destination. And others may wish to emigrate to the country. Individuals who are in transit need to be processed quickly to cause them minimum inconvenience and to disrupt the border control area as little as possible.

Depending on a traveller's country of entry – and origin – those entering for a limited period may be asked a selection of questions to establish their motives for travelling.

Such questions could include:

- ▶ Why are you visiting this country?
- ▶ Where will you be staying?
- ▶ Who will you be visiting?
- ▶ How long do you intend to remain here?

Individuals wishing to enter a country for immigration purposes will be subjected to a more thorough examination of their travel documents. They will also need to be formally interviewed and will be required to show evidence that backs up their application to enter the country. For those seeking refugee or asylum status this would include evidence to back up their claim for having fled and being unable to return to their country due to a well-founded fear of persecution, war or civil conflict. Economic or lifestyle migrants would have to provide proof that they were financially able to support themselves.

#### **1.1.iii Exit barred – preventing entry**

Border officials must also follow well-documented procedures, as set out by the country whose borders they are protecting, to prevent the entry of individuals considered to be a threat to the interests of the country. Preventing entry is a comprehensive task, because of the different requirements at air, land and sea borders, and may include the use of a range of devices, from radar stations and fences to mobile control units. At official points of entry, biometric technology may come into play, with officials being required to take a biometric sample of a traveller and compare it with a database or watch-list of potential criminals. Individuals barred from entering a country could include – but will not be limited to – those who are suspected of entering the country to engage in terrorist, subversive or criminal activities; individuals who the authorities believe will be unable to support themselves and will not be able to provide any economic benefit to the country they are visiting; and those who have previously visited the country but violated the terms of their visa.

#### **1.1.iv Documentation of immigration**

Border control officials must document the movement of all travellers entering the country. Considering the challenges described above, establishing appropriate entry-exit documentation becomes an important task for border authorities. Where the latest border control technology is being used,

an official may scan the details of the passport and the immigration card and store it into a border control system. In such instances, not only do border control staff visually examine the passport for signs of obvious tampering or forgery, they also use passport readers to read the Machine Readable Zone (MRZ) in the document. Some countries even authenticate the security features using latest imaging and pattern recognition technology. Yet only few countries have empowered their border authorities to read ePassport chips.

### 1.1.v Beyond documents

Having examined a traveller's credentials, border police must also carry out a number of security checks on the individual. These could include searching the traveller and his or her luggage for explosives or prohibited weapons, such as knives, guns and ammunition.

Both border police and customs officials play a role in areas such as counter-terrorism, detecting and preventing the smuggling of narcotics and the trafficking of humans, as well as facilitating travel and tourism. Detection of hazardous materials, such as radioactive, biological and chemical substances will also become more important in future. However, in many countries there is a big difference between what border police and what customs officials will be searching for. As the World Customs Organization (WCO) highlights, the role of customs officials is to:

- ▶ Protect revenue;
- ▶ Protect security through prohibitions and restrictions;
- ▶ Identify and prohibit illegitimate trade;
- ▶ Maintain trade statistics.

All countries must have an effective system for capturing any immigration and customs data that is collected by officials. This means establishing and maintaining cooperation between all the parties involved in entry and exit controls, monitoring the length of stay, issuing visas and intelligence gathering.

With inter-agency coordination a priority, some governments believe the merger of customs and immigration departments result in better information sharing and improved efficiency. Enhanced intra-agency cooperation is now one of the focal points of governmental integrated border management approaches worldwide.

Integrated border management can be divided into two categories:

- (1) Domestic integration between government agencies within one country or customs union; and
- (2) International integration between neighbouring countries.

Both require inter-agency cooperation, parallel processing, and coordination at land, air and sea border points of entry so that border control is as efficient as possible. This also brings into the loop agencies that traditionally only work within one country.

In future, border control will integrate all authorities and agencies that can contribute to a more secure border control process. Of course, this requires enhanced communication and decision models as well as the technical means for cooperation.

## 1.2 CONVENTIONS AND AGREEMENTS

All nations are signatories to a number of international, regional or supranational conventions governing border security and immigration. Such conventions are usually designed to ease travellers and/or goods through borders as quickly and as conveniently as possible, while at the same time ensuring a high level of security is maintained. Because of the growth in the number of travellers – as well as changes in the macro environment – governments are under constant political pressure to handle entrants to their country in a way that stands up to international scrutiny. This chapter examines some of the framework conditions that governments have signed up to.

### 1.2.i Schengen Convention

For many European governments, the Schengen Convention is one of the most important principles governing travel in Europe. The concept of free movement within the European Union (EU) through the abolition of internal borders and the creation of a single EU external frontier was first set out by the Schengen Agreement in 1985. The subsequent Schengen Convention, in 1995, abolished controls on internal borders between signatory countries. The Amsterdam Treaty on the European Union, which came into force on 1 May 1999,

incorporated the set of measures adopted under the Schengen umbrella into the EU's legal and institutional framework (see box 1).

Schengen Convention measures are now fully accepted by 13 EU member states, as well as other non-EU countries (Norway, Iceland and Switzerland).

The Schengen Convention has meant that Schengen countries have had to change their immigration processes to fall in line with other member countries – a lengthy process which requires clear direction. For Schengen principles to be achieved, participating countries must coordinate their external controls and create a unified immigration policy, because an individual acceptable to one country but not to another can still enter both if one of them admits the individual. Every country intending to join Schengen must also have its preparedness assessed in three key areas: borders, visas and police cooperation. This is one of the major reasons for the establishment of the Schengen Information System II (SIS II, see below).

Although border controls have been abolished in the Schengen area, the member states have adopted the idea of flexible controls within their territories. In fact, in central Europe there will soon be countries without a controlled land border.

This development creates new challenges, because governments now need mobile and flexible devices to handle entry into – and movement within – the Schengen zone.

#### **Key rules adopted by Schengen members:**

- ▶ *Removal of checks on individuals at common EU internal borders;*
- ▶ *Unified set of rules applying to people crossing EU external frontiers, regardless of the EU country in which that external frontier is situated;*
- ▶ *Separation at air terminals and seaports of individuals travelling within the Schengen zone from those arriving from outside the area;*
- ▶ *Harmonisation of the rules regarding conditions of entry and visas for short stays;*

- ▶ *Coordination between governments on border surveillance;*
- ▶ *Definition of the role of carriers in preventing illegal immigration;*
- ▶ *Enhanced police cooperation;*
- ▶ *Faster extradition system;*
- ▶ *Creation of the Schengen Information system (SIS);*
- ▶ *Creation of the Visa Information System (VIS).*

#### ▶ *Box 1*

##### **1.2.ii Schengen Information System (SIS)**

The Schengen Convention includes an agreement to share information about people via the SIS. This is a secure governmental database established to enable police forces and security agencies from the Schengen zone to access data on specific individuals as well as on goods which have been lost or stolen.

The second generation of the system, SIS II is being established to allow more types of personal information to be stored on the database. The storage and processing of biometric identifiers and images is still being debated in the EU. The system will also provide law enforcement and administrative agencies, such as the judicial authorities and the security services of member states, e.g. Europol and Eurojust, with greater access to this information. SIS II is an important prerequisite for the entry of the new EU member states to the Schengen convention and the abolition of internal borders.

##### **1.2.iii Visa Information System (VIS)**

In 2004, the European Justice and Home Affairs Council agreed guidelines for the development of the VIS. This is being set up to enable the exchange of Schengen uniform visa data and 'national' visa information between those member states that have abolished border checks. According to the European Commission the objective of the VIS is "to facilitate the fight against fraud, to contribute to the prevention of 'visa shopping', to improve visa consultation, to facilitate identifications for the application of the Dublin II regulation [a regulation that determines which member state is responsible for an asylum application] and return procedures, to improve the administration of the common visa policy and to contribute towards internal security and combating terrorism."

The VIS will have a major impact on procedures at Schengen member consulates. For example, during the application process 10 fingerprints of each visa applicant will be recorded, which will be stored with the holder's facial image in the database.

SIS II and VIS will also change the way visa holders are checked at border control points. Both systems require visa holders to present their credentials when requested by consular officials and border police. This means tight inter-authority cooperation and secure, integrated processes at consulates and borders are key to ensuring the integrity of border control. Consequently, processes at consulates and borders have started to merge.

#### **1.2.iv US Enhanced Border Security and Visa Entry Reform Act**

The US Enhanced Border Security and Visa Entry Reform Act of 2002 was one of the measures passed in response to the tragic events of 9/11. Initially, the act required all 27 Visa Waiver Program (VWP) countries to begin issuing electronic passports including biometric identifiers from 26 October 2004. When it became obvious that this deadline was not going to be met, it was extended for another year. When this, too, looked unachievable, the deadline was extended until 26 October 2006.

In addition to the changes for VWP members, the act also required US consular posts to capture biometric data of visa applicants, store it in databases and issue visas linked to these biometric identifiers. The act has also been the legal base for the establishment of a biometric entry-exit system known as US VISIT, which integrates all border control points and allows matching of biometric live data with electronic passports, visas and other databases.

In another move, aimed at beefing up security, US public authorities are requiring private institutions to participate in selected steps of the control process. For example, airlines must send each traveller's Automated Passenger Information (API) data to the US a maximum of 15 minutes after boarding the plane. Moreover, the US authorities can claim access to the Passenger Name Record (PNR), which is stored in the airline's system (see glossary for further information).

#### **1.2.v Bilateral agreements**

It is not unusual for countries that have a particularly strong geographical, economic or diplomatic tie to establish bilateral agreements to help facilitate the movement of goods and people, stimulate their economies or address challenges to the macro environment.

#### **1.3 Emerging trends**

The challenge of controlling a country's borders effectively is greater than ever. Somehow, governments must meet this challenge of improving border security while at the same time ensuring that citizens can travel freely, without undue hindrance. Get it right, and they can enjoy the economic benefits of global travel. Get it wrong, and a country could expose itself to illegal immigration, terrorism, organised crime, and accusations that it is not protecting citizens.

Excessive security can cause severe problems at airports. Witness the scenes at UK airports during August 2006 following a major terror alert and it can be seen that highly restrictive border control methods are sustainable for only a very short period of time before they cause massive damage to the airline industry, airport operators as well as other commercial enterprises and have an impact on the wider economy<sup>1</sup>.

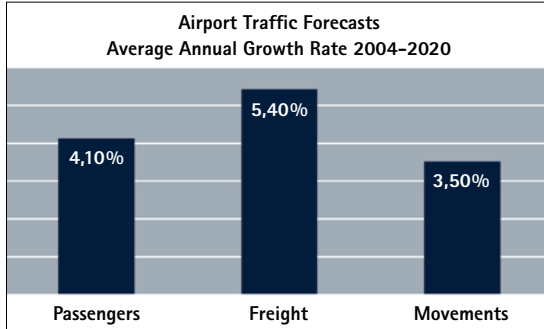
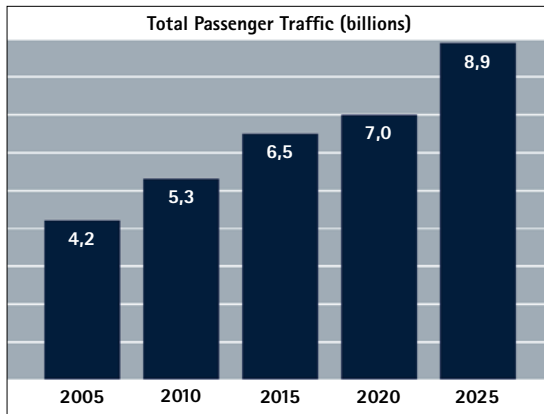
However, security must be good enough to allow border control authorities to counter the many serious threats already mentioned.

#### **1.3.i Growing traveller numbers**

The way passengers travel is changing. The success of low-cost airlines in penetrating the short-haul market and the setting up of new point-to-point connections has resulted in a surge in passenger numbers in many developed countries. Major airports have grown to accommodate these new players, while regional airports have expanded enormously.

Market studies forecast an annual growth in air passenger numbers of 4–6%. This means that air passenger numbers will double in the next 20 years.

<sup>1</sup> *The British Airports Authority (BAA), owner of seven major UK airports, says this terror alert cost it €13 million in increased security measures and lost revenues from cancelled flights.*



At international destinations, such passenger volumes will put a strain on existing border control resources, so authorities have to ensure that border control is not the bottleneck in international travel.

### 1.3.ii Bigger aircraft

As well as the growth in passenger numbers, airlines are also planning to operate larger planes. For example, the Airbus A380, which was first presented in 2005, is capitalising on projected passenger growth worldwide by being marketed as the world's first true double-deck passenger airliner designed to carry more passengers over longer distances. However, the use of larger aircraft could slow down passenger embarkation and disembarkation and, of course, border control. So new solutions are required to avoid delays.

### 1.3.iii ePassports

The leading economies which handle the largest percentage of travellers are already taking steps to improve their borders by introducing biometric ePassports.

*Bundesdruckerei has provided ePassport systems for many countries such as Germany, Luxembourg, Venezuela and Lithuania. We are a leading supplier of integrated ID systems. Regarding this topic, please refer to our ePassport-Booklet*

Although ePassports are currently a rarity at border controls, this situation is going to change rapidly. After 2010 ePassports are expected to be the most common travel documents.

### 1.3.iv Flows of migrants

Globalisation has put more pressure on governments and border control officials to deal with a number of challenges that have taken on an international dimension. Changing geopolitics as well as numerous humanitarian crises have had an impact on the flow of migrants. Civil war, unrest and severe economic problems in regions as far apart as Africa, Latin America, the former Yugoslavia, Asia and the Middle East have also had an impact on the numbers of citizens seeking to enter a new country for humanitarian reasons over the past few decades.

More citizens are migrating to foreign countries than ever before. According to the UK's Office of National Statistics, 4.9 million (8.3%) of the UK's total population in 2001 was born overseas, compared with 2.1 million (4.2%) in 1951. And the increase in absolute numbers of the foreign-born population between 1991 and 2001 was greater than in any of the preceding post-war decades.

### 1.3.v Illegal immigration, human trafficking and ID document fraud

Although the vast majority of travellers enter a country legitimately and of their own volition, border officials must implement procedures to deal with the growing problem of illegal immigration.

Strategies also need to be adopted to deal with the illegal immigrants who simply pass through normal border control (green and blue) channels. It also means to establish strategies to prosecute those who make money from people trafficking as well as dealing with the individual needs of those who are being trafficked.

Although the media has focused on the problems of human trafficking and illegal entrants through normal border crossing channels, other forms of illegal immigration actually occur more frequently. Many visa holders do not leave the country after visa expiry – so-called overstayers.

Moreover, trials have demonstrated that visa and passport ID fraud is increasing. This includes visa shopping, document forgery, multiple IDs, and document trading. Smart border control solutions must prevent these types of fraud.

#### **1.3.vi International terrorism**

Procedures must also be implemented to reduce the potential threat of terrorism. While individuals being trafficked may enter a country hidden in the back of a lorry, terrorists are more likely to enter through normal ports of entry at land, sea and air borders. Given the vast financial resources behind some terrorist organisations, border security officials need to challenge such groups with equally large resources and sophistication. In addition to examining luggage and goods being transported across borders for explosive substances, and chemical, biological and nuclear weapons – or the means to make such devices – border officials must also carry out thorough ID checks. This is especially important given the fact that over the past few years, a number of major terrorist suspects have been found to have multiple IDs when arrested, with some having up to 50 aliases. One of the 9/11 hijackers is alleged to have had 30 false IDs.

*The 9/11 Federal Commission's report says: "Travel documents are as important as weapons. Fraud is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are."*

## **1.4 REQUIREMENTS FOR FUTURE BORDER CONTROL**

The international trends of increasing traveller numbers, larger aircraft, ePassports, illegal migration, international terrorism and organised crime require new strategies and technologies as well as cooperation between governments and airlines.

### **1.4.i System interoperability**

Future border control solutions must be able to communicate with different information systems, read all kinds of travel documents and be flexible regarding the position of the chip and the integration of any future standards. Biometric identifiers should not be stored in proprietary formats, interfaces should use standard protocols, and the whole setup of the system should be modular and based on standard components.

### **1.4.ii Increasing throughput**

With international travel and the exchange of goods constantly growing, increasing throughput capacity is vital for border control authorities, airlines and airport operators. New technologies should be used not only to increase security but also to enhance convenience, e.g. to reduce time spent at border control posts.

### **1.4.iii Biometric verification and identification of travellers**

Progress has been made with electronic documents, an essential element in the automation of traveller processing. Machine Readable Travel Documents (MRTDs) containing eye and machine-readable data have been in circulation since the 1990s.

Significant steps have been taken with ePassports. In an effort to enhance security further, the ICAO has been moving towards biometrically enhanced ePassports since 1997. Full rollout of the first of these documents to citizens began in 2005. A modern electronic MRTD contains an RFID chip, which, in a standard format, stores the holder's identification details, including a digital image. Most ePassports include 64KB chips or bigger, because many governments plan to implement biometric fingerprints or other biometric identifiers in addition to the face, which is the primary and mandatory biometric.

However, in most countries document authentication is still based on simple MRZ readers or even performed manually. Even the automated steps are mostly based on traditional MRTDs and are not yet adapted to take advantage of ePassports, electronic visas and biometric identifiers. Verification is based only on the visual comparison of the holder with the printed facial image, and a search of one or more proprietary databases is still the preferred identification approach.

Consequently, it is required to take advantage of ePassports for biometric verification and identification of individuals at border control points.

## 1.5 ACTION ALTERNATIVES FOR BORDER CONTROL

Border control authorities are examining a number of strategies to help them achieve their aim of processing millions of low-risk passengers quickly, conveniently and cost-effectively while also weeding out potentially high-risk travellers and responding quickly to higher-risk situations.

If security is increased and traveller numbers double, there are only three strategies to prevent capacity bottlenecks at border control.

- 1) Capacity extension. Authorities would have to increase the number of control facilities. With many governments imposing public spending restrictions, this option is unlikely to be implemented.
- 2) Longer waiting times. Travellers would have to wait longer at border control. In a worst-case scenario, waiting times could increase significantly and border control would become a bottleneck. It is also unlikely that this alternative will be favoured.
- 3) Process automation. This option will be the preferred way to solve capacity problems. Authorities have the choice of automating selected parts – or even the whole – of the process. Border police could focus on supervising automated crossings and controlling selected-risk travellers. This would give the ‘human factor’ a new role and enhance the importance of border police work.

Action alternatives for border control can be summarised as:

- ▶ Process automation
- ▶ Separation of traveller flows
- ▶ Pre-processing of data
- ▶ Process acceleration and optimisation
- ▶ Implementation of new technologies
- ▶ Automated detection of hazardous substances

### 1.5.i Process automation

Moves are now afoot to introduce greater levels of process automation to overcome some of the bottlenecks experienced by travellers. Different levels of automation will be the key to facilitate border control.

Even in a **staffed border control scenario**, border police will take advantage of automated travel document readers to read electronic and conventional passports and use biometric equipment to verify a traveller's ID.

Some inspection points, particularly those with a high volume of travellers, may choose to **separate the process**. Process separation enables the efficient use of traveller moving and waiting time for necessary background control procedures. The traveller will be able to start the control process in a self-service gate and trigger the required background checks while approaching the staffed inspection point. This approach allows all the checking results to be available when the passenger reaches the staffed inspection point, significantly speeding up the border control process.

The pre-processing of data can also be carried out by private parties such as airlines. The Automated Passenger Information System (APIS) and the Automated Passenger Profiling (APP), which is used by airlines to send passenger data to destination authorities prior to – or within a short time of – boarding, is already being implemented.

**Fully automated checkpoints** will also be increasingly important for future border control. This concept has been proven in several trials worldwide. For fully automated checkpoints pre-enrolment will be mandatory. But current trials have shown that an electronic travel document on its own may not be sufficient for travellers to participate in automated environments. It is likely that the implementation of automation concepts will require to issue additional credentials and a registration.

Vertical process separation will also help to segregate traveller streams. Those travellers with a document that could be used in a self-service kiosk can be separated from those with ones that are not MRTDs. And individuals willing to participate in such a process can be streamed through faster channels than those who are not. This will be a self-adjusting model, which can be achieved over time with intelligent use of information technology.

Horizontal separation could take place along the control chain. For example, registered traveller programmes can be used to allow registered travellers to be processed faster through border control, using their biometric identifiers. In practice, registered and non-registered travellers will be processed in separate lines. This not only makes it more convenient for registered travellers but it also frees up resources that can be used to control non-registered travellers. This demonstrates how shifting certain steps in the process upstream can help to relieve the primary checkpoint of some of its roles in the future.

#### **1.5.ii New strategies**

The high-tech security industry has to work with government authorities to redesign border control processes so that they can be optimised and speeded up while also keeping pace with constantly changing security requirements. Also, all players involved must ensure that passengers have a good travel experience, while keeping costs down and continuing to provide effective security. Achieving all these requirements might seem impossible, but they can be achieved if systems are implemented that use innovative technologies such as electronic travel documents and biometrics, and if strategies focus on user friendliness and areas that are operationally critical for border authorities.

#### **1.5.iii Recycling data**

Border control authorities must also implement network technology that enables passenger data captured upstream to be reused downstream. This is essential if they are to simplify the journeys of the vast majority of passengers who are regarded as low-risk and so do not warrant any special kind of attention. It also means that security checkpoints must be networked with entry and exit border controls and departure procedures. For example, at airport borders,

airlines already perform a number of pre-processing steps for border authorities when capturing API data (see above). With airports being stretched to capacity, it makes sense for more passenger data to be pre-processed before travellers even enter the airport.

Such analysis could include searching for names against a watch-list of suspects and examining unusual patterns in passenger behaviour. Encouraging remote – and kiosk – check-in would also provide authorities with more time to examine passenger data.

#### **1.5.iv Simplifying immigration**

Moreover, once a passenger has landed at his or her destination, immigration procedures must be followed. Currently, certain passengers have to fill out landing cards and customs declaration forms. Because this information has already been given upstream, it could be incorporated into the overall border management process, enabling governments to make immigration, customs and security decisions about a person early, remotely and cost effectively, while enhancing the travel experience. Similar integration steps must be taken at land and sea borders.

The move towards the pre-processing of data requires information to be captured and shared in a timely manner between all parties involved in the travel process. This is a considerable challenge that must be tackled in a way that does not breach any national or international privacy regulations.

#### **1.5.v New technologies**

To achieve the aim of simplifying border control, new technologies are being piloted. Following the introduction of ePassports the use of biometric verification and identification will become common in future. Machine assisted verification can even solve the look-a-like problem. Machines could differentiate images and faces much better than humans even without getting tired. Within the last decade the information available at the border control desk increased. As a result it is more and more difficult to differentiate between all the information provided and to make the right decisions.

In a few years, ePassports will be the most common travel document at border control. New technologies, such as 3D

face recognition and multimodal biometrics, will allow more accurate recognition and create completely new applications.

The combination of automation with the exploitation of biometric technologies will make the primary inspection process more secure and more efficient. Advanced full-page document readers with RFID capabilities provide the potential for automated and semi-automated high-speed optical and electrical document authentication, as well as reading the biometric identifiers stored on ePassports.

#### 1.5.vi Speed is essential

Today, biometric technologies are being trialled in many parts of the world as a way of clearing travellers swiftly and securely through immigration control, thereby enabling authorities to deploy their resources more efficiently. Biometric fast-tracking, e.g. in Registered Traveller Programmes, will also play a role in other processes such as security control. Eventually, biometrics will be even used by airlines for check-in and boarding.

Of course, all these ideas require a high level of system integration and inter-system communication. Instead of the proprietary information systems currently used by border control authorities, standardised or even joint networks which are able to communicate across borders will be installed.

Bundesdruckerei uses its many years of experience of developing complex ID system solutions to provide a holistic approach to border control. It offers a broad spectrum of products and services, from risk assessment and security plans to process optimisation. Its expertise includes providing solutions ranging from the acquisition of personal data to the checking of ID credentials. It offers for example:

- ▶ Consulting, project management and services;
- ▶ Dedicated consular and border control systems;
- ▶ Hardware and software integration;

As part of border control systems, Bundesdruckerei provides devices for border control that authenticate, verify and identify documents. Its product portfolio includes stationary and mobile systems for checking document authenticity.

## 2.1 PROCESS MANAGEMENT

Although technologies and systems exist that enable border authorities to improve security and convenience in advance, many have opted to continue basic background security checks at borders. Because these checks must be carried out quickly, only basic inspections can be carried out, such as passing MRZ data from a passport to an information system in the background and consolidating the resulting data. Most of the systems used can handle only text data. They need to be updated not only to handle certificates and biometric data, e.g. images captured in a live environment, but also to provide a level of interaction with the traveller.

At the border there are to many systems that supply decision relevant information but they tend to overcharge the officers being forced to take a decision.

The screens used by border control officers when gathering and analysing this data can be overly complicated and display too much information at one time. With the introduction of biometrics, the interaction with the traveller increases. While today he pushes some questions and checks the document he will be forced to enrol one or more biometric identifiers. Consequently, there is a risk that there may be an increase

in human error and that officials could fail to identify a potentially high-risk traveller. For this reason it is essential to ensure that the human interface is well designed and supports the workflow.

In addition to having to cope with overcrowded screens, the sheer number of network systems and information silos currently used at border control means that border control officials must frequently jump back and forth between different programs. Others have the opposite problem – they use information technology very little. In either scenario there is a good case for system optimisation.

Bundesdruckerei provides solutions that address these needs. By consolidating all data into one workflow management software with a single user interface, border authorities can achieve their security requirements.

## 2.2 DOCUMENT CONTROL

With new security features such as Optically Variable Devices (OVDs), holograms, hidden information and radio frequency technology featuring in innovative travel documents, border authorities need to invest in extensive staff training as well as in technology. Bundesdruckerei's VISOTEC range of products has been developed to meet these needs.

### 2.2.i Optical authentication

VISOTEC is an automated document reading and checking system that recognises forged or manipulated ID documents and identifies and verifies documents and their owners. It automatically classifies different types of travel documents and considers the specific parameters for each document so that all customary security features are examined. It also analyses security features, including RFID, MRZs and security paper, and carries out laser feature checks such as kinegram and Diffractive Area Code (DAC), pattern and image recognition, retroreflecting foils, 2D barcodes and hidden images.

The VISOTEC document-checking device can be integrated into other systems, such as staffed terminals as well as self-service kiosks, and is available in Expert 100, Expert 300 and Expert 500 formats.

With high-tech security printing incorporating even more innovative security features, border authorities need more specialised equipment to visually authenticate documents to ensure that they are genuine. Visual authentication of documents can take a number of forms: looking at different light sources, using technology to perform pattern recognition and comparing images against a picture database. VISOTEC devices take a multi-level approach to authentication. Initially, the system subjects all the usual security features to an automated forgery recognition check. This includes using different light sources to examine highly secure and even 'invisible' printing. Users of VISOTEC technology have access to a continuously updated document database which can be used to automatically check standard ID documents used worldwide.

### 2.2.ii Electronic authentication

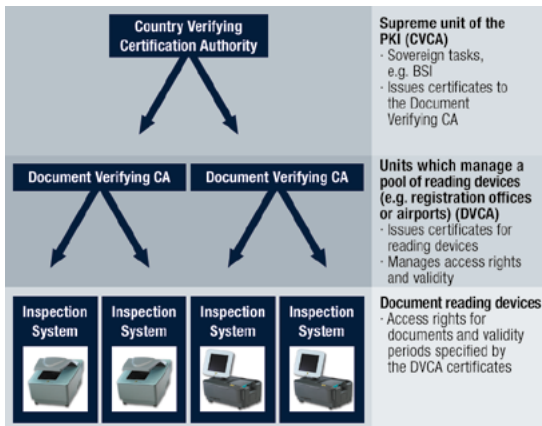
The launch of ePassports has made it possible, for the first time, to establish a unique connection between a document and its owner. With the improvements to passport documents through electronic storage of biometrics and other personal data, passport issuers have had to ramp up the level of access protection to the passport chip to ensure that a citizen's personal data is reliably protected from unauthorised access or reading. In order to establish the connection between the document and the document holder, a 1:1 comparison of the individual data of the person presenting the document is then carried out with the reference data of the document.

### 2.2.iii BAC

Most ePassports use Basic Access Control (BAC) to protect access. This method, which uses challenge/response mechanisms based on ICAO recommendations, is compulsory for all EU member states with the introduction of ePassports. Using BAC, the passport reader is able to access the personal information stored in the chip only by reading the MRZ of the passport.

### 2.2.iv EAC

Building on the BAC system, many countries will be required to implement supplementary protection functions in the form of Extended Access Control (EAC) to protect fingerprints stored on the passport chip. These by far exceed the mechanisms of BAC and must be implemented in European ePassport projects by 2009.



► Box 2

EAC is based on a combination of protection mechanisms provided by the chip and the reader unit. It involves checking data authenticity as well as monitoring access authorisations. Asymmetric cryptography techniques based on a complex interplay between public and private keys are used to encrypt and decrypt the sensitive data.

EAC comprises two distinct phases: chip authentication and terminal authentication. This does not replace BAC. Instead, in future, the process of reading a biometric-based ePassport will follow the sequence:

Basic Access Control + Chip Authentication + Terminal Authentication.

During the chip authentication phase, secure communication between the chip and the reader is established. At this point an implicit authenticity check of the stored information is also carried out. This process enables authentication of components that were allocated during personalisation to take place. This is because during personalisation, an individual pair of keys is allocated to the chip, the private key being stored in the secure part of the chip memory itself, and the public key in data group 14 of the Logical Data Structure (LDS). Because only a 'genuine' chip is capable of establishing communication with the reader unit which is protected by both keys, chip authentication also ensures automatic 'copy-proofing' of the stored chip contents at the same time.

During terminal authentication, only authorised reader units with precisely defined access rights can gain access to the information stored in the chip. Whenever communication is established between the chip and the reader unit, the reader unit's authorisation certificate is automatically checked. To guarantee the authenticity of the certificates used in terminal authentication, the certificates must be derived from secure certification authorities, and the certification chain must be traceable back to a superordinated root authority, as illustrated in the graph (box 2). This requires the establishment of a Public Key Infrastructure (PKI).

*Bundesdruckerei has accomplished the world's first live field EAC trial during the 2006 FIFA World Cup in Germany.*

## 2.2.v PKI

Many high-tech secure travel documents such as ePassports rely on electronic certificate, signature and PKI technology to provide confidential, secure and legally binding communications in open, unsecured electronic communication networks. Using PKI, an individual key pair, comprising one private and one public key, is assigned to each user. Using this key pair, users in a communication network can authenticate each other and communicate confidentially. Each PKI requires a reliable authority – such as Bundesdruckerei's subsidiary D-TRUST – to generate the keys and issue them to authenticated users. Through D-TRUST, electronic certificates, signatures and PKI technologies are developed and marketed for companies, agencies and citizens. D-TRUST offers a number of services related to electronic signatures as well as a range of trust-centre services, from the signature card to PKI design and the virtual Certificate Authority (CA).

## 2.2.vi Database queries

Efficient authentication of travellers requires swift access to databases – something that is made even more challenging by the sheer demand border authorities may place on a database ID system. In future, not only will new national and international databases be established, they will also be interconnected. And, even more challenging, all these databases will have to be accessible not only from stationary access points but also from mobile devices – wherever authorities conduct controls throughout a country.

Mobile devices need to be all-in-one devices that can be easily transported, and must also be able to gain access to databases through GSM/GPRS or other wireless technology. And because they will be used for standalone operations, they must also have a long battery operating time. Under this scenario, interaction with central databases becomes more and more relevant.

Bundesdruckerei's border management systems, which include stationary, mobile and self-service systems that can be configured for different biometrics, and linked to various systems to conduct background checks. Equally they support the workflow and the decision making process.

Bundesdruckerei's holistic approach covers everything from the acquisition of personal data to the checking of ID. It includes consulting, project management and other services, dedicated border control systems, as well as hardware and software integration.

## 2.3 CONTROL OF INDIVIDUALS – A FACE TO THE FUTURE

When it comes to verifying and identifying individuals, biometric technology is playing an increasingly significant role worldwide (see breakout box 1). The technology has been developing a good track record in corporate and government sectors, where it is being applied both to add convenience and to improve security.

In the case of border control, biometric methods can be used either for verification or for identification. In verification mode, they can check and verify the claimed ID of an individual against a stored reference, in what is referred to as 1:1 matching. In identification mode, biometric systems can identify the individual's biometric against a database or watch-list of individuals in what is referred to as 1:n matching.

With the rollout of biometric technology, new procedures will have to be implemented by the issuing authority as well as at the point of entry. This includes introducing a PKI infrastructure to secure the integrity of the data, as well as quality assurance measures for capturing devices.

### 2.3.i Building on experience

Bundesdruckerei is at the forefront of developing and rolling out biometric ePassport technology worldwide. Its experience has helped Germany to become the first EU country to roll out a real-world, ICAO-compliant ePassport system. Since November 2005, Bundesdruckerei has been producing the BAC ePassport documents and has also supplied the 5,700 German registration offices with a high-security enrolment and communication infrastructure, quality assurance tools and ePassport readers.

In future it will be necessary to link all registration authorities, consulates abroad and points of entry to the national PKI infrastructure to enrol and read fingerprint data. As well as verifying document authenticity, biometric technologies could be used to establish the link between the document and its owner. Bundesdruckerei is the sole provider for the whole enrolment process at German registration authorities.

The company applies its knowledge of biometric technologies and procedures to ensure that ePassports meet border officials' demand for security and travellers' need for convenience.

### 2.3.ii It's your choice

As a solution provider Bundesdruckerei is not biased towards any biometric technology. However, because the ICAO recommends the use of face, fingerprint and iris in electronic travel documents, the company focuses on these three biometrics.

### 2.3.iii Biometrics at border control

Bundesdruckerei also provides the technology for the capture, verification and identification of biometric identifiers at border control points. Quality control is crucial in this environment, and underpins all of its e-border solutions. To ensure that the data enrolled are of a consistently high standard, Bundesdruckerei also provides tools to evaluate the quality of captured biometrics.

While document and live features can be matched locally to reduce data traffic, it may also be necessary to conduct biometric verification or identification centrally via a database. Because of this, biometric databases need a system of reference numbers. For example, a visa database could use the unique number of the visa or the MRZ as a reference. Using this reference number the data required for the verification will be retrieved from the database.

### 2.3.iv Quality is the key

It is important to remember that biometric technology provides only a highly probable answer, that is, a tiny percentage of false positives or false negatives is to be expected. In verification mode, this is easy to handle but it becomes more complicated in identification mode because the number of data sets in databases can amount to several millions.

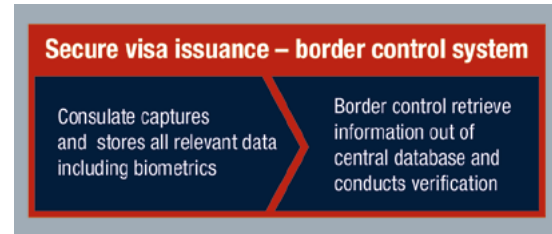
With its years of experience, Bundesdruckerei delivers biometric solutions, and assists its customers in establishing rules and criteria for judging biometric matches and displaying the results.

How biometric results are displayed is often overlooked. But Bundesdruckerei believes this is a crucial area in which border security can be enhanced. If results are clearly and unambiguously displayed on a screen, it will be much easier for an official in a busy border control environment to make a decision about a traveller. But if every bit of information about the traveller and his/her biometric is displayed the border official could easily get stuck in an information 'jungle'. Therefore Bundesdruckerei helps its customers to narrow down the data that needs to be displayed, so officials can make considered decisions regarding the traveller standing in front of them and grant – or deny – them entry.

The number of security tasks carried out by border officials will further increase in future, procedures will become more complex, and additional sets of information will be required to aid the decision-making process.

## 2.4 INTEGRATION OF VISA ISSUANCE INTO THE BORDER CONTROL CHAIN

Bundesdruckerei recognises the need to move control tasks from border authorities upstream. As discussed in chapter 1, the biometric identifiers of visa applicants will increasingly be captured at consular points in future, and be stored either in the visa sticker or in databases. The data will then be verified at the point of entry. Consular and border authorities will even have joint access to certain information systems. An inevitable consequence of all this is that consular and border control processes will become closer in future.



As a result, visa issuance is increasingly being integrated into border control processes. This is an essential development given the need for border authorities to know more about incoming travellers before they arrive in a country. Furthermore, the sheer growth in the number of travellers supports the rise in new technologies being used in visa issuance procedures.

This is why Bundesdruckerei's visa issuance and border control solutions cover the whole process, from the visa application to border control. The company equips consular posts with appropriate enrolment and control infrastructure – including document readers to check applicants' travel documents, biometric devices for verification and identification and the required workflow software.

### 2.4.i Visas come in many shapes and sizes

There are numerous types of visa, including simple visa stamps, more advanced visa stickers without MRZs, those with MRZs, and electronic visas. Most options can be combined with biometric technologies.

Whether the visa is an electronic one, such as the Australian ETA, or a physical sticker, by moving visa issuance upstream, pre-processing of data in consulates can give border control authorities more time to check data and improve convenience for travellers.

*Bundesdruckerei has developed and integrated electronic stickers for Lithuanian passports. These have full ePassport functionality. Similar stickers may in future be used for electronic visa stickers.*

	Stamped	Sticker without MRZ	Sticker with MRZ	Electronic visa
<b>No biometrics</b>	<ul style="list-style-type: none"> <li>- Visa is stamped in the passport</li> <li>- Most simple form of visa</li> </ul>	<ul style="list-style-type: none"> <li>- Visa sticker is sticked into the passport</li> <li>- No ICAO compliance</li> <li>- Can be filled by hand or printed</li> <li>- Simple form of visas</li> <li>- Not machine readable</li> </ul>	<ul style="list-style-type: none"> <li>- ICAO compliant visa sticker with Machine Readable Zone</li> <li>- Machine readable</li> </ul>	<ul style="list-style-type: none"> <li>- Web-based visa application</li> <li>- Unique serial no. or barcode issued to traveller</li> <li>- Advanced visa</li> </ul>
<b>Biometrics in database</b>	<ul style="list-style-type: none"> <li>- No realisticv Option because no unique Identifier such as visa number available</li> </ul>	<ul style="list-style-type: none"> <li>- Unique link from visa to database possible</li> <li>- linking information need to be keyed in</li> </ul>	<ul style="list-style-type: none"> <li>- Unique link from visa to database possible</li> </ul>	<ul style="list-style-type: none"> <li>- Traveller presents code at point of entry</li> <li>- Unique link from visa to database possible</li> </ul>
<b>Biometrics in visa</b>	<ul style="list-style-type: none"> <li>- Not possible</li> </ul>	<ul style="list-style-type: none"> <li>- Integration of RFID in visa Sticker possible</li> </ul>	<ul style="list-style-type: none"> <li>- Integration of RFID in visa Sticker possible</li> </ul>	<ul style="list-style-type: none"> <li>- Not possible</li> </ul>

#### 2.4.ii Establishing a connection between the visa and its holder

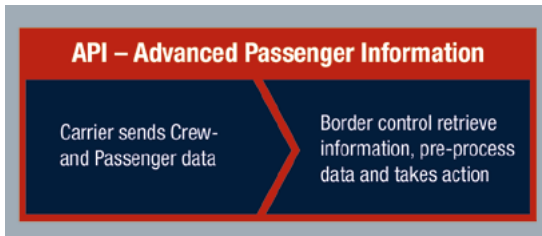
By integrating biometrics into a national or supranational database, governments can establish a reliable connection between the visa and its holder. However, when biometric technology is applied to visa schemes, new procedures for enrolment, personalisation and issuance have to be adopted. Border officials could also capture biometric data to detect common fraudulent practices associated with visa issuance, such as one person applying for a visa under two different names, in different consulates or with a false document. At the personalisation stage, the visa sticker will be printed and personalised with information, such as the traveller's personal details – and, in certain countries, their biometrics – as well as the validity of the visa. During issuance, the visa sticker will be placed in the traveller's passport. Bundesdruckerei's visa issuance solutions cover the visa process from biometric and biographic enrolment, verification, identification and document personalisation to document issuance.

#### 2.4.iii Joined-up thinking

Today's border controls require the involvement of numerous stakeholders. For example, carriers must now send Advanced Passenger Information (API) to border control authorities. This information originates from the passport and, depending on the country's requirements, comprises information such as the traveller's passport number, country of issue, expiry date, given names, last name, gender, date of birth and nationality. This data is submitted to authorities and is checked against the databases of various agencies. In turn this procedure has indirectly made carriers responsible for border security through their own security checks.

Bundesdruckerei understands the needs and requirements of the parties involved, and provides customizable systems to fit these needs.

By passing a traveller's documentary information obtained during check-in to the destination control authority in real time, authorities can even decide whether to allow the passenger to board a plane or vessel. For example, this is realized in the Automated Passenger Profiling (APP) approach.



Such issues become even more important when considered in the context of seaports, where large ships may dock with thousands of passengers needing to be processed quickly. Given the rapid increase in security requirements at all borders, including land and air, the need for seaport authorities and boat operators to carry out border security checks as early as possible – even before travellers board the boat – is paramount.

Although many countries are now requesting API data, it is highly probable that future datasets will also include biometrics. Bundesdruckerei is able to supply solutions to meet these future needs.

#### 2.4.iv Optimising border control

The key to successful border control is to have the right data – at the right time captured with the right tools. This is important, because there is no shortage of data out there. In fact, weaknesses in border control have often been caused by mountains of data being obtained at the wrong time, without the correct tools or intelligence techniques to interpret it. However, it doesn't have to be this way. A more appropriate solution is for border authorities to take a holistic approach that enables them to implement systems for managing visas, improving security with biometrics and making use of any advanced passenger processing data whenever and wherever it has been collected before the passenger's departure.

### 2.5 EXIT-ENTRY SYSTEM

Documenting entry and exit requires a flexible approach that maximises efficiency while providing a suitable level of security. In a move aimed at speeding up entry processes, some governments now document entry and exit before passengers have even set foot in the country.

However, entry and exit documentation takes place at the point when a traveller arrives in – or departs from – a country. In the future, more countries will use systems to record the entry and the exit of all those entering or leaving a country. Such systems – which mark a move away from the traditional approach of merely giving a travel document a cursory glance – will be able to instantly verify whether or not a certain person is still in the country. Countries adopting this approach can keep detailed records of how long an individual is allowed to stay in a country and they can also quickly track down the names and contact details of individuals who are due to leave the country or who need to request an additional visa. Of course, this is a complex task and authorities need tools that have been designed for the purpose.

#### Dealing with 'overstayers'

Implementing systems to record entry and exit will help solve the problem of so-called 'overstayers' – visa holders who remain in the country after their visa has expired. In some countries overstays are a serious problem. Unless a country's border authorities have the tools in place to detect them, such tasks will have to be carried out by overstretched local authorities.

To tackle the challenge of overstayers, authorities need tools to efficiently and systematically query border entry and exit databases.

*Bundesdruckerei offers mobile inspection systems that help officials to conduct mobile controls, read documents, and capture biometric features. These devices can access remote databases such as the exit-entry register on the move.*

## 2.6 IMPLEMENTATION SCENARIOS AT THE POINT OF ENTRY

The general trends and requirements described in chapter 1 are the framework for Bundesdruckerei's product and solutions portfolio, which has been developed to meet the needs of border control authorities. But how will process management, document control, and biometric verification and identification be implemented in the real world? What options do border authorities have when designing their processes in real life, beyond laboratory tests and field trials?

Bundesdruckerei believes a customised approach to border management is the most effective. In fact, one system configuration definitely does not fit all countries' needs. When considering implementing a new system, border authorities need to ask questions such as:

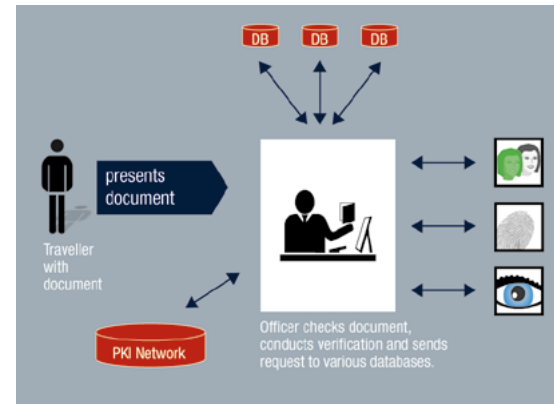
- ▶ Who are the stakeholders of the borders – and how influential are they?
- ▶ How many travellers are expected to pass through these borders every day?
- ▶ What are the peak periods for traveller throughput?
- ▶ How much luggage/cargo is carried through these borders each day?
- ▶ What are the nationalities of most travellers?
- ▶ Why are they coming into the country? For example, how many are frequent travellers who live in another country and visit on a daily basis for leisure/work activities?
- ▶ What is the standard level of education/technical ability of travellers passing through the borders?
- ▶ What is the budget?

Depending on the answers to these questions, border authorities will then be able to consider a customised Bundesdruckerei solution that fits their needs.

Although border control systems could be optimised and prepared to tackle all these requirements, the interaction with the traveller, the enrolment of biometrics, and the variety of options and controls will slow down throughput. Thus new process models will be required.

Bundesdruckerei believes that there will be three possible real-life scenarios at the point of entry, which are semi-automatic processes, separated processes or automated processes.

### 2.6.1 Staffed semi-automatic process



In this scenario, the traveller has the advantage of a border official being present and able to undertake some of the more complex procedures. The traveller will present his or her travel documents to the border official, who will use the latest technology to process all data. The official will visually examine and use document readers to check the authenticity of the travel documents. Border authorities will need a good level of technology and decision-making assistance to do their job. Officials need to be prepared not only to read electronic travel documents but standard MRTDs as well and even documents without an MRZ.

Moreover, the official will have to capture travellers' biometric identifiers, verify them against a reference dataset stored on the electronic document or in a database, and match them with databases for 1:n identification purposes.

#### Dealing with any travel document

The system needs to be highly flexible so it can support a range of different procedures. For example, procedures carried out today depend on the origin of the traveller and his/her documents. In other words, interoperability is central to the smooth running of a border system. However, interoperability depends not only on the document but also on the reader, the infrastructure and, as such, on the capability of the vendor – a fact reiterated in the 2006 global ePassport interoperability tests.

The sheer variety of procedures will increase with more electronic travel documents hitting the market. The numerous types of travel document will be combined with biometric or conventional traveller controls, resulting in many different possible border control scenarios. Border officials will therefore need to be prepared to deal with questions such as:

- ▶ Does the traveller have an electronic travel document?
- ▶ Which biometric data is stored in the chip?
- ▶ Can the chip be accessed with our equipment?
- ▶ Has the issuing country provided our country with the necessary link certificates?
- ▶ Can all areas of the chip be accessed?
- ▶ Do we need to conduct special checks based on the traveller's origin?
- ▶ Does the traveller need a visa?
- ▶ Is there a visa in the passport?
- ▶ Is the document machine-readable or not?

Additionally border officials will need to be able to deal with biometric visas which are glued into the document. Some countries will follow the EU approach of enhancing visa issuance by storing biometric identifiers in a central database. Others will opt for RFID visa stickers, where all the information is stored on the sticker's chip. Somehow, border officials need to be able to process both types of visa.

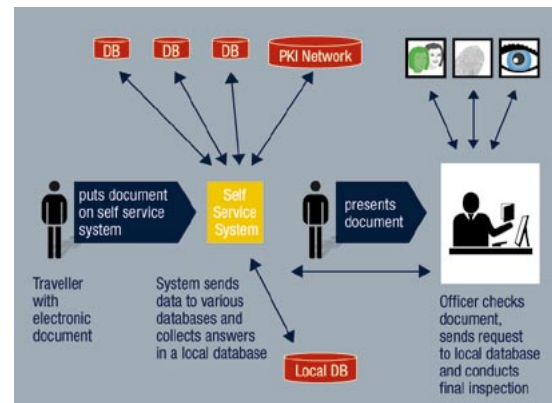
Bundesdruckerei believes officers should concentrate on the document and the traveller's behaviour. To help them with this task, it gives border officials the technical means with which to make their decisions. Border control technology must provide all necessary data and matching results and even suggest a positive or negative decision. Meanwhile, the border official can focus on the traveller and rely on the 'human factor' to make a final decision. All these activities have to be carried out in less than 30 seconds, while dozens of people wait in line. This is a big challenge for the technology and for the border officials, so Bundesdruckerei has focused its development efforts on making this possible. Border officials also need appropriate training to operate the new systems and make decisions based on the mass of data that they are presented with.

Make the most of new technology

Based on information obtained from the traveller's documents, Bundesdruckerei's border control solutions can decide which process should be carried out. And the system should initialise the process without the officer having to hit a single button.

Of course this will not always be possible, but an automated approach will help to optimise the process and give more time to focus on the real problems such as suspected illegal travellers.

### 2.6.2 Separated process



When separated processes are implemented, the traveller will go through a self-service verification procedure followed by a process that involves interaction with a border official. Using this approach, the traveller will begin the process at the self-service station by inputting data or scanning travel document into the system. Background checks on the passenger will then be carried out while he or she is progressing from the self-service point to the staffed counter. The results of these background checks will then be sent to the inspection server and will be ready for the border official to conduct the final inspection of the traveller and his or her travel document. Because ePassports have the highest levels of security, special queues for ePassport holders can be established, enabling these travellers to be processed quickly. This reduces overall queuing and enables border officials to speed up the

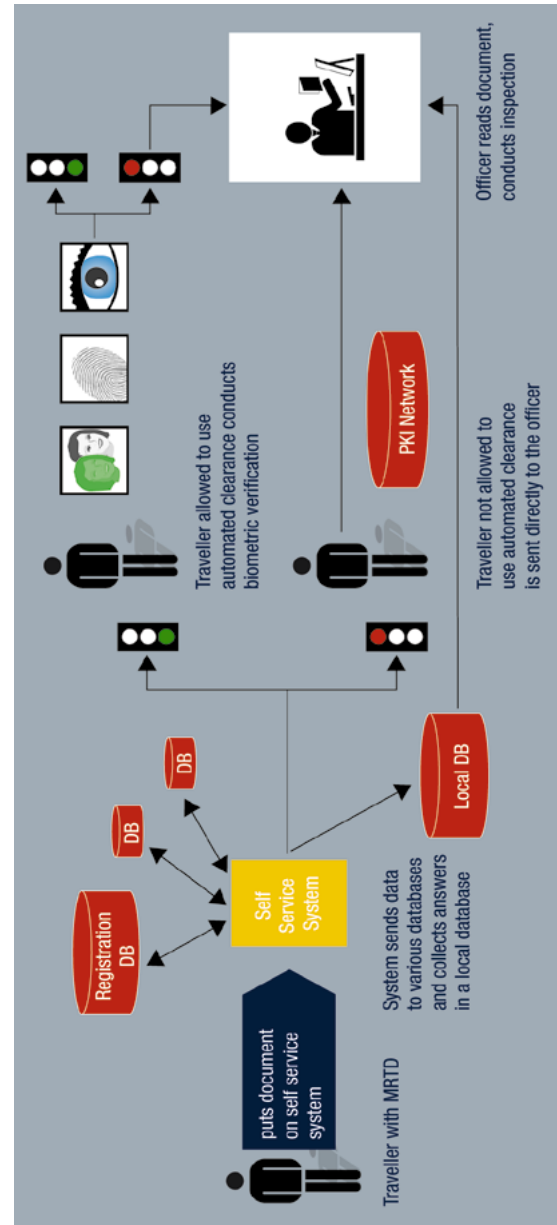
processing of every traveller. By providing ePassport holders with the quickest and least inconvenient route through immigration, governments may even speed up the take-up of ePassports, because some individuals may be prepared to upgrade to an ePassport before their existing document requires renewal. This approach also enables authorities to devote the greatest amount of time and resources to identifying those travellers considered high-risk.

*The separated process would speed up the penetration of electronic travel documents.*

Bundesdruckerei's border control solutions are highly flexible, modular and scalable, enabling border authorities to optimise processes and reduce bottlenecks at primary inspection points.

### 2.6.3 Automated process

If a border authority adopts an automated process, the traveller is responsible for using it. With this approach, resources can be redirected from manpower to intelligent systems. The process is fully automated, but border police still supervise it and perform random checks. The advantages of this approach are that it removes border officials from the more tedious tasks and frees them up to concentrate on high-quality supervision and high-risk travellers.



Automation can be carried out in more than one way. While some applications might work based on the official travel document, others will issue additional credentials to store biometrics, such as smart cards. Whatever the approach, the system will rely on registration and database polling every time it is used.

System enrolment requires easy-to-follow procedures and applications that can be defined by border authorities, which will also be responsible for establishing their own enrolment strategy, possibly using additional biometric identifiers that are mandatory.

At the inspection point, special equipment will be needed, and some aspects of inspection will require special procedures determined by the authorities.

For example, automated lanes will be supervised by border officials and travellers will have to be segregated. To cope with this, door systems need to be implemented that control the flow of people entering the automated gate. Authorities also need to decide whether travellers will be separated into channels or simply have to pass through automated doors.

Two-door exit systems are expected to become very popular for border control. With this approach, a decision to admit the traveller will be made at the first door, if he or she is a known participant in the programme.

Once access has been gained, they will be asked to enrol their biometric identifiers. The system will immediately verify the passenger against the reference stored in the database. If more than one reference has been stored, multiple biometrics could be used at this point.

If border crossing is denied, this is because either the traveller has been identified as being on a watch-list, the travel document could not be read properly, or a random check is required. He or she will then be required to go through an exit gate that leads directly to a staffed control point for further verification. If the traveller is successfully verified, and is not on any watch-list, a second door opens to the further normal border control environment.

Although the installation of automated lines is much more complex than separation and pre-processing of travellers' data, the benefits are much greater. With modern applications that steer and gear the whole process and seamlessly integrate it a nation's border management strategy is unbeatable.

Bundesdruckerei is prepared for further automation at borders and frequently consults its customers to ensure they have the most appropriate systems for their needs.

#### **2.6.4 Mobile control**

The process models described above apply only to stationary border control. However, with border control being carried out on trains, on ships or even within a country, new control applications are required.

While stationary controls are linked to the border control network using a fixed connection, mobile solutions use wireless technology for database polling. Now that wireless technologies are so widespread, it is no longer necessary to store watch-lists directly on the wireless device.

There is a growing need for mobile controls that can be quickly established whenever, and wherever, necessary. For example, if one part of an airport becomes very busy, mobile devices can be quickly deployed to cope with a sudden influx of passengers. And within continental Europe, where many border control points have been removed over the past decade, this is an appropriate approach if there is a sudden need to police internal borders again, such as in Germany during the 2006 football World Cup.

With Bundesdruckerei's mobile document readers, authorities can carry out control tasks in any situation, independent of workstations or other fixed locations. This will clearly facilitate authorities' work and increase a country's security.

### 3.0 CHOOSING AN INTEGRATOR

Many companies operating in the global market provide systems integration services, and it is not always easy to differentiate between their offerings. Although individual governments have their own set procurement methods that may impact on the choice of systems integrator, it is worth remembering that a company should be selected on criteria such as track record, experience and the ability to work with a variety of different partners from both the public and the private sectors. Considering the unique requirements of a government, it also makes sense to select an integrator with well-documented experience of large-scale rollouts in the public sector.

#### 3.1 RESPONSIBILITIES

The systems integrator should be able to support the government at every stage: from the initial idea through to product delivery and integration. It must be able to meet a clear brief, for example, to provide an automated process that will quickly and securely verify the identity of travellers. In addition, it should be able to adapt its solution to work with existing suppliers while providing cost savings to the government and bringing the border management system to market quickly. To achieve this, the systems integrator should be flexible enough to take on a variety of roles that may range from defining and designing platforms and systems to providing ongoing support and training.

#### 3.2 DEFINING THE SYSTEM

It may seem an obvious statement, but rolling out a border control system is not going to happen overnight. Think of all the issues involved and all the challenges associated with adding new technology and new partners. Add to this the numerous other components involved in border management systems – from passport readers to biometric equipment, not to mention complicated back end systems – and you're close to grasping the technical, organisational and process complexity involved. But it doesn't stop there: you've also got to factor in traditional taxpayer scepticism about whether

or not more expensive, high-tech control applications are actually worth having.

Take all these factors into account and you get an idea of the challenges any government is up against when it attempts to successfully roll out an border control system.

It is therefore essential to consider the scope of work required for implementing a new border control system and to understand the roles and the responsibilities that may be involved for the various parties enlisted to deploy the system.

### 3.3 SUPPLY AND INSTALLATION OF THE SYSTEM

Whether fixed or mobile, semi or highly automated border control stations, a central host system will need to be supplied and implemented. In addition, the border crossing points, local police offices and other authorities being part of the integrated border management strategy may need to be established with both the technology and the staff in place to deal with the greater demands of the new control applications.

### 3.4 PROJECT IMPLEMENTATION

ePassport systems are rapidly becoming a reality. Many government watchdogs and taxpayers are rightly concerned that public money shouldn't be wasted on schemes that do little to beef up a country's border security or improve passenger throughput at airports. With many critics standing on the sidelines, waiting for the rollout of a new border control system to flounder, it is essential that precautions be taken to guard against such an occurrence. The chances of achieving this may be greatly enhanced by rolling out the system in a number of phases, possibly involving the implementation of an initial pilot project before moving forward to a full nationwide rollout.

### 3.5 FITTING THE PROJECT TOGETHER

The role of the systems integrator is key to the ultimate success or failure of a border control project. After all, this is where the nuts and bolts of the project will be put together. So an integrator with real commitment, leadership and

experience of secure, large-scale government projects should be selected. It is essential that the integrator can establish and maintain relationships between all suppliers, while ensuring that implementation remains on track and on budget – a pretty hard task to achieve!

The systems integrator is directly responsible for defining the overall border control system architecture. This is a complex task that requires configuration skills as well as an ability to understand and address the various technical requirements by implementing the most suitable technologies. The integrator should also be able to define appropriate platforms and interconnectivity mechanisms.

By communicating with its clients, the integrator should be able to define levels of centralisation and appropriate workflow. Here, the integrator should take into account issues such as how a government's bureaucracy works as well as any national data protection requirements.

Depending on the nature of the national civil registry, the integrator needs to consult on how to modernise the existing registry to comply with future requirements such as the introduction of new technologies and online databases. This is a complex task that requires conformity with national laws. Here, security mechanisms such as passwords, smart cards or biometrics may be applied to ensure only those authorised to access the system can do so. Furthermore, parameters will need to be set so different members of staff can access only the parts of the database that are relevant to their particular job.

### 3.6 ESTABLISH REALISTIC PLANS

Having defined and designed the total system, the integrator should provide an overall project plan and schedule. This is key for managing the expectations of all stakeholders – from taxpayers to government watchdogs and government workers as well as all other organisations involved in rolling out the border control application. Many projects fail at this point because integrators provide overly ambitious time frames that do not take into account the length of the decision-making process within individual governments. It is therefore essential that realistic plans are made and achievable targets are set.

### 3.7 TRAINING AND SUPPORT

After the system has been installed successfully, the integrator must ensure that government employees are fully trained in all applications of the system. This may include data entry as well as more skilled training such as biometric enrolment and system maintenance.

Finally, once the border control system has been completely rolled out, the system integrator should provide ongoing first-line support.

**Advanced Passenger Information System (APIS)**

With APIS, passenger and crew travel document data is read by the airlines, temporarily saved, and then transmitted within 15 minutes of aircraft takeoff to the customs and border authorities of the destination country. Increasing numbers of countries are demanding this data.

**Advanced Passenger Profiling (APP)**

Prior to boarding, the airline or shipping company sends the data contained in the travel documents of passengers and crew to the border control authorities. Passengers are not allowed to board if they do not have a valid visa or are not permitted to enter the country of destination for any other reason.

**APIS Quick Query (AQQ)**

During the check-in process and up to 15 minutes before boarding, AQQ enables airlines and shipping companies to send the data from passenger travel documents to the US Customs and Border Protection before departing to receive entry approval.

**Authentic**

An authentic document is one which is issued by an officially recognised issuing authority, which controls the data and all the security features.

**Authentication**

Checking whether a document is genuine, the validity of the security features and its expiry date.

**Basic Access Control (BAC)**

An ePassport access protection system that permits the RFID chip to be read only after the Machine Readable Zone (MRZ) has been read. The reading device uses the data from the MRZ to generate a key with which it must authenticate itself to the chip in the passport. Communication between ePassport and reading device is always encrypted.

**BioAPI**

A programming interface defined by industrial associations to standardise communication between application software and biometric systems.

**Biometrics**

Biometrics (from the Greek, Bios=life, Metron=measure) measure quantitative features of living beings such as face, finger and iris using mathematical methods for the purposes of identification and verification.

**Checksum**

A checksum is a feature that warrants data integrity when saving data. In order to obtain a checksum, the basic components of a message are multiplied by a certain factor and then added up in sequence. The resultant value is then saved as the checksum. When reading the 'copy' of the data, a checksum of this can also be calculated and compared with the saved checksum of the original file. If the two checksums differ, this indicates that there is a saving error and saving must be repeated. If both checksums are identical, the data has been correctly transferred.

**Coding**

Converting data (for example, text) to a code.

**Counterfeit**

Illegal copying of an ID document or other products.

**Country Signing Certificate (CSC)**

A certificate issued by the Country Signing Certification Authority (CSCA) and used to certify the chip in sovereign documents of this country. The CSC is part of a Public Key Infrastructure (PKI).

**Crew Member Licence**

This is issued by an airline to employees to confirm employment as a member of an airline crew. It is valid only when presented together with a personal ID document, and allows the holder to enter a country without a visa and stay in a community adjacent to the airport.

**Document Adviser**

A border control officer of a country who in the pre-frontier area of, for example, an airport, advises on the authenticity of the ID documents presented by flight passengers, by instructing airline check-in staff on what documents will be accepted on arrival at the destination airport. Background: If an airline flies a passenger with forged papers into a country, the airline is obliged to return this passenger to the airport of departure at its own expense.

**Document Database**

An electronic collection of images showing travel documents from different countries, including the security features for manual or automated authentication of a document at the border.

**Document Reader**

An electronic device which reads the personal data on a Machine Readable Travel Document and displays it on a computer screen for further analysis. We distinguish MRZ and full-page readers. Devices for reading the RFID chip in electronic documents will become increasingly important in future.

**Electronic Passport (ePassport)**

ICAO-compliant Machine Readable Travel Document (MRTD) into which a passive RFID chip is integrated. The chip stores the same data as the data page of the passport, along with a digital photo of the passport holder. Starting 2007, images of the holders two index fingers must be stored on the chip.

**Electronic Signature**

The Electronic Signature (also called Digital Signature) refers to electronic data attached or linked to a message which guarantees the authenticity and integrity of the message. Its purpose is to ensure that the sender is who he/she claims to be and that the message was not changed during transmission from the sender to the recipient.

**Encryption**

Is the process of obscuring information to make it unreadable without special knowledge (key). Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure, particularly to verify the integrity and authenticity of a message. (e.g. electronic signature)

**Enrolment**

One-off capture of a biometric feature as a reference for the future verification of an individual.

**Entry/Exit system**

A database system used by a country to monitor the residency status of foreigners in the country.

**Eurodac**

Database on asylum applicants and individuals who have illegally crossed an outer border of the EU. By comparing fingerprints, a member state can check whether an asylum applicant or foreigner who resides illegally in the member state has applied for asylum in another member state. Eurodac comprises a database for fingerprints managed by the European Commission and electronic systems for data transmission between the member states and the central database.

In addition to fingerprints, the data transmitted by the member states also includes the member state of origin, the place and time of application, the gender of the applicant and their ID number.

**European Union (EU)**

An alliance of states comprising 27 member states and a total population of 493 million. The member states are Belgium, Bulgaria, Cyprus, Denmark, Germany, Estonia, Finland, France, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Sweden, Slovakia, Slovenia, Spain, the Czech Republic, Hungary and the UK.

**Extended Access Control (EAC)**

The EAC protocol has been developed by the European Union to protect the more sensitive data on biometric travel documents, in particular the holder's fingerprint images.

EAC comprises two distinct phases: chip authentication and terminal authentication. During chip authentication, secure communication between the chip and the reader is established. At this point an implicit authenticity check of the stored information is also carried out. This process enables authentication of components that were allocated during personalisation to take place. Because only a 'genuine' chip is capable of establishing communication with the reader unit which is protected by both keys, chip authentication also ensures automatic 'copy-proofing' of the stored chip contents at the same time.

During terminal authentication, only authorised reader units with precisely defined access rights can gain access to the information stored in the chip. Whenever communication is established between the chip and the reader unit, the reader unit's authorisation certificate is automatically checked.

### **Facial Recognition**

*A biometric method in which the face of the person being checked is compared with one or several photos stored.*

*Using the ICAO-compliant photo of the passport holder stored in the electronic passport, the holder of the passport can be verified using this method.*

*Currently, efforts have been made to develop more sophisticated facial recognition technologies. 3D face recognition adds a third dimension to facial recognition, which increases performance and security significantly.*

### **False And Authentic Documents (FADO)**

*European image archiving system (Council resolution of 27 March 2000) to combat illegal immigration and organised crime. FADO is designed to enable the fast and simple exchange of information about authentic and false documents between member states. The FADO database contains the following information:*

- ▶ *Images of forged or manipulated documents*
- ▶ *Images of authentic documents*
- ▶ *Information about forgery methods*
- ▶ *Information on security methods*

### **Fantasy**

*A counterfeit which is not based on a real, existing document.*

### **Fingerprint recognition**

*An individual's fingerprint comprises papillary lines (ridges) and minutiae (branches) and is unique to each person.*

*In fingerprint recognition, a fingerprint scanner first takes an image of the fingerprint. Either the image or a template of the fingerprint is then saved. Storing the fingerprint of the 2 index fingers in the electronic passport will make the verification of the passport holder even more reliable than only storing the facial image.*

### **Forensic examination**

*Laboratory examination by highly qualified experts of documents for authenticity features which cannot be identified by citizens and control officers in Primary Inspection.*

### **Full-Page Reader**

*An ePassport reading device which scans the complete data page of the document and displays data on the screen.*

### **Identification**

*Finding a set of data, e.g. an individual's biometric identifier, from a large parent population (1:n)*

### **Identification Document**

*A document issued by an authority containing permanently applied information which permits an authenticity check. It proves the identity of the document holder.*

### **International Civil Aviation Organization (ICAO)**

*A sub-organisation of the United Nations (UN) which aims to harmonise rules for international civil aviation.*

### **International Maritime Organisation (IMO)**

*A sub-organisation of the United Nations (UN) which aims to harmonise rules for international maritime traffic.*

### **Iris Recognition**

*A biometric identification method. The iris is the diaphragm of the eye which is coloured by pigments and regulates the amount of light that enters the eye. Its pattern is unique to each individual. Using this method, a live photo of the iris of the person to be verified is captured and then compared with a previously stored reference. A laser beam is not used.*

### **Machine Readable Passport (MRP)**

*One category of MRTDs, complying with ICAO Document 9303.*

### **Machine Readable Travel Document (MRTD)**

*An international travel document that contains certain eye and machine readable data, complying with ICAO Document 9303. MRTDs can be passports, visas and ID cards.*

### **Machine Readable Zone (MRZ)**

*The Machine Readable Zone in the lower part of ICAO-compliant travel documents which makes it possible for document readers to quickly capture the document information. The specification is laid down in ICAO Document 9303.*

### **Optical Character Recognition (OCR)**

*Optical Character Recognition is used to extract text information from images because text cannot be further-processed in image format. When a travel document is scanned on a Full-Page Reader, a file image is created. OCR recognises the characters on the image and enters these into a search mask from where database queries can be started.*

### **Passenger Name Record (PNR)**

Since 5 March 2003, airline companies whose aircraft arrive in and depart from the US, or fly over the US, have been obliged to provide US customs and border authorities with online access to the booking data record, the Passenger Name Record (PNR), which is saved for each passenger in the reservation systems used by the airline companies. The European Court of Justice has criticised the exchange of this data. Meanwhile, a new contract has been signed to overcome the critics.

### **Primary Inspection**

A regular part of border control through which all individuals must pass. This inspection may involve:

- ▶ Authentication of the passport and the visa;
- ▶ Verification of the document holder;
- ▶ Identification of the document and the holder;
- ▶ Questioning on entry, including checking the details of the place of departure/destination and whether an individual has a sufficient means of support while in a country;
- ▶ Under certain circumstances, carrying out vehicle checks and examining items carried by passengers.

### **Public Key Infrastructure (PKI)**

This refers to an IT system which issues, distributes and checks digital certificates. The certificates issued within a PKI guarantee that the holder of the certificate has the authorisation by a trusted authority and that the data contained in the message was not altered during transmission.

### **Registered Traveller Programme**

An RTP could be implemented for a number of reasons. Solutions mainly used at airports are implemented to speed up the entry to the secure part of the airport. Registered travellers (RTs) are considered to be 'security cleared' and will also not be randomly selected for in-depth checking.

Alternatively, the RTP could be a pure border control solution that gives RTs the possibility to use automatic gates.

Both solutions are based on pre enrolment.

### **RFID Chip**

A microprocessor chip which can be used to store or process information. The chips are divided into active and passive RFID. Active chips have their own source of energy (battery) whereas passive chips get their electricity from the reading device by way of induction.

Simple chips are only used for logistics purposes while sophisticated chips include a crypto-controller to process information.

### **Schengen Agreement**

An agreement by several European countries to abstain from checking passenger traffic at their internal borders, as well as establishing a joint external border.

Countries that have already implemented the Schengen Agreement:

- ▶ Belgium (26 March 1995)
- ▶ France (26 March 1995)
- ▶ Germany (26 March 1995)
- ▶ Luxembourg (26 March 1995)
- ▶ Netherlands (26 March 1995)
- ▶ Portugal (26 March 1995)
- ▶ Spain (26 March 1995)
- ▶ Italy (26 October 1997)
- ▶ Austria (1 December 1997)
- ▶ Greece (26 March 2000)
- ▶ Denmark (25 March 2001)
- ▶ Finland (25 March 2001)
- ▶ Iceland (25 March 2001)
- ▶ Norway (25 March 2001)
- ▶ Sweden (25 March 2001)

Countries who signed the Schengen Agreement on 1 May 2004 are set to implement it between 31 December 2007 and 29 March 2008

- ▶ Czech Republic
- ▶ Estonia
- ▶ Hungary
- ▶ Latvia
- ▶ Lithuania
- ▶ Malta
- ▶ Poland
- ▶ Slovakia
- ▶ Slovenia

*Signatories yet to implement the agreement:*

- ▶ Cyprus
- ▶ Switzerland

*EU members not to join the Schengen Agreement:*

- ▶ Ireland
- ▶ United Kingdom

### **Schengen Information System (SIS)**

*A database which continuously compares the contents of the national SIS-compatible databases of all Schengen Agreement states. Currently, 13 EU member states, along with Iceland and Norway, use the SIS. The respective ministries of the interior operate the national SIS. It stores data related to the outer border controls or 'upstream border controls' in the area behind the border. The information is available to all Schengen Agreement states. The following information is stored as text:*

- ▶ Individuals who have received a residence ban;
- ▶ Stolen objects;
- ▶ Stolen or lost documents.

### **Schengen Information System II (SIS II)**

*The successor of SIS which can also store additional information such as graphic data, and enables extended search functions. Its data is used to check individuals at the outer borders of the EU or in the respective national territories and to issue visas and residence permits, as well as for co-operation between the police and judiciary in criminal matters. There are still discussions whether to include biometric data in SIS II or not. Operation of SIS II will start with some delay.*

### **Seafarer ID**

*A travel document for seafarers introduced by the International Maritime Organisation which, in countries that have ratified the ICAO Convention, permits holders to go on land without a visa and to enter the community adjacent to the port of call.*

### **Secondary Inspection**

*Thorough inspection based on sample checks or concrete suspicion from the primary inspection.*

*If there is doubt as to whether a document is authentic or if verification with ePassport failed or was positive with a watchlist, or the traveller was identified on a watchlist, the individual is searched for on different databases.*

### **Swipe Reader**

*A document reader which can only read the Machine Readable Zone (MRZ). To do this the MRZ of the ID document must be swiped through the device's reading slot.*

### **Template**

*A file which contains only the information most needed to identify a previously captured biometric feature and which consequently takes up much less memory. To cut the amount of computer processing required, biometric methods can compare a reference template created during enrolment with a template of the live data captured. The similarity between the live and the reference template is sufficient for verification, because two biometric captures can never supply identical results.*

### **US Visit**

*A US entry/exit system which saves data from all travellers who require a visa to enter the US.*

*Biometric data is captured in the form of a photo and two fingerprints. Also recorded are name, gender, date of birth, nationality, passport number, place of issue, home address, visa number, data of issue and place of issue, registration number (if already assigned during a previous visit) and the address during the stay in the US.*

*Exit is documented by comparing the stored biometric data and the passport. Various US authorities have access to the data, particularly immigration, border and police authorities, as well as consular offices. The data is taken directly from travellers.*

### **Verification**

*Identifying whether a person is who she/he claims to be.*

### **Visa**

*A permit to cross a country's border. Usually only required for entry, seldom for exit, although the latter is required in countries such as China. It gives permission to stay in a country or group of countries for a limited period of time and is issued by the consulate (and/or the consular department of an embassy) of the country of entry.*

**Visa Information System (VIS)**

*This is designed to improve the issuing of visas in the Schengen territory. The EU plans to set up a Visa Information System (VIS) similar to the SIS. Work on it was commissioned in 2004. All embassies and consulates will consult the system for visa applications and save information to it about the applicant, including ten fingerprints. Embassies and consulates, border control and security authorities will also be granted access to the VIS.*

**Visa Sticker**

*A sticker with a unique serial number which is attached to the travel document when entry is permitted and which is regarded by the border control officers in the destination country as confirmation of permission to enter.*



