



FRONTEX
LIBERTAS SECURITAS JUSTITIA

European Agency for the Management of Operational Cooperation at the External Borders
of the Member States of the European Union

BIOPASS
Study on Automated Biometric
Border Crossing Systems for
Registered Passenger at Four
European Airports.

Warsaw, August 2007



Legal notice

The contents of this publication do not necessarily reflect the official opinions of any institution or body of the European Union. Neither Frontex nor any person or company acting on behalf of Frontex is responsible for the use that may be made of the information contained in this report.

All rights reserved

No part of this publication may be reproduced in any form or by any means electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without the permission in writing from the copyright holder. For translation or reproduction rights please contact Frontex (address information below).

Information about the European Union is available on the Internet. It can be accessed through the Europa server (www.europa.eu).

Frontex
Rondo ONZ 1
00-124 Warsaw
Poland
Tel.: + 48 22 544 9500
Fax: + 48 22 544 9501
Web: www.frontex.europa.eu
Enquiries: frontex@frontex.europa.eu



Acknowledgements

This report was prepared by the Research and Development Unit of Frontex in close collaboration with the Institute for the Protection and Security of the Citizens (IPSC) of the European Commission's Joint Research Centre (JRC).

Frontex wishes to thank Dutch Ministry of Justice and Schiphol Group, German Federal Ministry of Interior and Federal Police, French Ministry of Interior and Sagem Defence Security as well as UK Home Office for the cooperation and support extended to the core team before and during the study-visits. Furthermore, Frontex gratefully acknowledges the support of those who contributed text, data and figures.

Finally, Frontex acknowledges all who commented on the draft report, in Frontex (Air Borders Sector, Operations Unit) and the European Commission (DG JLS and JRC).

Frontex is also grateful to the copyright holders for granting their permission to reproduce the images used in this work.



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA

The table of contents

	Legal notice.....	2
0	Summary.....	6
1	Introduction.....	7
2	General background for the study.....	9
2.1	Theory of Biometrics.....	9
2.1.1	Biometric modalities.....	9
2.1.1.1	Facial recognition.....	9
2.1.1.2	Fingerprint.....	10
2.1.1.3	Iris.....	12
2.1.2	Biometric authentication.....	14
2.1.2.1	Accuracy.....	14
2.1.2.2	Variability of biometric characteristics.....	14
2.1.2.3	Error rates.....	15
2.1.3	Large scale biometric systems.....	19
2.1.4	The liveness problem.....	20
2.2	Electronic passports.....	21
2.2.1	The Machine readable zone.....	21
2.2.2	Contactless smartcard technology.....	22
2.2.3	Security of the electronic passport.....	23
2.2.4	Data structure.....	24
2.2.5	Biometric data.....	25
2.3	Biometric border crossing.....	25
2.3.1	The concept.....	26
2.3.2	The implementation.....	26
2.3.2.1	Biometrics.....	26
2.3.2.2	Enrolment.....	27
2.3.2.3	Border crossing.....	28
2.3.3	Disabled passengers.....	29
2.3.4	Different types of border crossings.....	29
3	Case studies.....	30
3.1	Amsterdam Schiphol Airport.....	30
3.1.1	Short description of the airport.....	30
3.1.2	The project.....	30
3.1.2.1	The users.....	31
3.1.3	Procedures – Enrolment – Biometrics.....	31
3.1.4	Biometric error rates.....	36
3.1.5	Problems.....	36
3.1.6	Security.....	36
3.1.7	Costs.....	37
3.2	Frankfurt airport.....	38
3.2.1	General characteristics of Frankfurt airport.....	38
3.2.2	Automated Biometrics-Supported Border Control (ABG) – Overview.....	38
3.2.3	Passengers.....	39
3.2.4	Procedure.....	39
3.2.5	Provider.....	44
3.2.6	Operators.....	44
3.2.7	Difficulties and Problems.....	45



3.2.8	Security.....	45
3.2.9	Costs.....	45
3.3	Paris Charles de Gaulle Airport.....	46
3.3.1	Airport characteristic.....	46
3.3.2	Project.....	47
3.3.3	Passengers.....	48
3.3.4	Biometrics.....	49
3.3.4.1	Technology	49
3.3.4.2	Error rates	49
3.3.5	Procedures	49
3.3.5.1	Enrolment	49
3.3.5.2	Verification.....	52
3.3.5.3	Provider	56
3.3.5.4	Operators	56
3.3.6	Difficulties and problems	57
3.3.7	Security.....	58
3.3.8	Costs.....	58
3.4	Biometric systems at UK Airports.....	59
3.4.1	The IRIS system.....	60
3.4.1.1	Enrolment	61
3.4.1.2	Post-processing	62
3.4.1.3	Data use	64
3.4.1.4	Procedures on arrival.....	65
3.4.1.5	Other errors and related problems.....	66
3.4.1.6	Training of staff	67
3.4.1.7	Price of the system	67
3.4.1.8	Maintenance of the system	67
3.4.2	miSense and miSense ^{PLUS}	68
3.4.2.1	miSense.....	68
3.4.2.2	miSense PLUS	69
4	Conclusions.....	73
4.1	Biometrics	73
4.2	Booths	73
4.3	Privacy	74
4.4	Future.....	75
4.5	Summary	75
5	References.....	77
	Annex 1: Acronyms and abbreviations	79
	Annex 1: Biometric airport border control survey.....	81



0 Summary

FRONTEX
LIBERTAS. SECURITAS. IUSTITIA

This report concerns a case study of automated border crossing systems based on biometrics at the four largest European airports: Schiphol, Frankfurt, Charles de Gaulle, and Heathrow.

All four systems are fully working and enable the registered passengers to cross the border in a convenient way. Both iris-based and fingerprint-based systems operate well without significant differences. The encountered problems do not concern the biometrics, but rather the practical design of the checkpoints and the human interfaces.

However, all systems operate on a small scale and cover only about one percent of the passenger flow. Furthermore, the systems are highly different in many ways including how they store the data, what token the passenger needs, and the design of the gates. As a consequence, the systems are currently specific to the respective airport with no interoperability at all.

Despite the limited scale of the studied systems, they prove the concept of automated biometric border crossing.



1 Introduction

The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union – Frontex - was established by Council Regulation (EC) 2007/2004/ (26.10.2004, OJ L 349/25.11.2004) to coordinate operational cooperation between Member States in the field of management of external borders. Under the aforementioned mandate, Frontex can carry out study visits to assess the situation of technologies in the field of border management and examine the existing equipments available in the Member States, which should foster the improvement of integrated border management of the EU's external borders.

On the occasion of the grand opening of the new premises of Frontex in Warsaw, Vice-President Franco Frattini stressed the possibility for future technological developments at the EU's external borders, developing systems on entry-exit and registered travellers at the external borders with a full use of biometrics and other new technologies. Some of the EU national governments have already begun the use of biometric modalities for automated border crossing systems at selected airports as a risk-management tool with potential for improving security and facilitation to participating travellers.

The study covers automated border crossing systems at the four largest European Airports, which have been the pioneers in this field:

- Schiphol Airport in Amsterdam, Netherlands – PRIVIUM programme – based on iris recognition;
- Frankfurt Airport in Frankfurt, Germany – ABG pilot – based on iris recognition;
- Charles de Gaulle Airport in Paris, France – PEGASE pilot – based on fingerprint;
- Heathrow Airport in London, UK – IRIS and miSense pilot– based on iris recognition.

There are also other automated border crossing systems based on biometrics. In Portugal, a pilot project – RAPID – started in May 2007 at Faro airport, and in August 2007 the system was implemented in the new Terminal 2 of Lisbon airport¹. The RAPID system is based on facial recognition biometric modality and allows an automated border crossing of passengers in possession of electronic passports.

In response to requests expressed by the end users at the border guard institutions of the Member States to have more thorough analyses on the deployment of biometric modalities in border control, Frontex has carried out a study on automated biometric border crossing systems for registered travellers at the European airports. The Core Team of experts comprising Frontex staff and EU Joint Research Centre experts visited Amsterdam, Frankfurt, London, and Paris airports during December 11 - 18, 2006 to collect the information and assess the state of art of the existing automated biometric border crossing systems at the above mentioned airports, and in doing so to increase comparative knowledge of biometric systems used for border control.

¹ Frontex is planning to carry out a study visit to Lisbon airport in October 2007.



The experts familiarised themselves with the automated border passage and procedures in use at Schiphol, Frankfurt, Paris Charles de Gaulle, and Heathrow airports. They held meetings with and interviewed the key stakeholders, including the respective authorities of the participating Member States, vendors developing and testing automated border passage applications as well as airline industry. In addition, the team visited Research and Development Centres of Sagem (PEGASE system provider at the Paris Charles De Gaulle airport) and Dartnagnan (Privium system provider at Schiphol airport).

The experts also attempted to empirically validate the information expressed by the stakeholders. The Core Team was allowed to enrol and actually imitate the border crossing using the automated border control lane at Frankfurt, Heathrow and Charles de Gaulle. This enabled them to test the performance and effectiveness of these systems.

In addition to the interviews and presentations, other relevant documents - provided by the stakeholders - and available literature were made use of. Information and data obtained from the survey (Annex 2 Biometric airport border control survey) – prepared by the Core Team and delivered to the participating countries in advance - served as a tool to structure the study and obtain the necessary information.

This study is intended to examine and inform the respective Member States on the performance of various biometric authentication systems, their benefits and drawbacks as well as impact on border crossing based upon case studies of biometric modalities for automated border crossing systems for registered travellers in Amsterdam, Frankfurt, London and Paris airports. Four case studies are presented in this study, covering the European pioneers in the area of automated border crossing. All four examined systems are fully working and enable the registered passengers to cross the border in a convenient way.

Chapter 2 gives an overview of biometrics, electronic passports, and automated border crossing. Chapter 3 presents the four case studies, while the conclusions are given in Chapter 4.



2 General background for the study

This chapter gives an overview of biometrics and electronic passports. A more thorough presentation on these topics is given by Vakalis, Hosgood and Chawdhry [JRC06]. The chapter ends with brief discussion on systems for automated border crossings, which serves as an introduction to the four case studies presented in Chapter 3.

2.1 Theory of Biometrics

Generally, there exist three principles on how to identify or authenticate individuals. Identification/authentication can be based on something that people **have** (chip card, ID card), they **know** (passwords or PINs) or something they really **are** (their biometric features). These methods can be used either on their own or in various combinations. In border control typically a combination of “has” (travel document) and “is” (the picture in the travel document must match the traveller’s current look) is used.

Biometrics ([ancient Greek](#): *bios* = "life", *metron* = "measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Biometrics offer automated methods of identity verification or identification based on the principle of measurable physiological or behavioural characteristics such as a fingerprint or a voice sample.

2.1.1 Biometric modalities

The International Civil Aviation Organization (ICAO), a UN Specialized Agency, is the global forum for civil aviation. ICAO works to achieve its vision of safe, secure and sustainable development of civil aviation through cooperation amongst its member States [ICAO07]. This includes the worldwide coordination in the field of travel documents. After executing several studies, ICAO issued specific recommendations for travel documents (including the electronic passport) inviting its members to use facial images and optionally fingerprint or iris as a biometric modalities. The following sections will explain these three modalities more in detail. Other biometric modalities include voice recognition, retina scanning, signature and keyboard dynamics, hand geometry, hand vein patterns, ear shapes and gait or odour recognition.

2.1.1.1 Facial recognition

Facial recognition is the most natural means of biometric identification. The method of distinguishing one individual from another is an ability of virtually every human.

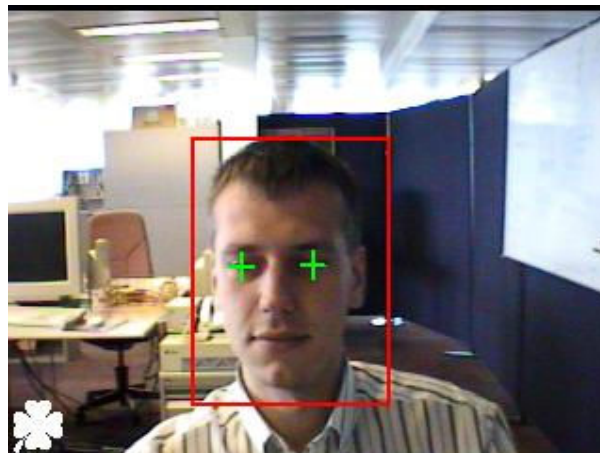
Any camera with sufficient resolution can be used to obtain the image of the face (scanned pictures can be used as well). Generally speaking the better the image source the more accurate results we get. The image recognition algorithm can be based on a 2 dimensional or 3 dimensional face properties. Facial recognition systems usually use only the grey-scale information. Colours (if available) are used only to locate the face in the image only. The lighting conditions required are mainly dependent on the quality of the camera used. In poor light condition, individual features may not be easily discernible. There exist even infrared cameras that can be used with facial recognition systems. The characteristics of facial pictures used in the context of travel documents is



standardised by ISO/IEC 19794-5. This standard distinguishes and defines the “basic face image”, the “frontal face image”, the “full frontal face image” and the “token face image” and gives basic guidelines for acquisition and image processing. This standard is the basis for ICAO requirements.

In electronic passports, the facial images are stored as JPEGs or JPEG2000 files with optional coordinates of important facial features (e.g. eyes). There are no standardized formats for the processed facial templates.

The first task of the processing software is to locate the face (or faces) within the image. Then the facial characteristics are extracted. Facial recognition technology has recently developed into two areas: facial metrics and eigenfaces. Facial metrics technology relies on the measurement of the specific facial features (the systems usually look for the positioning of the eyes, nose and mouth and the distances between these features). Another method for facial recognition has been developed in the past few years. The method is based on categorizing faces according to the degree of fit with a fixed set of master eigenfaces. This technique is in fact similar to the police method of creating a portrait, but the image processing is automated and based on a real picture.



Picture 1: The first task of the facial recognition is to locate the face in the scene. Then the position of eyes must be determined within the facial region.

Face recognition systems have problems to distinguish very similar persons like twins and any significant change in hair or beard style requires re-enrolment. Glasses can also cause additional difficulties. However, the performance of face recognition improves constantly and modern algorithms now show better performance than trained humans [FRVT06].

2.1.1.2 Fingerprint

Fingerprint identification is perhaps the oldest of all the biometric techniques. Systems that can automatically check details of a person's fingerprint have been in use since the 1960s by law enforcement agencies.



Picture 2: Fingerprint reader

To get a digitalized image of a fingerprint livescan fingerprint readers are used. Livescan fingerprint readers are most commonly based on optical, thermal, silicon or ultrasonic principles. The resulting image is a greyscale bitmap with a resolution between 500 and 1000 DPI. JPEG compression is not suitable for fingerprint images, therefore images either use lossless image compression formats (e.g. TIFF) or the WSQ compression algorithm which is optimized for fingerprint images. Fingerprint images which will be stored in European electronic passports will use the WSQ compression. There are also several standardized formats for processed fingerprint templates.



(a)



(b)

Figure 1: Fingerprint bitmap as obtained from the reader (a) and after processing (b) where the minutiae found are highlighted in red.



The fingerprints are not compared as bitmaps. Fingerprint matching techniques can be placed into several categories: minutiae-based and correlation based. Minutiae-based techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands. In recent years, automated fingerprint comparisons have been most often based on minutiae. Other methods for fingerprint comparison are based on fingerprint pattern spectral data or fingerprint pattern skeletal data.

2.1.1.3 Iris

The iris is the coloured ring of textured tissue that surrounds the pupil of the eye. Even twins have different iris patterns and everyone's left and right iris is different too.

A near infrared grey-scale camera in the distance of 10 – 40 cm takes the iris pattern from the camera. There are several types of iris cameras with different requirements on user behaviour and different levels of user friendliness. The iris scanning technology is not intrusive and thus is deemed acceptable by most users. The iris pattern remains stable over a person's life, being affected only by some diseases. There is a standardized format of the iris image, but no standard exists for the iris template.

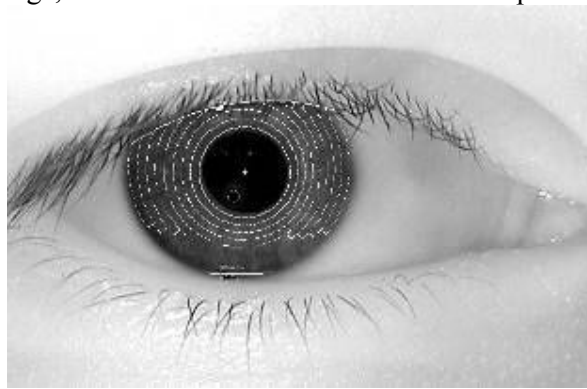


Figure 2: Biometrics based on the unique pattern of the iris.



Picture 3: The OKI iris camera.



Picture 4: The LG iris camera.

Once the grey-scale image of the eye is obtained, the software tries to locate the iris within the image. If an iris is found, then the software creates (by using the Gabor



wavelets) the Iriscode, which characterizes the iris. When computing the Iriscode two influences have to be taken into account. First, the overall darkness of the image is influenced by the lighting conditions, so the darkness threshold used to decide whether a given point is dark or bright cannot be static; it must be dynamically computed according to the overall picture darkness. And second, the size of the iris dynamically changes as the size of the pupil changes. Before computing the Iriscode, a proper transformation must be done.

2.1.2 Biometric authentication

Biometric systems can be used in two different modes. Identity **verification** -also called **one-to-one** matching - occurs when the user (in our case the traveller) first presents his/her identity (e.g. shows his/her passport); based on this identity the biometric data are recalled from the passport or from a database and then compared against the current biometric data of the traveller. **Identification** -also called **search, recognition** or **one-to-many** matching - occurs when the identity of the user is *a priori* unknown. In this case the current biometric data are matched against all records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all.

Before a user can be successfully verified or identified by the system, he/she must be registered with the biometric system. A user's biometric data are captured, processed and stored. The process of the user's registration with the biometric system is called **enrolment** (see 2.3.2.2).

The aim of biometric authentication systems is to verify identity of a user or identify the user. While automated biometric authentication is attractive because it principally authenticates the user (and not something which can be disclosed (PIN) or passed on to a colleague (chip card)), its shortcomings relate to problems with accuracy, the secrecy of the biometric data and implementation details of “liveness” testing.

2.1.2.1 Accuracy

The most significant difference between biometric and other authentication techniques lies in the answer of the biometric system to an authentication/identification request. Biometric systems do not give simple yes or no answers. While the password either is 'abcd' or not, and the PIN 1234, either is valid or not; no biometric system can verify the identity or identify a person absolutely. One's signature is never absolutely identical and the position of one's finger on a fingerprint reader will vary as well. Rather than a simple yes or no answer, therefore, the biometric system gives a measure of how similar the currently obtained data are compared to the stored data.

We have to allow for some variability of the biometric data in order not to reject too many authorised users (this would be a case of **false rejection** error). However, the greater variability we allow the greater is the probability that someone with similar biometric data will be accepted as an authorised user (this is a case of **false acceptance** error). The variability is usually called a **(security) threshold** or a **(security) level**.

2.1.2.2 Variability of biometric characteristics

The performance of a biometric technique depends on what features – whether genotypic or phenotypic – the technique is based on. Genotypic features do not change over time. This is good news for the false rejection rate, which may remain low as the



matching algorithm does not have to adapt to changes. The bad news is that genotypic features cannot distinguish monozygotic twins. So the percentage of identical twins² in population sets the lower limit on the false acceptance rate (so called **genotypic error rate**).

The phenotypic features, on the other hand, do not set limits on the false acceptance rate, but it is clear that the phenotypic variation over time imposes a lower limit on the false rejection rate (so called **phenotypic error rate**).

More precisely, the performance of biometric techniques is determined by two kinds of variability among the acquired biometric characteristics:

- **Within-subject variability:** As biometric measurements are never the same the biometric system must accept similar biometric characteristics as a true match. Although the matching algorithm may allow for a variability of the input measurements, it is clear that higher within-subject variability implies more false rejects. Therefore within-subject variability sets the lower limit on the false rejection rate.
- **Between-subject variability:** If between-subject variability is low then it is more difficult to distinguish two subjects and a false accept may occur. The lower between-subject variability the higher false acceptance rate. Therefore between-subject variability sets the lower limit on the false acceptance rate. An ideal biometrics has very high between-subject variability.

2.1.2.3 Error rates

The interaction with a biometric system starts with the enrolment. The aim of the enrolment is to capture **biometric data** of the user for further authentication/identification attempts. Because this biometric data will be used as a reference for all subsequent comparisons, the quality of the enrolment data is very important and significantly influences the performance of the system.

During the processing of biometric samples, the system evaluates the quality of the sample (e.g. the number of feature points extracted). If the quality of the input sample is not sufficient for the enrolment, the sample must be re-acquired. For some individuals even repeated acquisitions of biometric data do not yield sufficiently good samples and consequently the enrolment fails.

The probability of a person not being able to enrol in a biometric system is called the Fail to Enrol rate (FTE). It is computed as a fraction³ of people who could not enrol in the system out of the complete group of people. The FTE rate includes people without fingers (for fingerprint systems), visually impaired people (for iris-based systems), etc.

Sometimes the minimal quality required for a successful enrolment can be configured. It is clear, however, that the stricter the quality control at the time of enrolment (i.e. the better quality of the template), the better results later in verification/identification

² The probability that a person has an identical twin is estimated as 0.8% [DAUG98].

³ The computation gets more complicated when some people can enrol only sometimes (i.e. their enrolment sometimes succeeds, sometimes fails). In such a case the personal FTE is computed (i.e., fraction of unsuccessful enrolments in all enrolment attempts of that person) and then the personal FTE rates are averaged.



attempts and vice versa. Therefore matching error rates can be traded off with the enrolment quality requirements. In 2004 Atos Origin (commissioned by the UK Passport Service) ran a biometric trial. Facial, iris and fingerprint systems were tested in real conditions with 3 groups of participants: Quota (representative sample of the population), Opportunistic (volunteers) and Disabled (several types of disabilities). The results can be briefly summed up in Table 1. It is worth noting that being stricter at the time of enrolment (higher FTE value) brings better matching error rates (FNMR) and vice versa. For details (explanation of some the results, shortcomings of the trial etc.) see the final report of the trial [UK05].

	Face				Iris				Fingerprint			
	FTE	FTA	FNMR	FRR	FTE	FTA	FNMR	FRR	FTE	FTA	FNMR	FRR
Quota	0,15%	0,00%	30,82%	30,92%	12,30%	0,44%	1,75%	14,22%	0,69%	6,98%	11,70%	19,24%
Disabled	2,27%	0,00%	51,57%	52,67%	39,00%	0,68%	8,22%	44,43%	3,91%	3,14%	16,35%	22,64%

Table 1: The error rates of facial, iris and fingerprint systems in a UK 2004 enrolment trial [UK05].

For verification/identification attempts, the biometric input sample is obtained and its quality is verified. If the quality does not satisfy certain minimal quality requirements, the acquisition process must be repeated. If all repeated acquisitions do not yield sufficiently good samples, the person cannot be identified/verified and such an attempt increases the Fail To Acquire (FTA) rate. Sometimes the minimal quality can be configured and then it is clear that the stricter we are with the quality check the better result we get during the biometric matching process and vice versa. The FTA rate therefore can be therefore traded off with biometric matching error rates.

Input samples of sufficient quality are processed in the biometric matching algorithm. The matching algorithm compares the input sample with a template (in the case of verification) or number of templates (in the case of identification). The result of the matching algorithm is either correct or incorrect. If an error occurs, the resulting decision can either incorrectly refuse an authentic person (this is so-called false non-match – FNM) or match an impostor with another person's template (this is so called false match – FM). What happens next depends on the system policy. In the case of single attempt scenario, the verification/identification ends. In the case of, e.g., three-attempt scenario, a re-acquisition is possible if the person is not being recognized (either false non-match or correct refusal of an impostor).

The final result of an authentication/verification attempt is correct acceptance or correct refusal, false acceptance or false rejection. In the case of single-attempt scenario the FRR and FAR can be computed as:

$$FRR = FTE + FTA + FNMR$$

$$FAR = (1-FTE) \cdot (1-FTA) \cdot FMR$$

For the purpose of FAR computations the so-called **zero-effort** (also called **random forgery**) unauthorised authentication attempts are taken. In this case the unauthorised users are not actively changing their biometric characteristics (e.g., with a plastic layer around their finger).



The correct way to calculate error rates is to compute personal error rates for each person who contributes to the tests and then average the rates over the group of all the people. Otherwise, the results can be biased by multiple verification/identification attempts done by some people.

As we have seen, the accuracy/usability of biometric systems can be measured in the terms of FTE, FTA, FMR, FNMR, FAR and FRR. When comparing different systems typically only the resulting FR and FA rates are used. The FAR and FRR can be graphically expressed in a FAR-FRR graph, where both the error rates are a function of the threshold value or can be plotted in a ROC (originally **Receiver Operating Characteristics**) graph where the FAR is a function of FRR or vice versa (thus eliminating the threshold value from the graph). Figures 1 and 2 give a simplified example of such graphs. The point where FAR and FRR has the same value is called the **equal error rate (EER)** or the crossover accuracy. Such a threshold does not have a particular importance, but the resulting EER can be used as a (rather simplified) performance value of a biometric system in evaluations.

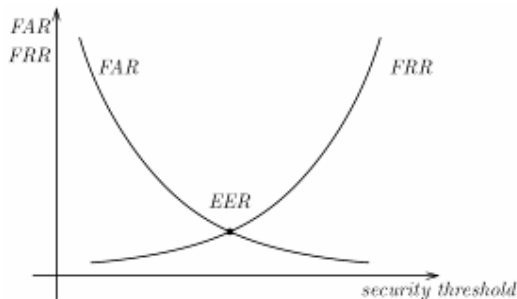


Figure 3: FAR-FRR graph

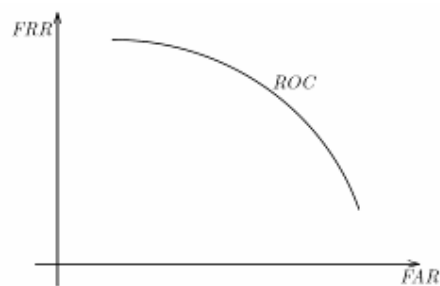


Figure 4: ROC graph

Even if biometric systems are good at recognizing people, they are never 100 % accurate. A very important factor, which influences the resulting error rates, is the quality of the input biometric data. Therefore environmental conditions, quality of the sensors and the training of users play a key role in actual implementation.

There exist a couple of different types of tests [BWG00] and not all the results must necessarily be comparable. The American National Institute of Standards and Technology (NIST) is regularly testing the accuracy of fingerprint and facial biometric systems. The verification ROC graph of facial biometric systems from 2006 at Figure 5 is one of the results of their tests. The details of the NIST tests can be found on websites fingerprint.nist.gov and face.nist.gov.

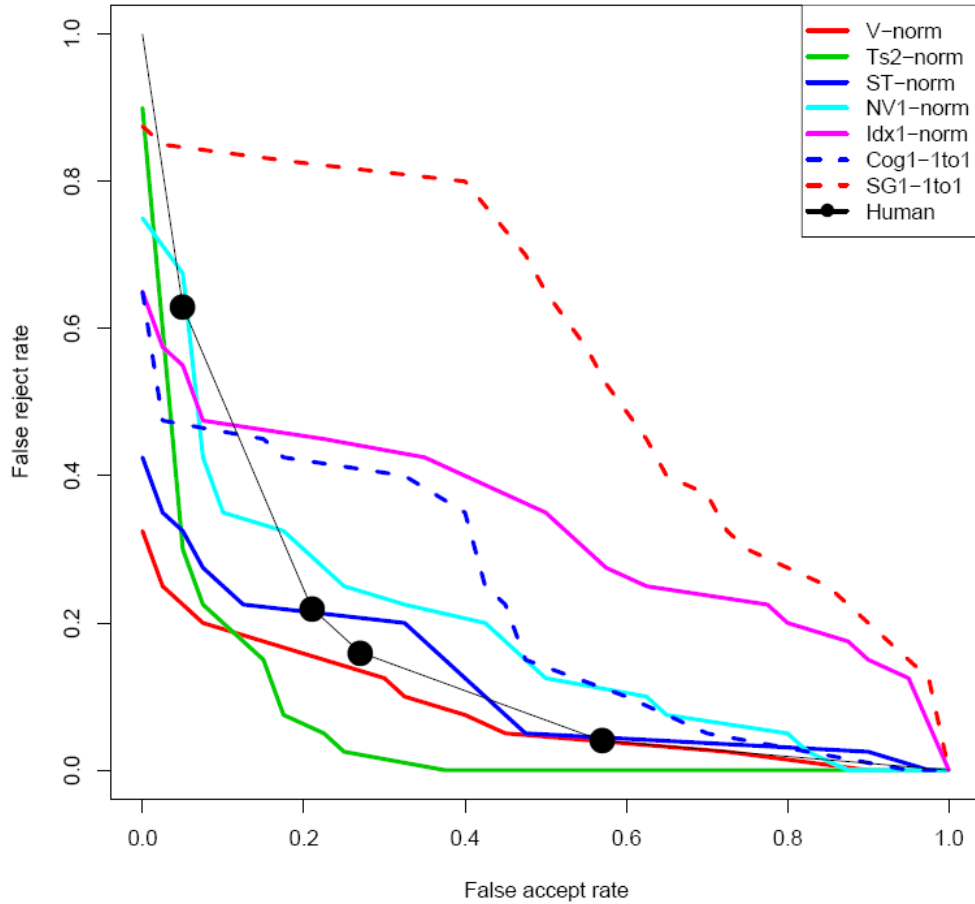


Figure 5: The ROC graph of several facial recognition algorithms (FRVT 2006 ran by NIST [FRVT06]).

In 2000 the British NPL (National Physical Laboratory) has tested several biometric systems in an office environment. The tests included facial, fingerprint, hand, iris, vein and voice systems. The single-attempt ROC (FAR vs. FRR) graph is shown at Figure .

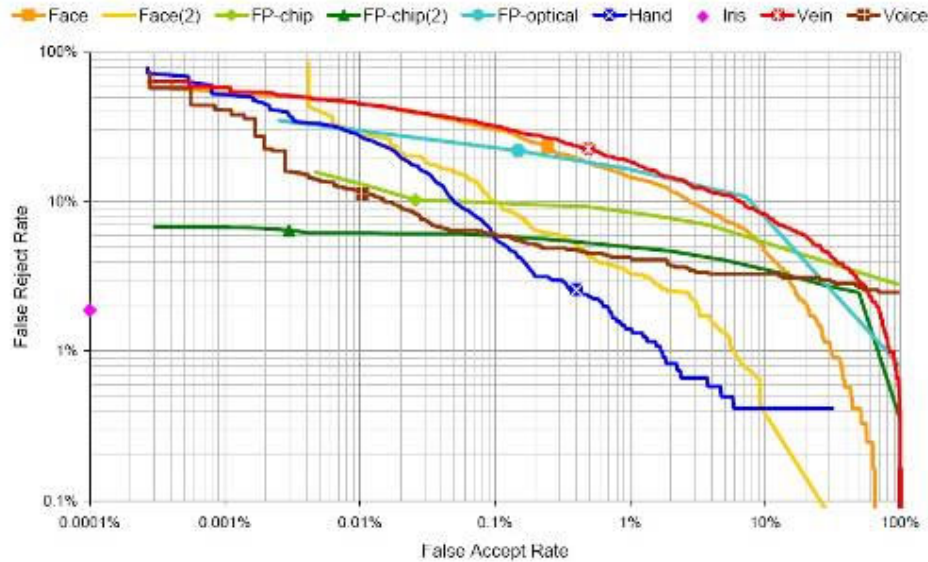


Figure 6: The ROC graph of several biometric systems (NPL 2000 test [NPL01]).

2.1.3 Large scale biometric systems

Designing a biometric system for a couple of users is relatively easy. Tuning a system for millions of users is significantly more challenging.

While the **verification** speed and accuracy is essentially the same for a system with 10 users and for a system with 10 million users, the **identification** mode makes the difference.

In addition to false rejections and false acceptances there is another type of error in identification systems. **False identification (FI)** is an identification mismatch where the user is falsely assigned to a biometric template (identity).

The value of FIR can be derived from verification FAR_1 as follows:

$$FIR_x = 1 - (1 - FAR_1)^{(x-1)}$$

where x is the number of templates in the database.

The false rejection rate of an identification system⁴ with x users remains the same $FRR_x = FRR_1$, but the false acceptance rate is a function of x :

$$FAR_x = 1 - (1 - FAR_1)^x$$

Let us illustrate the identification accuracy with an example. Let us have a biometric system with the verification FAR of 0.5 % and FRR of 5 %. The false acceptance rate of 0.5 % ($FAR_1 = 0.005$) may look attractive. Let us further have a biometric system with 100 users. If the abovementioned biometric system is used in the identification mode, the following identification accuracy is achieved:

⁴ Here we simplify and assume that one-to-many match is performed as series of x one-to-one matches. The identification system typically uses clustered databases and runs the comparisons only within the relevant part of it. No matter whether the matches are done explicitly or implicitly the size of the whole database is a crucial factor for the accuracy of the system.



$$FAR_{100} = 1 - (1 - FAR_1)^{100} = 1 - 0.995^{100} \cong 0.3942 = 39.42\%$$

$$FRR_{100} = FRR_1 = 5\%$$

A system with the FAR of nearly 40 % is useless. Even if the verification FAR of 0.5 % may look impressive it is not suitable for identification even within a small group of people. Large scale identification systems need algorithms with much better accuracy. Currently only the top fingerprint and iris based systems are suitable for identification within larger databases.

2.1.4 The liveness problem

Attackers could try to employ some means to make one person match someone else's recorded biometric characteristics or at least to change their own biometric characteristics to remove any subsequent match to a hotlist. Examples of such attacks can be silicon fingerprint layers or irises with printed patterns. To stop such attacks or at least make them more difficult, the biometric input devices must implement so called liveness (or also liveliness) tests. However, the design of a secure and reliable liveness test is a real challenge and in fact many liveness tests under certain circumstances reject genuine users (e.g. users' fingers are too dry).

Liveness tests are specific for a particular biometric modality and can be roughly divided into two categories. Static tests measure some physiological characteristics (like the finger temperature or conductivity) that discriminate between the living human and an artificial fake. Dynamic tests verify the reaction of the user to an impulse. The impulse can be the increase in light intensity to see the pupil contraction or asking the user to pronounce a particular phrase.

Many various kinds of liveness tests are used today. For example to verify the liveliness of the fingerprints it is possible to measure the temperature, reaction to hot and cold stimulus or pressure stimulus, conductivity and other electrical properties, the perspiration, optical properties of the skin, contact scattering, pulse or blood oxygenation. For the iris liveness test we can use hippidus effect, reaction to the volume or position of the illumination or look at the Fourier plane to deal with colour contact lenses. Facial recognition systems either use several cameras to obtain 3D properties of the head (to avoid simple attacks with a photo) or ask the user for a particular reaction (to blink, to move left or right, to open or close the mouth).

Unfortunately, many liveness tests are weak and can be easily fooled by using materials having the same properties as the human body or can be simulated in other ways. It is by no means trivial to come with a liveness test that would be very difficult to fool and would not reject too many genuine users. For example, it is not sufficient to measure the brain activity of the user to verify she is in fact alive if the user is using a plastic layer on her finger to fool the reader. The liveness test is therefore not only about measuring the liveliness of the user but more or less about resistance to attacks with non-genuine biometric samples (sometimes the term **liveness+** is used). It is sometimes claimed that if you know what the liveness test is looking for you can always fake it. This is also the reason why details of many liveness tests are kept secret and evaluation of their security is not possible or at least not straightforward. In the past, many readers could easily be fooled with simple biometric copies. Many cheap fingerprint readers can be cheated with silicon or gelatine copies of fingers [MATS02, CCC04]. It is also necessary to



	separated by <
Ccccccccc	passport number
K	check digit of the previous field
Nnn	citizenship of the holder
RRMMDD	date of birth of the holder
G	gender (F for female, M for male)
Rrmmdd	expiration date of the passport
Ooooooooooooo	optional data (e.g. personal number)
X	check digit of the whole line

Table 2: Composition of the MRZ.

Because the amount of data storable in the MRZ is only very small (88 characters) and the only security factor is the check digit, new ways of storing data for automated processing have been investigated. The latest version of the ICAO standard 9303 uses the technology of contactless smartcards (a kind of RFID), asymmetric cryptography and biometrics. New passports equipped with contactless chips are called electronic passports. Electronic passports are marked with a special logo.



Picture 5: Symbol used to label electronic passports [ICAO04].

2.2.2 Contactless smartcard technology

RFID (Radio Frequency Identification) [WIKI07] is a collective name for technologies transmitting data by using an electromagnetic field. There is a range of RFID standards varying in the frequency used and the distance they are able to communicate over. There are two major categories of RFID chips: active and passive. Active devices have their own source of energy, are able to communicate over a longer distance and can use more complicated processors. Passive devices on the contrary do not have their own source of energy and rely on the energy obtained by induction from the electromagnetic field of the reader. They can operate only in the proximity of the reader. Thanks to the limited source of energy their complexity (also computational capacity) is restricted and the distance they can communicate over is also shorter than in the case of active RFID devices.

Due to a relatively long lifetime of passports (up to 10 years) and limited lifetime of batteries in active RFID devices, passports can only use passive RFID chips (see [ICAO04_2] annex I). As the amount of data that needs to be stored in passports is relatively large, many RFID standards (proprietary technologies are not suitable for global interoperability) cannot be used because the supported amount of data is too low (hundreds of bytes at maximum - e.g. ISO 15693). Due to many restrictive conditions, ICAO chose the standard ISO 14443 (in both its variants A and B) for use in electronic passports. The standard uses the frequency 13.56 MHz and enables contactless communication over a distance of up to 10 cm at a speed of 106 kbps (up to 848 kbps is possible, but not required at this moment) (see [ICAO04_2] Annex I).



RFID devices consist of a small integrated circuit (chip) and antenna which is used to obtain energy and to communicate. The reader creates a strong electromagnetic field and thanks to inductive coupling the RFID obtains energy. The reader at the same time uses this electromagnetic field for communication with the RFID chip by using amplitude modulation (in the A variant of the standard 100% amplitude modulation is used (i.e. for bit 0 the field is switched off completely), in the B variant it is only 10 % (i.e. for the bit 0 the strength of the field drops from 100 % to 90 %)). For communication from the chip to the reader the chip uses a load resistor. The reader monitors the amount of energy provided to the chip and recognizes data “transmitted” by the chip (so called load modulation). The standard also addresses situations where there are several chips within the reader’s range. In such a case the reader communicates with the chips one after another. Such an algorithm (a so called anticollision algorithm) is different for different versions of the standard. The A version uses a binary tree (i.e. serial numbers of the chips are important), the B version uses a slotted Aloha algorithm (the order is random).

Although the anticipated communication distance is in the range of 0-10 cm, it does not mean automatically that communication is not possible over longer distances. If a potential attacker constructs a special reader with a stronger electromagnetic field (in particular if he does not respect limits imposed by hygienic norms) then he can achieve communication over longer distances. Passive eavesdropping is also possible at distances larger than the anticipated communication range.

Devices based on the ISO 14443 standard are often called “contactless smartcards” (and not RFID chips/tags which are generally understood as simple identification chips readable over a distance of at least several decimetres).

2.2.3 Security of the electronic passport

The main reason to introduce electronic passports is the increased security of passports, faster reading speed and larger storage space.

Data stored in the electronic passport must be digitally signed by the issuing institution. This is an important security factor, because even in cases when a counterfeiter has the newest technical equipment for printing and personalization of the passport at his disposal, he will not be able to create the correct digital signature of the fake data without access to the proper country private key. This way of protecting the data is called **passive authentication** and is an obligatory part of every electronic passport. Passive authentication cannot prevent production of exact copies of data. To avoid such copying, additional techniques are necessary (active authentication, see below). The Public Key Infrastructure (PKI) hierarchy for passive authentication is reduced to a single level [ICAO04]. Every state creates its own national Certificate Authority (CA) which signs the document signing authority keys; these authorities then sign data in electronic passports.

Data in the electronic passports can be remotely readable by anybody without authentication. Most countries, however, have decided to implement a protection mechanism called **Basic Access Control** (in EU countries this is in fact mandatory). Basic Access Control is an authentication mechanism that only allows reading the data



after authentication which requires knowledge of some data printed in the passport. These data items can only be obtained after the passport is open, therefore we can assume that successful authentication will imply the readers have the passport in their physical possession (i.e. this happens with the consent of the passport holder). Technically the passport number, birthday of the holder and the passport expiry date are hashed and such a hash is used to obtain two 3DES keys to authenticate and establish a shared encryption key, which is then used to secure subsequent communication. This way the whole communication is secured against eavesdropping. A well known shortcoming of the basic access control is the small entropy in the data used to authenticate. Although the theoretical maximum is about 56 bits, not all the values are equally probable and thanks to additional knowledge it is possible to execute an attack in a more efficient way than just by trying all possible values.

The use of digital signatures for data integrity does not imply that the attacker cannot read all the data including the digital signatures from the chip and create another chip into which this data are loaded (so called passport cloning). Against such attacks, the electronic passports can be equipped with a technology that is called **active authentication**. In the passport chip an asymmetric private key is stored. Such a key never leaves the chip (there is no command to read the key), the reader can only verify whether the chip has access to the private key. The public key of the chip (including the digital signature made by the issuing authority) is part of the readable data. The reader reads the key and then by using a challenge-response protocol verifies if the chip has got access to the private key corresponding with the public key. Therefore, the counterfeiter cannot make a complete copy of the chip, because the private key cannot be read from the original chip. He also cannot create another pair of keys because the public key must be digitally signed by the issuing authority (verification of the public key digital signature is therefore an important part of active authentication). The impossibility of reading the private key from the chip is based on the assumption of the chip's tamper resistance.

2.2.4 Data structure

The data structure on the chip uses a file system where the directories are called dedicated files (DF) and files are so called elementary files (EF). The data are stored in several files in a common directory. One file (EF.COM) is reserved for metadata (data format version and the list of stored data groups), one file (EF.SO_D) contains information about security (digital signatures of hashes of all the files) and other files include the data, which are grouped into several data groups (DG). The list of data groups is shown in the table number 1.

Data group	Stored data
DG1	Machine readable zone (MRZ),
DG2	Biometric data: face
DG3	Biometric data: fingerprints
DG4	Biometric data: iris
DG5	Picture of the holder as printed in the passport
DG6	Reserved for future use
DG7	Signature of the holder as printed in the passport
DG8	Encoded security features – data features
DG9	Encoded security features –structure features



DG10	Encoded security features – substance features
DG11	Additional personal details (address, phone)
DG12	Additional document details (issue date, issued by)
DG13	Optional data (anything)
DG14	Data for securing secondary biometrics (EAC)
DG15	Active Authentication public key info
DG16	Next of kin

Table 3: The data structure of electronic passports.

In the future the DG17 will be used for automated border clearance, DG18 for electronic visas and DG19 for travel records. Currently the format of these data groups is not standardized.

2.2.5 Biometric data

Electronic passports enable the storage of large amounts of data. Such storage space is typically used to store biometric data. In accordance with the ICAO standard the chip has to include a facial image of the holder. Other biometric characteristics (possible alternatives are fingerprints or iris scans) are only optional and the decision whether to store them on the chip or not is left up to the issuing state.

Most member states of the EU started issuing electronic passports with the face of the holder in DG2 at the latest on 28 August 2006 and after 28 June 2009 passports also have to include fingerprints in DG3. Access to fingerprints is protected by so-called **Extended Access Control**, which ensures that only authorized parties can read the sensitive data.

The possibility of biometric verification is an important security factor for electronic passports accompanied by biometric data (so called biometric passports). Even if the picture of the holder can also be verified manually, automated biometric verification is more accurate and can be done without the presence of border control staff. The major disadvantage of biometric verification based on the face matching is its high error rate (even so, automated verification is usually more accurate than manual verification). In the case of controlled light conditions, the error rate (in terms of rejecting authorized holders – FRR) can reach about 10% (and the probability of an unauthorized acceptance – FAR of 1 %), in cases where the light conditions cannot be optimized for the biometric system the error rate can even reach 50 % [EZO05]. The accuracy for example achievable with biometric systems based on fingerprints is FRR around 0.5% at a FAR of 0.1%. [EZO05].

2.3 Biometric border crossing

The use of biometric characteristics in border control is nothing new. Passports have contained the image of the holder for about 100 years and before that a verbal description of the holder and his/her characteristic features was used. What is new is the automation. As soon as the biometric characteristics are reliably processable by computers, such biometric systems have the potential to automate the border crossing for example for low risk passengers. This could free border guards from routine checks so that they can focus on higher risk passengers. The first such cases already appeared at the end of the last century. In 1992 Amsterdam Schiphol Airport, as the first airport



in the world, introduced the Schiphol Travel Pass, a fingerprint-based predecessor of the current Privium system. The border control of Palestinians working in Israel has been facilitated by a biometric system based on facial recognition and hand geometry. In many cases the biometric systems do not constitute fully automated border control systems, but only form a part of the checks done during the border control. The American programme US-VISIT, the European biometric visa project BIODEV and the British experimental system miSense all belong to that category.

2.3.1 The concept

The idea of automated biometric border control is simple. Like in any other biometric system the user must be enrolled first. The enrolment links the biometric data with the identity (passport and other immigration data in this case). Biometric data can be stored in a central database, a separate smartcard or directly in the electronic passport. As soon as the passenger is enrolled, he/she can benefit from the automated biometric border control system. Instead of the classical encounter with an immigration officer, the passengers use the lane with a biometric device, which acquires the biometric characteristics and then either directly identifies the passenger or, with the support of some identification device the passenger presents to the system (passport or smartcard), obtains the biometric template and verifies the identity of the passenger. If the biometric matching (and possibly other checks) is successful, the way forward is open.

2.3.2 The implementation

Even if the basic idea of biometric border control is simple, that does not mean that the actual implementation is easy. The complete system needs to be carefully designed to ensure secure, convenient and efficient operations.

2.3.2.1 Biometrics

The first point to focus on will be the biometrics and the ways to store and protect the biometric data. Because the passengers are obliged to carry a valid travel document when crossing the border, one logical option is to use the biometric data stored there. ID cards of most EU countries do not contain any machine readable biometric data so far although in the future it is likely that they will. However, electronic passports (with contactless chip) are designed to carry biometric data in machine readable form. Currently, electronic passports of EU member states only include facial pictures of the holder (in the form of a JPEG or JPG2000 image with optional coordinates of certain facial features). Unfortunately, biometric systems based on facial recognition are significantly affected by light conditions and their error rates are relatively high. This limits the application of facial biometric systems for border control to a certain extent. Nevertheless, the Australians have introduced a project called SmartGate which uses facial pictures in passports for automated border control. Thanks to controlled light conditions the false rejection rate is kept under 10%. A biometric system based on facial biometric has been also implemented at the airport in Santiago in Chile as well as Faro and Lisbon airports in Portugal.

Electronic passports are ready to carry secondary biometric data by means of fingerprints or irises. Such data were not available in EU passports in the past. As soon as the biometric data will be stored in passports, they will be usable for reliable automated border control. According to EU regulations, the storage of fingerprints will be mandatory for EU member states and the deadline to introduce fingerprints into



passports is set for June 2009 at the latest. Fingerprints in European passports will be stored in the form of WSQ-compressed images of both the index fingers. Reading access to secondary biometrics will only be given to authorized border control authorities. Biometric data in electronic passports are digitally signed by the issuing country, so both integrity and confidentiality of the secondary biometric data are guaranteed.

If the biometric registered traveller system does not rely on electronic passports, then it needs its own biometric enrolment. In such a case it is not bound to ICAO-chosen biometric modalities (face, fingerprint and iris), but any large scale system will naturally prefer proven methods and therefore fingerprints and irises will play an important role here.

There are principally two options on how to store the biometric data. Either a central system (database) is used or portable data storage is issued to the traveller. When using the passenger held data storage the data integrity and confidentiality must be assured. Whenever the biometric data are stored in the central database, the dual identity check can be performed during the enrolment and the biometric system at the border can work in the identification mode (systems based on fingerprints or irises are both sufficiently accurate even for identifications within larger databases).

From the perspective of passenger privacy, any secure means for user-held storage (where the database storage is omitted) is an advantage. From the passenger user friendliness point of view, any additional card might be less convenient. Concerning user friendliness, the systems working in the identification mode and not requiring any passport or token are the more user-friendly ones.

Systems, which use the Machine Readable Zone (MRZ) of the passports as pointers for database records, also have the advantage that the automated system verifies the passenger has got his/her travel document with him/her.

2.3.2.2 Enrolment

During the enrolment, the biometric data are bound to data in the travel document (typically, the passport is required). From the security point of view the travel document must be carefully inspected (to reveal possible fakes), because during next biometric checks the passport will not be checked by the border officer anymore. This check includes the inspection of physical security features like watermarks, security printing, optically changing images etc. and is in fact similar to a thorough border check of a passport.

Naturally, also the current appearance of the traveller is checked against the photo in the passport. Care must be taken to make sure the enrolled biometric data are genuine biometrics of the passport holder (i.e. no silicon fingerprints or iris patterns printed on contact lenses). Based on the country and its legislation also the police database check may be necessary. That can be only a simple SIS (Schengen Information System) look up or a complete search including also local/national database as required by EU legislation for third country nationals.



Enrolments are usually limited by age above 18 years and by the citizenship of a particular set of countries (in the EU typically all EU countries – as these border crossings do not require visas and stamps in passports).

2.3.2.3 Border crossing

Biometric border crossing uses dedicated lanes with biometric scanning devices. The crossing point is usually designed as a so-called man-trap. When the passenger indicates interest in crossing the border (e.g. inserts the passport or a smartcard), the first door opens. After the passenger has entered, the door closes and the passenger must be biometrically verified / identified. At the same time, the police database check could be done (principally the same as during classical border check). If all the checks succeed, the door on the other side opens and the passenger can proceed. If any of the checks fail (e.g. the fingerprint is too dry or wet or the police database search does not succeed within a specified timeout), the side door opens and the passenger is directed to the border officer, who proceeds with the classical border check. There can be situations where the record in the police database indicates a wanted person. In such a case, the passenger remains “locked” in the mantrap until the police arrive.



Picture 6: The automated border crossing booth at Paris Charles de Gaulle Airport.

Depending on whether the automated border passage is unmanned or not, it might also be necessary to automatically verify that only a single person enters the man-trap (unicity detection) and that the biometric data are genuine (liveness detection).



2.3.3 Disabled passengers

Current systems do not support disabled people. This group of people typically already have a priority at the classical border check. Nevertheless, some systems could be used by people with certain disabilities. If the kind of disability excludes the person from the biometric enrolment, then this person cannot use the system. In some systems, certain constraints like geometrical dimensions for wheel chair users are taken into account, which allows this group of disabled people to benefit from the system.

2.3.4 Different types of border crossings

Automated border crossing systems based on biometrics work best in a controlled environment, where the flow of people is regulated and the conditions where the biometric data are obtained are controlled. This means that automated biometric border crossing systems are well suited for airports and major seaports. However, adapting them to landborders might be more challenging.



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA.

3 Case studies

In this chapter the four case studies are reported.

3.1 Amsterdam Schiphol Airport

3.1.1 Short description of the airport

Amsterdam Airport Schiphol in the Netherlands, abbreviation AMS and better known as Schiphol, is the 4th largest airport in Europe and the 10th worldwide. The airport has 5 runways and serves around 265 destinations worldwide. More than 150 destinations are situated in Europe. The remaining destinations are intercontinental. For 2007 there will be around 7,000 more flights compared to 2006 which leads to an amount of 430,000 flights to and from AMS.

The airport has a one terminal concept, with everything under one roof. Within this single terminal it has 4 arrival and departure halls. There is a Non-Schengen border control, a Schengen dedicated passage for security checks and a transit border control.

Air France – KLM is the most important client of the airport, but there are more than 90 companies flying to and from AMS. Fifteen of these companies are only transporting cargo. Cargo at AMS is as much as 1.5 million tons of goods. For 2007 almost 1.6 million tons are expected to be moved.

More than 46 million passengers travelled from and to AMS in 2006. The Schiphol Group expects the number of passengers to be almost 48 million in 2007. Around 40% of all passengers are travelling for business. The remaining passengers are tourists. 42% are travelling to AMS only for transit. AMS is a typical hub-and-spoke airport.

At Schiphol 57,970 people work from 543 companies (data from October 31st 2005). More than 70% of them do not have a nine-to-five job but work on a shift basis. This also includes the 12,000 persons qualified as flying personnel.

Amsterdam Schiphol Airport is a part of the Schiphol Group.

3.1.2 The project

The automated border crossing programme, named Privium by the Schiphol Group, started on October 23rd 2001 as a 1 year trial and has been in operation since October 23rd 2002 after the Ministry of Justice and the Koninklijke (Royal) Marechaussee stated that the pilot project on iris scan technology satisfied all security requirements. There is no intention to end this programme, as it is in operation and continues to be updated.

All Privium systems including the biometric systems are developed by Schiphol Group itself. In 2002 Schiphol Group transferred all knowledge and products it required with both the Privium and staff access control solutions to a separate daughter company named Dartagnan (fully owned since 2004) that maintains the Privium systems and is involved in several innovations for fast lanes at Schiphol Airport.



At the core of the Privium programme is the member smartcard. This contact smart card includes three elementary files: the passport data which are the so called “search string”, used for queries in the police databases, the Privium member number (relates to the membership database maintained by Schiphol Group) and two encrypted iris codes. These data are protected by authentication for confidentiality and by MAC (message authentication code) codes for integrity. The biometric data are additionally encrypted.

The iris cameras used are the LG Iris 3000 EOU for enrolment and the 3000 ROU for verification, but they are to be replaced by the 4000 models in the future. The biometric matching/verification software is provided by the LG SDK.

3.1.2.1 The users

Privium aims to facilitate the airports most frequent users (around 1% of the traveller population responsible for around 10% of the total traveller movements). Membership is open to the passport holders of all EU countries as well as Norway, Iceland, Liechtenstein and Switzerland. Also children can be enrolled but border police officer makes sure that no unaccompanied children cross the border. Persons should have a height of at least 1.5 m due to the iris scan camera which is at the height of 1.3 m.

Wheelchair passengers cannot be enrolled to Privium as the construction of the automatic border passage is not accessible for disabled people. Disabled people, if accompanied, always have priority at border passage.

As of beginning of 2007, Privium has around 36,000 members and grows by about 600 new members per month. There are two types of Privium memberships available: Privium Basic, costs € 99/year and Privium Plus which costs 119 €/year. Partners of a member have a 20% reduction, also children have this reduction. Around 94% of the members renew their subscription.

“Privium Basic” provides the members with convenient border and security passage. “Privium Plus” provides also priority parking, discount on Schiphol Valet Parking and business class check-in with any ticket at the check-in counters of the participating airlines to its members. Over twenty airlines are taking a part in the program.

Privium members collectively pass through the Privium passages at Amsterdam Airport Schiphol using iris recognition on average 13,000 times a week. At peak moments 450 passengers / hour use the biometric system through the 11 available Privium gates.

3.1.3 Procedures – Enrolment – Biometrics

Privium is a public private cooperation between Schiphol Group and the Dutch Royal Marechaussee and Immigration and Naturalisation Service. The public private partnership has the following division of roles and responsibilities:

- The Government Authorities set the rules and requirements of the border passage facilities and procedures in particular, determine eligibility of membership applications and are responsible and in control of (in fact oversee) every automated border passage.
- Schiphol Group has invested in Privium and operates the programme including all border passage facilities. All communication with customers, the performance,



quality and availability of programme facilities and services as well as payment processing are the responsibility of Schiphol Group.

Procedures: To be enrolled a valid passport is needed. The candidate has to provide a lot of information such as: exact data as on passport, address, which membership the person wants to apply for, how to pay the membership amount, how many flights the passenger makes on a yearly base from and to Schiphol, etc.



Picture 7: The PRIVIUM enrolment station.

Enrolment: The whole enrolment process takes about 15 to 20 minutes and is in 90% of all cases by appointment. Biometric enrolment is only a small part of the whole procedure as there is also the pre-enrolment. During this pre-enrolment the commercial database has to be filled in and the smartcard is prepared for the final enrolment. The enrolment is finalised in the governmental office and the card is issued to the passenger.

Authenticity of the passport is verified by a police check when a criminal search (including a list of unpaid fines) is done through blacklist databases. The Royal Marechaussee can deny the registration without giving a reason.



Picture 8: Controlling the light at the enrolment.

Enrolment: There is one enrolment point with two pre-enrolment computers, one police computer, four enrolment computers and finally two practice kiosks. Pre-enrolment can also be done on-line. The enrolment centre is open from 6:00 until 21:00 hrs. Around 600 people enrol every month.

The passengers can try to enrol as often as they want if there are some technical problems regarding the enrolment. As far as known, the fail to enrol rate is 0%. Only in one case has the enrolment been more problematic.



PRIVIUM MEMBERSHIP APPLICATION FORM



Please complete this form in capital letters. Mark the appropriate boxes with an X.
All boxes marked with an [*] must be completed.

Please provide details EXACTLY as recorded in your travel document (passport/European identity card)!

Personal details

Mr* Ms*

All initials* _____

Title(s) _____

Full surname* _____

Maiden name (if married*) _____

Date of birth* day month year

Place of birth* _____

Nationality* (only an EEA country or Switzerland) _____

Travel document* passport European identity card

Travel document number* _____

Expiry date* day month year

Home address

Street name* _____

House number* _____

Address suffix _____

Postal code* _____

City* _____

State/Province* _____

Country* _____

Home telephone number _____

Business telephone number _____

E-mail address _____

Invoice address

Name of person or company _____

Street name or P.O. Box number _____

House number _____

Postal code _____

City _____

State/Province _____

Country _____

Correspondence address*

Please send correspondence to my: home address invoice address

I would prefer to receive Privium correspondence in: English Dutch

By what surname do you wish to be addressed when receiving correspondence from Privium?
(if different from surname entered under personal details above)

Full surname _____

From time to time we send our members details of special Privium benefits and events.

Do you wish to be informed about these? yes no

If so, how would you prefer to receive the details? post e-mail

E-mail address (if different from that entered under home address above) _____

Types of membership*

Privium offers two types of membership. For which type of membership do you wish to apply?

Privium Plus (€ 119 per year): fast border passage, priority parking and Business Class check-in

Privium Basic (€ 99 per year): fast border passage

After you have received your Privium Card, you can apply for a Partner Card (€ 55).

Method of payment*

Which of the following payment methods do you wish to use to settle your account? (one choice only)

Bank transfer (only within the Netherlands)

Direct debit from bank or giro account (only within the Netherlands)
bank/giro account number _____

Credit card (your first credit card payment is required to be made at the Privium Service Point, when you collect your Privium Card)

Other information

How did you learn about Privium? advertisement brochure direct mail word of mouth seen on Schiphol Airport other

On average, how many times a year do you fly from (or via) Amsterdam Airport Schiphol? _____

Signature

The undersigned declares that he/she has read and agrees with the Privium General Terms and Conditions contained in this brochure.
The information I have given in this form is true and correct.

Date*: ___ day ___ month ___ year Signature*: _____

Thank you for your application! We will send you a confirmation of your application shortly together with an invitation to make an appointment at the Privium Service Point.

Picture 9: Enrolment form



Schiphol has also applied iris recognition for staff access control at Amsterdam Airport Schiphol. Around 40% of the 60,000 staff working at Schiphol Airport (only those who need access to restricted areas) have had their iris picture taken and stored on their ID badge. There are around 15 enrolment points for staff and around 40 special mantrap doors around the airport where staff can get access to restricted areas. During passage, a picture of the iris is compared to the iris picture stored on the ID badge.

Biometric: In 2000 AMS chose to use the iris biometric. AMS has performed several biometric comparison tests and has conducted interviews with system test users, to come to the biometric system of choice. The criteria that Schiphol used for the selection were accuracy, speed of recognition, ease of use, hygiene and invasiveness. Iris recognition had the best overall score on the weighted criteria set that was used.

At the Privium service point a scan is made of the iris, from which a maximum of 256 measuring points can be recognised. These measuring points can be used to reproduce the pattern of light and dark of the iris, which is unique to every individual. The scan is stored on the Privium Card when it is issued. When a passenger crosses the border, the iris is scanned and the data obtained is compared with the data stored on the card.



Picture 10: The PRIVIUM gate.

At least thirty photographs are made of the eye in less than a second. These are simple, digital, black and white photographs. No flash is used, but three weak red lights light up the eye from three different angles. A code is calculated on the basis of one of the photographs and this code is then compared with the code stored on the Privium Card.



3.1.4 Biometric error rates

Error rates are very low. There is a false operational false rejection rate of around 1.5% (that is the rejection rate at the automated border passage gates made up of not only biometric verification, but also reading of smartcard, watchlist checks, gate mechanics etc.)

3.1.5 Problems

Blacklist databases and the network connection operated by the Dutch Authorities can be down affecting regular functioning of the system. In such a situation the passengers are always directed to the border officers.

There can also be a number of reasons why the iris scan does not go smoothly. The passenger should make sure that he keeps a distance of 10 cm to 15 cm between his eye and the iris scanner, and that he can only see one eye in the scanner. Passenger has to keep his eye still in front of the iris scanner and continue to stand still until the computer indicates 'identification is completed. If the iris scan does not work, he will be taken to the front of the queue at 'regular passport control'. In this case, the passenger will not have to go to the back of the queue; a police officer will check the passport straight away.

The average speed to pass the procedure is about 12 seconds. This speed is comparable to the manual procedure as this one takes from 12 to 17 seconds. The user has only one attempt. During this attempt the iris gets matched against two stored eye templates. There is also a time-out for capturing the iris. Privium has a policy of having not more than three passengers waiting for being checked by the biometric check-point. If during peak hours waiting times increase, Schiphol extends the capacity of the gates.

3.1.6 Security

The Royal Marechaussee is in charge of border control at AMS. As already mentioned, this (military) police force is involved in the biometric enrolment and automated border passage.

Privium members using their privileged lane are guided by a TFT LCD display, indicating the gate's status. The border police officer controls the gate using a console at the officer's desk. The gate is a kind of man-trap, but it is still possible to jump over it.



Picture 11: Indication for enrolled passengers.

Members should be aware that the Royal Marechaussee carries out random passport checks. At least a few checks are done every day. The Marechaussee will check the passport and the boarding pass. Indeed, it is not allowed to use the Privium card when not in possession of a ticket as this ticket is needed to enter the clean area.

Schiphol Group satisfies all the statutory requirements with respect to privacy. No personal information is passed on to third parties. For the automatic border passage, the same information is passed on to the Marechaussee via a system link as would be passed on during a regular passport control at the border. The biometric information is stored locally (on the chip of the Privium Card) and not in a database. The plan for the use of the details of Privium members, including the use of information for the benefit of automatic border passage was approved by the Dutch Data Registration Authority. Furthermore, the Schiphol network and the Royal Marechaussee network are completely separate at the automatic border passage and no information is exchanged between the two systems. Biometric data from the biometric checkpoints is not kept but are deleted. This means that no information is logged.

Furthermore, Privium cannot be used once a passport has expired. This means also that the automatic border passage cannot be used. Upon loss or theft of the membership card, the customer has to inform Privium and the card will be blocked.

3.1.7 Costs

No cost information is available.



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA.

3.2 Frankfurt airport

3.2.1 General characteristics of Frankfurt airport

Frankfurt Airport (FRA) is the largest airport in Germany and third largest in Europe serving as an important hub for international flights from around the world. The airport is run by Fraport AG.

Frankfurt currently serves more destinations (265 non-stop destinations) than London's Heathrow Airport, but in terms of passenger traffic Frankfurt is third in Europe, behind London Heathrow Airport and Paris Charles de Gaulle Airport. The passenger traffic has grown in the last few years and currently the airport serves around 53 million passengers a year (2006 est.). Passenger facilities include 481 check-in desks, 147 gates, 63 air bridges, and 3 airport hotels.

Frankfurt Airport has two passenger terminals, which are connected by corridors as well as by people movers and buses. Frankfurt Airport Terminal 1 is the larger of Frankfurt's two terminals divided into three concourses, while Terminal 2 is divided into two concourses. The airport's high cargo flow is handled by 9 cargo terminals.

To meet the growing demand in air transportation, Frankfurt airport is in need to expand its capacities. The expansion plans until the year 2015 include a fourth runway and a new Terminal 3.

3.2.2 Automated Biometrics-Supported Border Control (ABG) – Overview

Following a Europe-wide call for proposals, the Federal Ministry of the Interior has authorized a project to test automated and biometrics-supported border controls at Frankfurt Airport. In February 2004 Germany launched a new biometric border control system based on iris scanning at Frankfurt airport. This pilot project is foreseen to run until the middle of August 2007. Evaluation of the results will be carried out at the end of the pilot.

The aim of the ABG project is defined as **(1)** fast crossing, **(2)** secure system, **(3)** saving personnel resources in the longer run. German Federal Police have been testing a system to replace a part of personnel-intensive border controls with a fully automated iris recognition system. The following trend could enable to shift personnel resources to the high risk passengers and make it possible to provide both easy of use and reliable authentication, which will contribute to the efficiency of Frankfurt Airport border checks.

In this project, persons (EU/EEC and Switzerland) travelling on non-Schengen flights whose entry and exit is unproblematic from a border policing perspective may enter and leave German territory without having to go through manual border checks. Passengers who wish to participate in the project must undergo an iris scan and register with the Federal Police the resulting biometric data along with their passport data. These data



will be used to verify enrolment in the project and for biometric authentication during subsequent border crossings.

Provided on a voluntary basis, these data are used exclusively to facilitate automated border controls for project participants. The Federal Commissioner for Data Protection is monitoring the project.

Frankfurt airport has **two** biometric-enabled gates for departures and **two** for arrivals located in Terminal 1, Concourse B. The enrolment centre is located at the departure level in Terminal 1, Concourse A, Level 2 (see Figure 7)

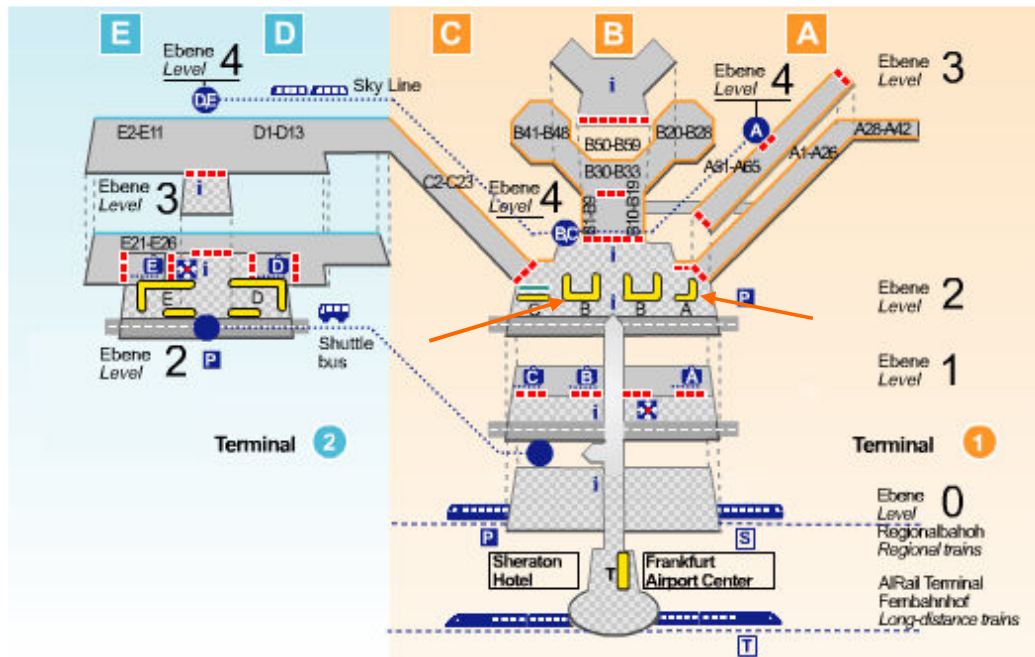


Figure 7: Position of the ABG barriers

3.2.3 Passengers

Biometric authentication system is designed for citizens of EU/EEC countries and Switzerland entitled to unrestricted freedom of movement who are 18 years or older and hold a machine-readable passport (valid for at least another six months). Citizens of other countries are not accepted at the moment. Registration is voluntary and free of charge.

As of January 2007, there were 20 900 passengers enrolled for the automated border control system. In total, the enrolled travellers pass the border 34 000 times per year.

ABG system does not have any specific user categorization nor does it have other benefits except for the automated gates offer. If the passenger wishes to opt out from the system, his/her data is simply erased (upon the request).

3.2.4 Procedure

The ABG system at Frankfurt Airport is based on OKI's IRISPASS iris recognition system. A key element in the ABG procedure is the machine-readable zone of the



passport, which all travellers must have with them whenever they cross the border. The procedure is made up of two steps **(a) enrolment initial registration in the project** and **(b) verification/automated control check when crossing the border.**

a) Enrolment

Passengers wishing to enrol in the ABG project are asked to sign a statement of consent -declaring their voluntary participation in the pilot- at the special enrolment centre located in the Terminal 1, Concourse A of Frankfurt Airport (see Figure 7). At the enrolment centre, Federal Police officers check to see whether the passport is genuine and valid. Passports with MRZ should be valid for at least six more months, so that passengers do not have to re-enrol in the project with a new passport. Passengers are allowed to enrol multiple passports by registering each passport individually. This is followed by a query of the INPOL police information system (German national system) and the Schengen Information System (SIS), as is standard procedure for conventional border checks including the passport authenticity, UV light and visual photo verification. At the enrolment more time is spent to perform the document check, thus enabling the overall security to be higher (as it has been emphasized by the ABG project group at Frankfurt airport).

If the passenger has no border police record, he/she will be asked to look into an iris recognition camera - four pictures are taken of each eye (4 images/2eyes) - which produces a biometric template of the passenger's iris scan. This is added to the passenger's personal data, encrypted and filed under his or her passport number in a local Federal Police database (ABG database).



Picture 5: The ABG enrolment.



In case of problems occurring during the enrolment process, the passengers are allowed to try to enrol not more than three times. The enrolment software also verifies the person has not been previously enrolled. A function called “fraud detection” prevents a person from enrolling multiple times with different identities.

After the enrolment process has been completed successfully, the passengers are given a statement describing their stored data (without decrypting the template) and explaining how they will be used (in accordance with sections 4a and 19 of the Federal Data Protection Act). No specific card is issued upon the enrolment since passengers are required to use their registered passport to enter the automated control lane.

Enrolment takes on average 10 minutes, including 2 minutes for iris scanning. Enrolment is followed by a simulated border control check to test whether the iris recognition procedure functions properly. It also gives the passenger an opportunity to practise using the auto control lane.


<p>Statement of Consent</p> <p>for voluntary participation in the pilot project "Automated and Biometrics-Supported Border Controls" (ABG)</p>	
<p>I hereby state that I am voluntarily participating in the pilot project "Automated and Biometrics-Supported Border Controls" (ABG) at Frankfurt Airport, described in further detail in the accompanying document. I understand that, as part of this project, personal data from my valid, machine-readable passport and data pertaining to my iris will be stored in a local ABG database and used in the automated and biometrics-supported border control procedure. These data will be used exclusively to enable me to enter and leave German territory at Frankfurt Airport via airline flights to and from non-Schengen countries without going through manual checks by border control personnel.</p> <p>The Federal Police Office at Frankfurt Airport is responsible for storing, using and guaranteeing the necessary security of these data. I understand that I may terminate my participation in the ABG project at any time and for any reason, with immediate effect and without penalty. Should I decide to end my participation, or should the ABG project be discontinued, all data related to my participation in the project will be immediately destroyed or anonymized to prevent me from being identified.</p> <p>I have been informed orally and in writing about my personal data collected and used as part of the ABG project. I understand that I may receive additional information at any time upon request.</p>	
<hr/>	<hr/>
Place and date of signing	Signature

Figure 8: Statement of Consent



b) Verification

To enter the automated border control lane, the passengers must use and place their passport on a document reader. If the passport is valid (in order for the procedure to work, the passenger must use the same travel document he/she used to enrol in the project), the data from the machine-readable zone - number and type of document, country of issue - will be transmitted electronically to the ABG database to check whether the passport holder is enrolled in the project.

If matching data are found in the database, the automatic doors to the auto control lane will open and the passenger's name, birth date and passport number will automatically be sent to INPOL/SIS to be checked against its database.



Picture 6: The passport reader in front of the automated gate.

After passing through the automatic doors, the passengers enter the inner control area – man-trap - where an iris recognition camera is located. When a passenger looks into the camera, it creates a current template of the iris, which is then compared to the template generated at enrolment and filed in the local ABG database (one image of each eye taken and matched against one stored iris template wherein the closest match counts). Every two seconds an iris image is taken and processed with maximum time set for verification to 20 seconds. If verification is successful and the passenger is not listed as a wanted person, he/ she may cross the border. Otherwise, the passenger will be directed straight to a conventional border control booth, avoiding the line, for further checks. In case the system fails while the passenger is in the auto control lane, the door to the conventional border control booth may also be used at any time as an emergency exit.



Picture 7: The ABG gates at Frankfurt airport.

Iris verification in the auto control lane takes only a few seconds. From the time passenger places the passport on the document reader until he/she crosses the border, takes only 10 to 15 seconds.



Picture 8: The inside of the automated gate.

3.2.5 Provider

BOSCH has been chosen by Federal Police as a primary contractor for the ABG pilot project at Frankfurt Airport (in accordance to the legal tender procedure). The chosen contractor provides delivery and maintenance of the hardware and software systems. As the prime contractor for the pilot project, BOSCH has been working closely with the three companies-Byometric systems, Iridian Technologies and Oki - to introduce the iris recognition system at Frankfurt Airport. Iridian is the core technology provider and patent holder for Iris recognition, Oki provided IRISPASS wherein Byometric designed and developed the iris recognition Software for the use with IRISPASS.

3.2.6 Operators

The ABG system at Frankfurt Airport is operated by the Federal Police of Germany. The current project support team entails seven enrolment specialists of which two are being present at a time for the enrolment procedures and three specialists are working on the project management itself. In case of problematic passengers who are directed by the automated system to the manual border control, border police officers – approximately 2000 border control policemen are working at the Frankfurt Airport - provide further support. Project management, enrolment, supervision of auto-control lanes as well as IT services are performed by Federal Police Officers and Federal Civil Servants.

The enrolment specialists are skilled and experienced police officers who have been selected during the selection procedure. They receive special training in languages, visual document checks as well as social skills. Additionally, they are trained to work



with enrolment applications and overall handling procedures of the system. The latter training does not exceed two hours. Training for the personnel is provided by BOSCH.

ABG system is monitored and operated by Federal Police IT specialists. Only in cases where the Federal Police is unable to solve incidents in a timely manner, the BOSCH service desk, which provides a 24/7 service in accordance with the contract, is contacted.

3.2.7 Difficulties and Problems

ABG system has not experienced any serious technical problems except for the minor ones pertaining to the document readers and INPOL database timeouts, which could affect the regular operating functions of the system.

The project group of Federal Border Police at Frankfurt airport carried out two surveys with the registered passengers to identify the user satisfaction and any existing problems concerning the user interface, ease of use and etc. Surveys have showed positive feedback – only minor details were addressed regarding the ease of iris acquisitions and MRZ recognitions.

3.2.8 Security

The data are used exclusively to enable passengers to participate in the ABG project and are stored in a local database system of Frankfurt airport. The Federal Police Office at the airport is responsible for storing and managing the data wherein only the officials, who are specially authorized to enrol and delete data, have access to stored data. The ABG database is protected by end-to-end encryption against unauthorized access. In addition, personal data are stored in encrypted form. Biometric data from biometric checks are immediately deleted after matching

ABG iris scans do not enable deduction of other information about the passengers. The ABG project involves only an automated check of the current template against the one on file, and no secondary information is created or processed. Therefore, the system cannot be used to draw any conclusions about the passenger's medical condition or other physical characteristics. Nor is it possible to reconstruct an image of the passenger's iris from the encoded file.

During the enrolment, the presence of contact lenses is detected by software programmes with possible visual inspection by the staff. Avoiding the use of printed contact lenses during enrolment is crucial for the security of the system.

It has been indicated by Federal Border Police at Frankfurt airport that ABG system has not experienced any infiltration by hackers and/or attackers. BSI has performed penetration tests wherein Federal Police have tested the system from the functional point of view.

3.2.9 Costs

No information about the costs is publicly available.



3.3 Paris Charles de Gaulle Airport

3.3.1 Airport characteristic

The Charles de Gaulle airport (also known as Roissy) in Paris (airport code CDG) is the largest airport in continental Europe. It is operated by the company “Aéroports de Paris”, which also operates some 14 other airports around Paris, 13 aerodromes (including Orly and Le Bourget) and 1 heliport. The passenger traffic has grown in the past few years and currently the airport serves around 58 million passengers a year.

The breakdown of the passenger traffic into the destination regions is illustrated in the following figure.

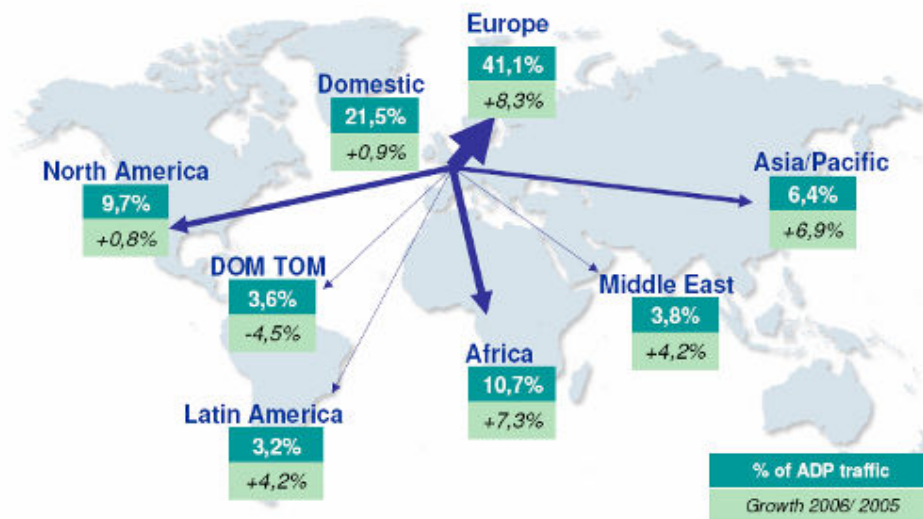


Figure 9: Breakdown of the CDG passengers into regions of the flight destination.

There are three terminals at the Paris Charles de Gaulle airport (terminal 1, 2 and 3). Terminal 2 is divided into parts A, B, C, D and E, F.

The automated biometric system for border crossing (named P.E.G.A.S.E. — Programme d’Expérimentation d’une Gestion Automatisée et SÉcurisée) is located in the terminal 2F. The system is solely used for border control, but there is another biometric system for employees’ access control to restricted areas (which is out of the scope of this study). The automated booths are open daily from 6:00 to 21:00 hrs on departure level and 24 hours a day on arrivals level.

There is one automated biometric booth for border control on departure level and one on arrivals level. The arrival booth is an older version while the departure one is the latest model. The basic functionality of both is the same, but some technical details (and the size) are different. The new version is wider and allows wheelchair passengers to use the booth as well. The enrolment centre is also located in terminal 2F and is equipped with two enrolment stations. The enrolment centre is open 5 days a week from 8:00 to 20:00 hrs and daily enrolls 64 to 76 participants of the PEGASE programme. For the position of the enrolment centre and the automated booths within the terminal 2F see Figure 10.

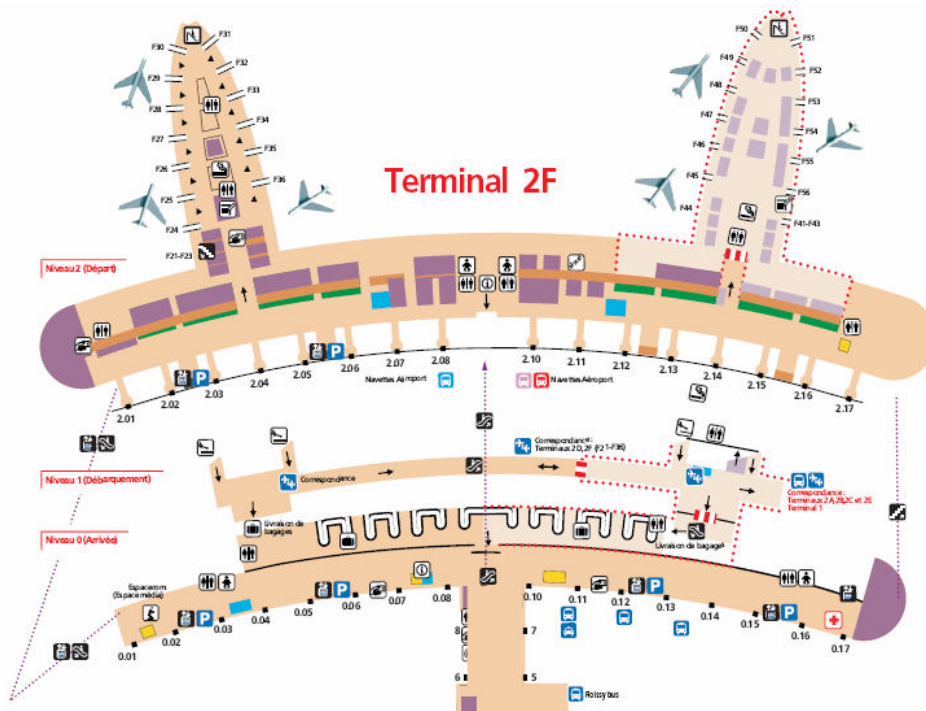


Figure 10: Terminal 2F of the Paris Charles de Gaulle airport: The enrolment centre is marked with a cross, the automated border control booths are marked by a circle.

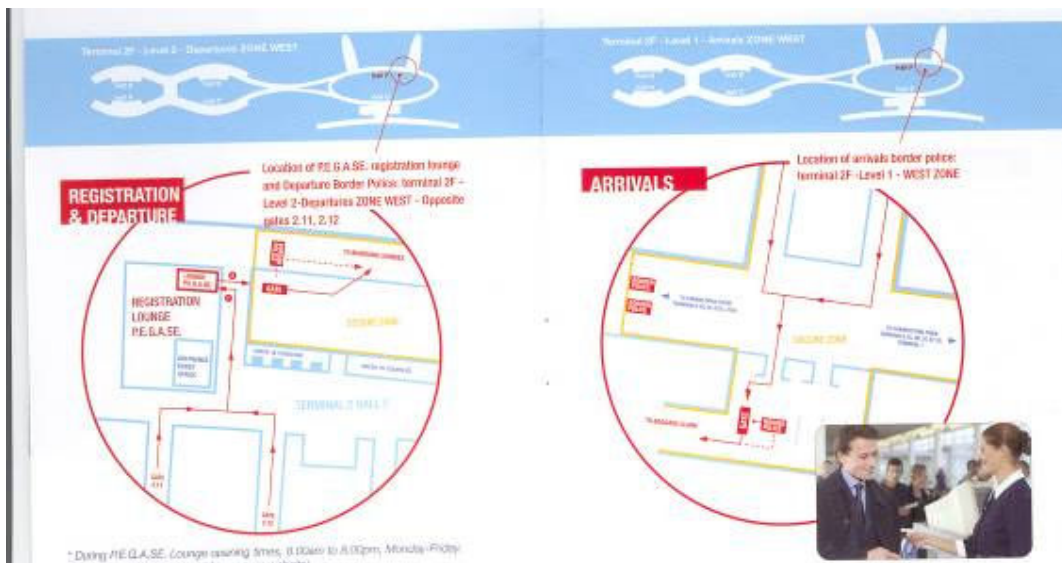


Figure 11: The detailed position of the PEGASE enrolment centre and the automated booth.

3.3.2 Project

Attempts to introduce an automated border control system at the Paris Charles de Gaulle airport have a long history. Unfortunately, the first projects were cancelled, one of them because of the collapse of the airport's terminal 2E.



The PEGASE project was awarded to the company SAGEM défense sécurité (now part of the SAFRAN Group) after the tender in August 2004. The system was opened to the public in June 2005 as a trial for one year (and has been in the experimental stage already since March 2005). The initial maximum number of participants was set to 5 000 volunteers. Later the trial has been extended until the end of May 2007 and the maximum of 10 000 participants. This maximum of participants was reached in the middle of January 2007 and after reaching the maximum the enrolment was stopped. The system stopped on the 27th of May 2007.



Picture 9: The PEGASE booth at the departure level.

There are two automated biometric border crossing booths installed, one for departures and one for arrivals. On average 100 to 150 people use the booths per day.

3.3.3 Passengers

The registration in the PEGASE system is open for any citizen of the EU and Switzerland. The system is primarily designed for Air France customers as the terminal 2F is mostly used by Air France and its Sky Team partners. The PEGASE system is however open for anybody (fulfilling the legal conditions) and is not bound or restricted to frequent flyers of particular airlines. The only purpose of the PEGASE system is the automated border control, no other privileges (like dedicated security checks) are linked to PEGASE users.



3.3.4 Biometrics

3.3.4.1 Technology

The PEGASE system is based on fingerprints. At enrolment, prints of two fingers are taken. The templates are stored in a local database of the French Border Police at the Charles de Gaulle airport and at the time of automated border control the 1:1 verification is performed. The whole system is using the SAGEM technology. The enrolment computers and the departure booth are using the SAGEM MSO 301 fingerprint scanners. These are USB fingerprint readers equipped with the live finger detection feature (i.e. liveness detection). Before this reader type was available the only SAGEM device equipped with the live finger detection was the Morphoaccess device, which can possibly be used in stand alone position. This fingerprint capture device is still used as the training device at the enrolment centre and in the automated booth on arrivals. The biometric matching software is SAGEM fingerprint matching working in 1:1 verification mode.

3.3.4.2 Error rates

The inherent problems of biometric systems are the false rejection (when authentic users are rejected) and false acceptance rates (when impostors are accepted). In the PEGASE system, the biometric false rejection rate is 1.6 % on average. There are differences on departures and arrivals (fingers can be too dry just after leaving the aircraft) and in the summer and winter time. The false rejection error rate of 1.6 % already includes false rejects caused by the liveness test (when the fingers are, for example, too dry or wet the liveness test can incorrectly conclude the finger might be a fake).

The operational usual Fail to Enrol (FTE) rate of the biometric system is 1:1000 for a complete population including manual workers and other difficult-to-enrol people. In practice there hasn't been any case of a traveller failing to be enrolled biometrically.

Because the border booth is automated, a unicity test is required. The unicity test verifies whether only a single person is present inside the border control booth during the border crossing (it is also able to check if there are any items left in the booth). The unicity detection is not at all a simple task and has to cope with various kinds of clothing (e.g. winter coats) and hand baggage of different size and shape. The unicity detection also has its error rates. The older version of the unicity test was falsely rejecting about 6 % of passengers (that includes also winter times when the false rejects are more common due to difficulties when coping with winter clothing). The new and improved version of the unicity detection is falsely rejecting about 3 % of passengers (but this number can increase slightly as the winter time results are still not available).

3.3.5 Procedures

3.3.5.1 Enrolment

During the enrolment biometric and passport data are captured, stored in a database and a card is issued to the registering passengers. During biometric data acquisition two fingerprints are scanned. Preferably the two index fingers are enrolled. If enrolment of index finger(s) is not possible, two other usable fingers are used. Biometric data are used to derive the fingerprint templates (minutiae) and then the complete database of



the PEGASE registered passenger is searched through to locate potential dual identities of the same person.

FRONTEX
LIBERTAS. SECURITAS. IUSTITIA.

Before a passenger can participate in the PEGASE system a light background check is performed. This check makes a lookup in the French database of *searched persons*, which includes SIS, the list of people who are not allowed to leave the country, people who have not paid fines etc. The same check is done twice a day against the list of enrolled PEGASE participants. Cards of people who match one of these lists are deactivated, which implies that the automated door at the border check does not open for these cards. Naturally, the passports are carefully examined during the enrolment, basically in the same way as during classical border checks.



Picture 10: The PEGASE enrolment.

The data from the MRZ (Machine Readable Zone) of the passport together with the biometric data are stored in the database of the French Border Police at the CDG airport. Biometric data are two fingerprints in the form of minutiae stored in the SAGEM proprietary format. Data processing complies with the national and European legislation and the passenger wishing to participate in the PEGASE programme has to sign a registration form (see **Error! Reference source not found.**). The database containing biometric and passport data will be destroyed at the end of the PEGASE trial period.

At the end, the passengers receive a PEGASE card, which is a contactless smartcard. The smartcard is a standard MiFare card and only stores the card number. When the passenger receives the card, the enrolment is over and the card is immediately active and can be used for automated border crossing. The enrolment centre is equipped with a



sample border crossing system and all passengers are given brief training on how to use the system.

The overall process of the passenger enrolment takes 4 minutes and 35 seconds on average. This total average time includes 2 minutes and 49 seconds to fill the form, verify the passport and screen the police file. The biometric enrolment needs 42 seconds on average. To print the card and deliver it to the passenger 37 seconds are needed. At the end the basic passenger training can be done in 26 seconds.



Picture 11: The passenger training at the end of the enrolment.

In the case of difficulties with the biometric enrolment, there is no upper limit of enrolment attempts. Generally, passengers can try as many times as they want until successfully enrolled. Until now (March 2007) there has never been a case when a passenger could not be enrolled in the PEGASE programme because of any problems with the biometric enrolment.



PEGASE PROGRAM

Form to be given each candidate
before his/her signing in the PEGASE PROGRAM

I the undersigned,, am aware that the Police aux Frontières (French Immigration Police Authorities), at the Airport Roissy-Charles de Gaulle in Terminal 2F, have at their disposal data processing facilities, so as to facilitate the checking of frequent flyers' identities, this by using biometrical databases, for example minutiae of finger prints, as well as data relative to the travelers' identities as they are stated in their traveling documents.

In accordance with the provisions of the modified French law No. 78-17 of January 6, 1978, relative to data processing, computer files and liberties, the processing of these data has been notified to the National Commission on data processing and liberties. The registered pieces of information are to be used only by the Police aux Frontières in Roissy and can only be communicated to third parties entitled to, in appliance to legal provisions.

I am aware that, according to the articles 39 and following of the above mentioned law, I am guaranteed the right to access and rectify my private data, thus entitling me to communication, and if need be, rectification or deletion of the said data, either by a direct request to the Police aux Frontières in Terminal 2F or by writing to the Police Immigration Authorities at the following address:

Monsieur le Chef de Quart de la Police aux Frontières
Aérogare 2F
6; rue des Bruyères
BP 20 106
95711 ROISSY-CHARLES DE GAULLE

I am aware that my private data will be deleted at the end of the PEGASE program, at the latest one year after my signing in.

After reading the information in the present document, I agree to the registration and processing of my private data (surname, first name, date and place of birth, nationality, address, minutiae of both my index fingers, number, validity date and type of my traveling document) thanks to the central data base of the Police aux Frontières, in the framework and for the needs of the PEGASE experiment.

Read and approved,

On/...../ 200_

Signature:

Figure 12: Statement of consent

3.3.5.2 Verification

The aim of the automated biometric border crossing is to verify identity of the passenger and if everything is all right let him or her cross the border in an automated way. In the PEGASE system, the passenger first presents his or her smartcard (containing only the card number) to the contactless reader in front of the booth. If the booth is available (open and unoccupied) and the passenger's card is active the door opens.



The passenger's personal and biometric data are located in the database (the card number gives the key) and the passenger's identity must be biometrically verified. The passenger's current biometric data are captured and verified against the two stored templates. If the match is not close enough, the passenger can re-try the biometric data capture, altogether 3 attempts within 30 seconds are allowed. If both the biometric verification and the unicity detection succeed the door opens and the passenger can proceed. If this is not the case (i.e. either the biometric verification fails or the unicity test detects more than a single person inside of the booth or the passenger presses the emergency button) the side door opens and the passenger proceeds to the immigration office for the classical border check.

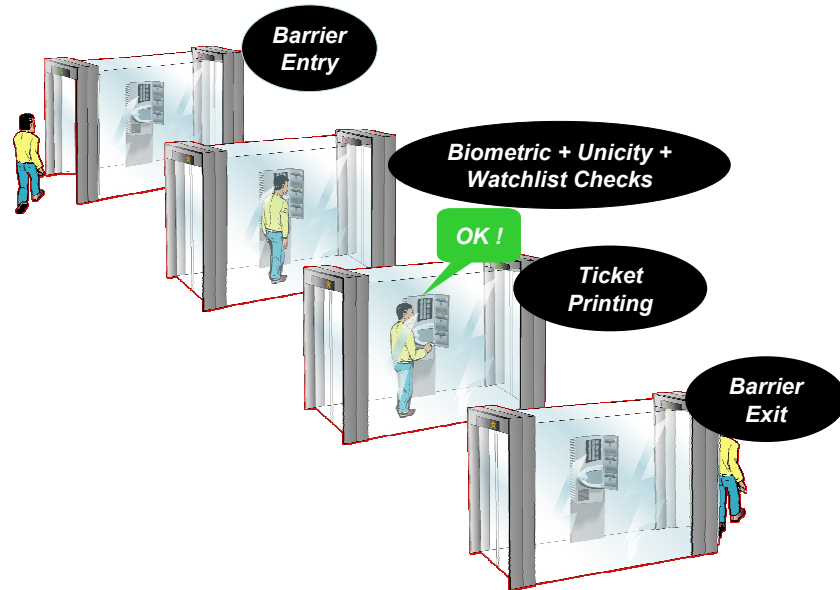


Picture 12: The user interface of the biometric verification – the new version.

The average duration of the automated border check is 12.5 seconds. The minimum time required for an experienced passenger is 6 seconds and the maximum time allowed for the border check is 30 seconds. If the biometric verification does not succeed within 30 s the side door opens and the passenger must proceed to the classical border check. The booth is then available for the next passenger. The duration of the automated procedure is more or less the same as for non-problematic classical check. The advantage of the automated border crossing is a shorter queue and a guarantee that if a problem arises the passenger proceeds to classical check and does not block the



automated booth. At peak times the automated border crossing booths offer real benefits to the registered passengers as they save minutes or even tens of minutes of the queue for the classical border check.



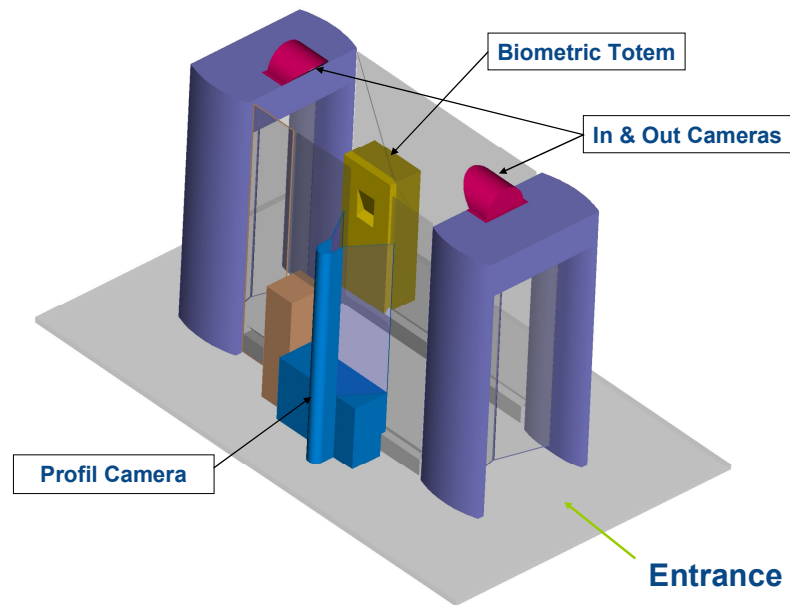
Picture 20: Illustration of the non-problematic automated border check.

Even when using the automated border check the passenger is obliged to carry a valid passport (if having multiple passports any valid passport is acceptable – not just the one used at the time of registration), but this is not automatically verified.



Picture 13: Interface of the older version of the PEGASE booth.

The design of the automated booths follows the classical man-trap approach. The entry door opens only when a valid card is presented, the exit door opens only after successful biometric verification and when unicity detection indicates a single person inside. The side door opens in the case of problems and leads to manual border check. If a searched person is caught in the man-trap the door does not open and a policeman has to open it manually by pressing a button. If a person is on the list of people not allowed to leave the country, he or she is not allowed to embark. If an unpaid fine is found, the fine has to be paid first. The list of PEGASE passengers is regularly checked twice a day against police databases, and no further real-time checks are done at the time of the border crossing.



Picture 14: Model of the automated border crossing booth.

The automated border crossing system logs the following information: booth identification, card number, date and time, result of the crossing attempt (biometric score and yes/no result, result of the unicity test). No biometric data are stored.

3.3.5.3 Provider

The PEGASE system (hardware and software, not the data) is owned by SAGEM. SAGEM rents the system to AIR FRANCE, the contract covers maintenance of the hardware and software and finishes in May 2007. SAGEM was chosen by Air France in a tender in the summer of 2004 when the SAGEM offer outperformed two other competitors. The tender call specified many technical requirements like the detailed design of the system, unicity detection, fingerprint biometric system, liveness test etc. This document remains confidential. Even through the costs of the automated border crossing is covered by the Air France, the system is in fact operated by the French border police.

The passengers' database containing passport and biometric data of enrolled people is maintained by the French border police, SAGEM only receives some statistical data. In the future it appears that the French automated border crossing system will be shared between the border police (core system) and the different French airports (mantraps). Anyhow, the system will be operated by the border police.

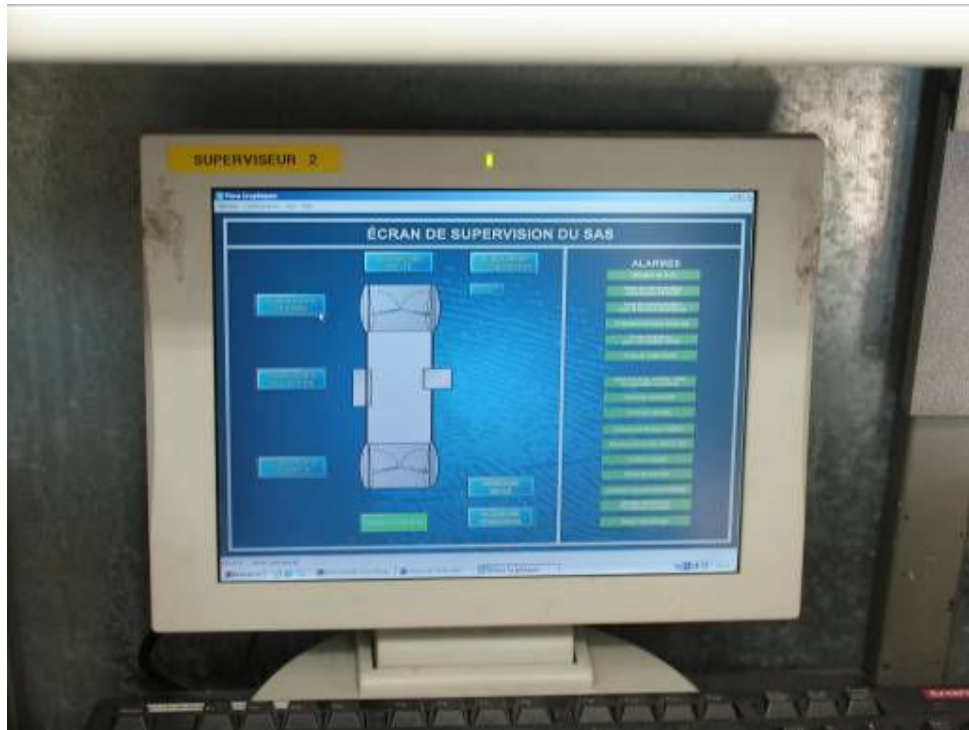
3.3.5.4 Operators

The automated booths are controlled and supervised by nearby border police officers. Next to each automated booth a classical border crossing booth with a border officer is present. This officer is responsible for opening (activating) the booth and supervising it. This border officer also checks the passengers who for what ever reason fail to be verified automatically.



The control and supervision of the automated booth is performed via a console (computer, see Picture 15), which displays events (like failure of the biometric verification or timeout) and can control the behaviour of the booth (e.g. to force to open the side door). The console is located in the nearby manned booth.

The officers working in the nearby booths who operate the PEGASE border control booths receive special training on how to operate the system. SAGEM trains instructors from the border police and these instructors then train the border officers. There are about 200 border officers trained to operate the automated system. An additional 30 people are trained to operate the enrolment centre.



Picture 15: The PEGASE supervisor console.

As the border officers supervising the automated border system remain to perform standard manual and human-assisted border control; they are not additional staff. The enrolment centre, however, does require additional staff. Currently the enrolment centre is closed. During the first year two enrolment stations were open and later only one enrolment station was active.

The PEGASE system (hardware and software) is maintained by SAGEM as specified by the agreement (between SAGEM and AIR FRANCE). Such maintenance, however, does not include cleaning. This is considered to be a problem that will need to be solved as soon as the PEGASE system starts the non-trial operation.

3.3.6 Difficulties and problems

No single novel and challenging system can avoid coping with some difficulties. While there were no serious problems when implementing or operating the PEGASE system, a lot of minor issues needed to be discussed, improved or redesigned. These issues include:



- Some mechanical problems occurred (e.g. the door opening was not 100% reliable)
- Unicity detection is not a trivial task. The test was improved several times to reduce the false rejection rate without compromising false acceptance.
- Some training issues were also raised. There were discussions about the specifications with the users of the system (i.e. the border control officers).
- Ergonomic aspects cannot be underestimated. Some of the falsely rejected passengers were rejected only because of the ergonomic issues. The initial version of the automated booth had double displays and included an unused keyboard. The reason for that was simple. At that time the only fingerprint scanning device incorporating the live finger detection (liveness test) was a standalone access control device (SAGEM Morphoaccess) equipped with a display and keyboard. Now a new separate fingerprint reader with liveness test is available (SAGEM MSO 301) and therefore the new version of the booth equipped with the new fingerprint reader improved significantly its ergonomics.

3.3.7 Security

As the automated booths replace the human border check the security of the automated process plays a crucial role. Critical security issues include the network and database security, biometric liveness test, unicity test and human supervision.

Fingerprint scanning devices used in the automated booths incorporate live finger detection (liveness test). This test was designed and tested in SAGEM laboratories. In addition, it was extensively tested by the UK, Hong Kong and French (immigration or civil aviation) authorities.

The unicity test was designed and tested in SAGEM laboratories. Within the next 6 months it is going to be extensively tested by the French Ministry of Interior.

Access to the database is provided via a dedicated and secured network.

Regarding the booth supervision there are three cameras in the booth (they are used primarily for unicity detection). In addition to that the booths are supervised by the nearby manual check points. The nearby border officers ensure that no damage is done and that everything goes smoothly.

The number of falsely rejected passengers is public knowledge (1.6 % due to biometrics and 3-6 % due to unicity test); the number of stopped offenders is not public. Until now there have been no identified hacking attempts or attacks. The only interesting event happened on the inauguration day when a camera flash (from a journalist taking pictures) confused the image processing and the side door to the manual border control was opened (which is not a security problem).

3.3.8 Costs

No information about the costs of the development, hardware, software or maintenance is publicly available. Registration in the PEGASE system and the use of the automated border booths is for free. The costs are covered by Air France at the moment.



3.4 Biometric systems at UK Airports

London Heathrow Airport

London Heathrow Airport is one of the busiest airports in the world and Europe's largest airport. Heathrow has four passenger terminals (Terminals 1, 2, 3 and 4) and a cargo terminal. The fifth passenger terminal, Terminal 5 is expected to open in March 2008, with construction of all satellite buildings completed in 2011. The airport is owned and operated by BAA⁵ -British Airports Authority. Heathrow is the world's third-busiest airport by total passenger traffic, after Atlanta-Hartsfield-Jackson and Chicago-O'Hare in the United States. Heathrow was opened in 1946 (Terminal 1 - 1969, Terminal 2 - 1955, Terminal 3 - 1961, Terminal 4 -1986). The airport employs 68,000 (4,500 are BAA Heathrow employees).

Gatwick Airport

Gatwick is the single-runway airport, the second largest airport in the UK and the sixth busiest international airport in the world. The airport offers flights to over 200 destinations by some 80 airlines. The airport is owned by BAA, it has two terminals, around 90 airlines, flying to 212 destinations, 32 million passengers per year and 25,000 employees (2,000 are BAA Gatwick employees).

Manchester Airport

Manchester airport is part of four airports owned by Manchester Airport Group⁶ (MAG). The airport offers 180 destinations worldwide by some 95 airlines, almost 28 million passengers every year; it has two parallel runways, three terminals and around 19,000 people employed on the site.

Birmingham International airport

Birmingham International is the UK's fifth largest Airport. In 2006, it handled over nine million passengers through its two terminals. The airport offers flights to over 100 destinations by some 50 airlines. The airport employs around 10,990 people.

Border control at the airports

Border control at UK Airports is carried out by immigration officers, who are part of the newly formed Borders & Immigration Agency (formerly the Immigration & Nationality Department). Border control is carried out only for arrivals. After the

⁵ BAA, the world's leading airport company, who also owns - Heathrow, Gatwick, Stansted, Southampton, Glasgow, Aberdeen, and Edinburgh.

⁶ MAG is the largest British-owned airport operator. Our four airports - Manchester, East Midlands, Bournemouth and Humberside – currently handling a total of almost 28 million passengers every year.



terrorists attack⁷ (2005), a targeted control for departures was introduced (“temporary embarkation control” for the people going out of the country). This control is manned randomly or based on intelligence.

3.4.1 The IRIS system

IRIS stands for “Iris Recognition Immigration System” and it means that the eligible person who pre-registers his or her iris patterns is able to use automated barriers to pass through the immigration control on arrival in the United Kingdom. The main purpose of the IRIS system is to provide fast and secure clearance through the UK immigration control for registered frequent travellers. It is a biometric system that does not use a smartcard or token; the system is based on a “one to many” check against the whole database.

IRIS is an operational system. It was introduced in June 2005 for 2 weeks, but the enrolment rooms were closed following terrorist attacks in London on 7th July 2005, when enrolment staff were redeployed to front line work. IRIS is part of the e-Borders program⁸ - a long-term business change programme until 2012 that aims to modernize the border services. With the help of new technology, the e-Borders programme is focusing on the key challenges in the border domain:

- Migration pressure
- Increased security threat
- Predicted increase in travellers to the UK
- The need to facilitate the arrival of low risk passengers
- The need of closer integration of border agencies

The second project of the e-Borders programme is SEMAPHORE that commenced in 2004 and provides the operational prototype to trial the e-Borders concepts and technology. In the SEMAPHORE project, arriving passenger lists are checked against a variety of watchlists. The Joint Border Operational Centre (JBOC) manages SEMAPHORE; JBOC consists of multi-agency operation staff (officers from HMRC, Immigration, Police and UK visas). Since December 2006, the IRIS biodata database is connected to SEMAPHORE.

⁷ The [7 July 2005 London bombings](#) were a series of coordinated terrorist bomb blasts that hit [London's public transport system](#) during the morning [rush hour](#). At 8:50 a.m., three [bombs](#) exploded within fifty seconds of each other on three [London Underground](#) trains. A fourth bomb exploded on a [bus](#) nearly an hour later at 9:47 a.m. in [Tavistock Square](#). The bombings killed 52 commuters and the four suicide bombers, [injured 700](#), and caused a severe day-long disruption of the city's transport and mobile [telecommunications](#) infrastructure.

⁸ The aim of e-Borders Programme is to establish a modernised, intelligence-led border control and security framework, based on the electronic processing of information relating to travellers to and from the UK for all modes of transport.



3.4.1.1 Enrolment

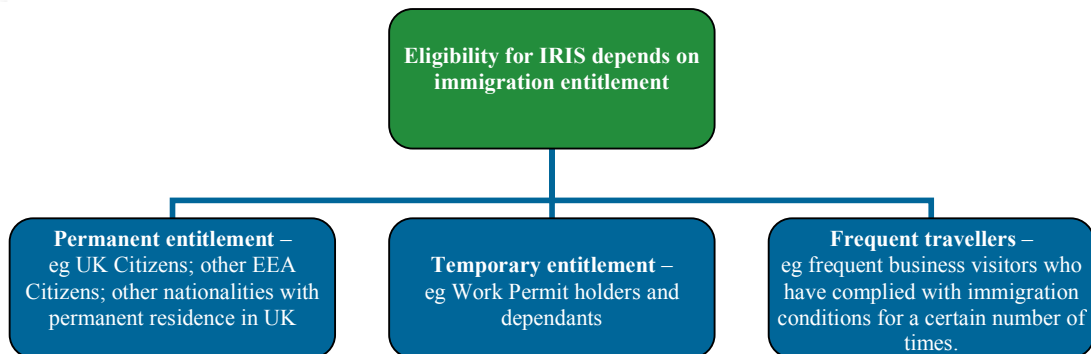


Figure 16: IRIS types of entitlement

Detailed information on who can apply for use of IRIS system:

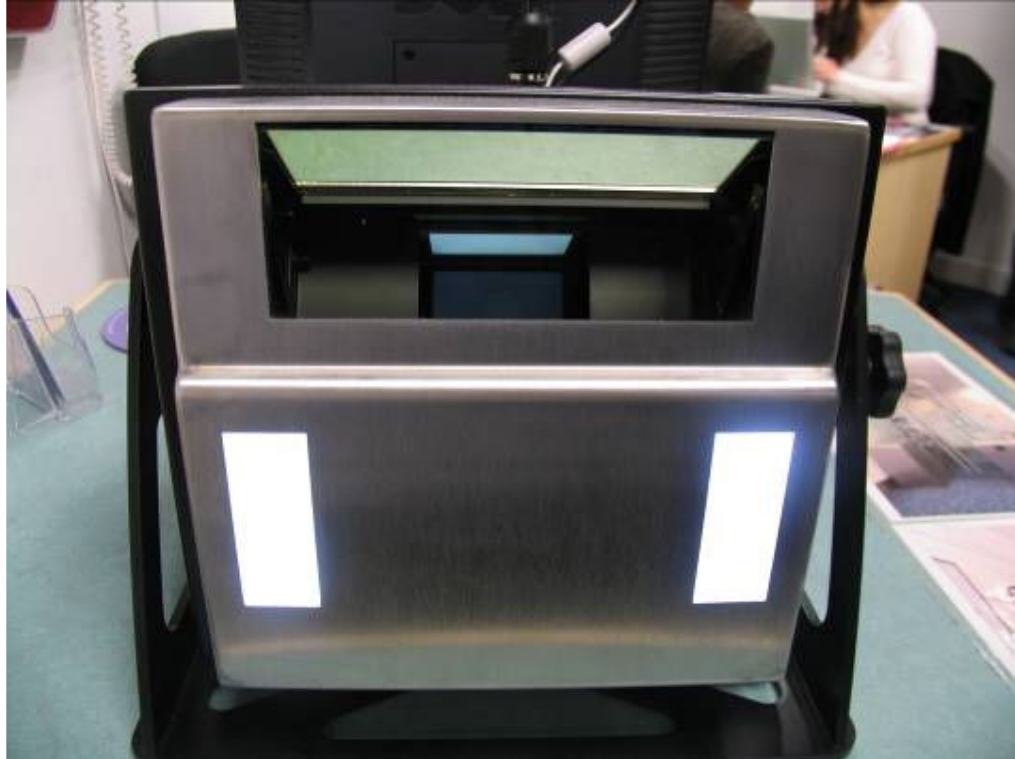
- a permanent resident of the UK,
- permitted to enter or remain in the UK for more than six months and having more than two months left of your leave to enter or remain,
- holding a current entry clearance that is effective as leave to enter the UK and the validity of the entry clearance has more than two months left,
- a short-term visitor to the UK and who can demonstrate that he/she has been granted leave to enter the UK as - a visitor on at least two occasions in the last six months, or four occasions in the last 12 months,
- exempt from immigration control and based in the UK, (including, for example, members of diplomatic missions in the United Kingdom and their qualifying family members, consular officers and employees and their qualifying family members and members of Commonwealth and NATO armed forces posted for service to the United Kingdom, or undergoing training),
- a family member of an EEA State national or of a Swiss national based in the UK,
- a British citizen or someone with the right of abode in the UK, or a national of an EEA State, or a Swiss national.



Picture 17: IRIS enrolment at Heathrow.

3.4.1.2 Post-processing

All IRIS enrolment rooms are located in the airside Departure Lounges of participating airports. This means that only those travelling out of the UK with a passport and boarding pass are able to enrol. The complete enrolment process takes less than 5 minutes. In the enrolment room (enrolment stations), there is an immigration officer, also known as "enrolment officer" who carries out the assessment of applications to participate in the IRIS system (immigration database check, passport examination, checks that the person is the actual holder of the passport, and some forgery test if necessary). The officer is responsible for examining the travel documents and may question the enrollee about the immigration status in the UK. If the person is qualified to enrol, then the enrolment procedure starts. The immigration officer swipes the passport MRZ data into the system and, either the validity date is set automatically for some categories, or the officer enters it manually for temporary entitlements. The camera operator then takes the person's portrait photograph of the face and iris pattern of each eye is captured using a camera. The iris pattern photographs are taken using standard video camera technology (there are no bright lights and no lasers involved). The experience is similar to having a photograph taken and the process takes a few seconds to complete in the majority of cases. The iris pattern images are then converted into iris codes by proprietary biometric algorithms supplied by Iridian.



Picture 18: IRIS camera.

Before enrolling, the biometric data is sent to the central database to check if the person is already enrolled in the system. The system is built as a network system - at the headquarters, there is a central database and on each location, there is a local server. Until the enrolment is complete, the data will stay in the local server. After completion the data is sent to the central database and in 5-10 minutes is sent to all other databases. Therefore, in each base (local server) there is a copy of central record (not the images – just the template) for recognition and for recording the arrival. The iris image is stored in encrypted form in a secure archive database, to which access is strictly controlled.

Additional information, such as a person's name, date of birth, nationality, gender, passport details and details of his or her immigration status in the United Kingdom are also recorded as part of the enrolment application process and entered into a secure database. An enrolment officer then explains the arrival procedure and the enroller can practise using the iris recognition camera. The person then receives printout information of captured data and a leaflet (guide) that will tell him - what to do on arrival back in the UK.

When people with a permanent UK immigration entitlement are enrolled, the time limit of validity is two years. Each time the person goes through the checkpoint (barrier), the validity is extended for another two years.

If the person does not qualify for IRIS, the immigration officer will give them a notification letter, which will explain the reasons of refusal (refusal for IRIS does not mean refusal for entry to UK).



Biometrics and System performances

IRIS system is based on iris image. Reader manufacturer types are the Panasonic with Sagem modifications. Iridian and Sagem provide the biometric matching /verification software.

The average time for enrolment is 4 minutes. Failure to enrol (FTE) is 1.47%, which is inside the requirement of 2%. 79% of the barrier crossings were completed in less than 15 seconds. There were no instances of false acceptance recorded (FAR). Barrier rejection rate was below 2%.

3.4.1.3 Data use

All personal data, including the record of iris patterns, provided by a person during the enrolment application process and held on the IRIS system are destroyed after a certain period, if the person is no longer actively participating in the scheme.

The iris images are stored in an encrypted form in a dedicated, separate, secure database, to which access is strictly controlled and may be used for a possible quality check. For biometric recognition, the Iriscode template is used.

Other information captured and held in connection with the system, including data collected at the enrolment application stage (regardless of whether the application is successful) and during use of the automated barriers, are processed by the Immigration Service for the purpose of the operation of the system including protecting it against fraud and security maintenance. The data can be used also for management information and statistical purposes.

Information, other than the iris images and iris codes, may also be disclosed, where appropriate, to other government departments, agencies, local authorities and other bodies where necessary for the purposes of the IRIS system and other immigration purposes.

Every night there is a “bulk” check of the IRIS database against a Border watchlist, and there are constant checks against other watchlists within Semaphore. This enables the IRIS record to be ‘de-activated’ so that the person would be unable to use the automated barrier. There is also a ‘Watch’ facility that checks the Arrivals data.

In some circumstances the use of the iris recognition automated barriers may be terminated at any time and without prior notice (and either temporarily or permanently). These rules apply to all users, or certain categories of users, or a specific individual or individuals. These circumstances are:

- As a result of any malfunction in the operation of the automated barrier(s);
- For national security reasons;
- As a result of changes to the United Kingdom's Immigration Rules (such as the introduction of a visa requirement in respect of a particular nationality);
- Where an individual no longer qualifies, or there is reason to doubt that they will continue to qualify, to use the barriers on the basis for which they have been enrolled;



- Where an enrolled person's leave to enter or remain in the United Kingdom is curtailed or cancelled;
- Where an enrolled person does not use the automated barriers for more than two years;
- Where an enrolled person notifies the Secretary of State that they no longer wish to participate in the project.

If the system recognizes the person, but membership is no longer valid, the person will receive the ticket “sorry your enrolment is no longer valid, please go to the main control”. The person can either take the ticket or he can walk out and the ticket will be taken back in to the machine.

Another ticket, the “leave to enter” ticket must be taken before the landside door will open and allow the person to enter the UK. Third country non-visa nationals who do not already have an existing UK immigration entitlement receive printed tickets instead of passport stamps.

Where a person's permission to participate in the project has been terminated or is no longer valid, they are unable to use the automated barrier on arrival in the United Kingdom. They must proceed to the immigration control to be seen by an immigration officer in the usual way.

For a high level of physical security of the hardware (HW) and network, penetration tests were done. For overall security, hired consultants performed various tests.

3.4.1.4 Procedures on arrival

When a person enrolled in IRIS arrives back in the UK, he or she can clear immigration using the IRIS system. The person follows the airport sign for arrival and baggage reclaim and looks for the IRIS barrier. Before entering the cabin (barrier), the sensor will detect the person and the first gate will open. As the person enters their height is assessed and one of the three IRIS cameras on different levels will be activated. The light beside the activated camera will go on and the person must look in to the digital mirror inside the camera. There is a voice guide (please look in to the mirror, please move back a little, thank you....) guides the person to align their eyes (iris) with the sensors and the IRIS camera photographs the iris patterns of the person. If the system recognizes the iris pattern and the record is still valid, the barrier will open automatically and the person is able to enter the UK (the system can be used with glasses). If the person is unsuccessful for three (3) times, then the first door opens again and the person must exit back. The person can enter several times. The design of the barrier (verification point) is not manufactured as a Man-trap – the person can always go back.

In case the person forgets pieces of luggage inside the cabin and leaves it, the exit door remains open for a certain time so that the passenger can still go back and collect the luggage. If the luggage is not collected within this time limit, an alarm will be set off.

Booths are part of the immigration arrivals control and a risk assessment has been carried out of the need to supervise/monitor them with CCTV cameras, depending on their location on the control. For overall supervision of the immigration control, there is



a podium (watch house) with one IRIS monitor, but the supervising officers in the watch house have other duties as well.

3.4.1.5 Other errors and related problems

No major technical problems have been identified except for the minor ones (many of which have now been solved) pertaining to:

- the uniqueness detection,
- the UPS – spikes in electricity,
- biometric matcher on server which leaked memory (and needed to be restarted from time to time),
- height detection (important for the choice of the camera – one of three cameras inside the barrier),
- synchronization problems of the central database,
- integration problems at different airports,
- illumination problems at Stansted airport (therefore the IRIS system is not implemented at the moment),
- working in difficult environments (space issue),
- the bureaucracy (fortunately the law had been already modified before the IRIS project started).

Informal market research at Heathrow (email) has shown that the position of the cameras in barriers is seen as problematic.

List of enrolment stations:

The enrolment stations are situated in the airports departure lounge, after passing through security. To apply to join IRIS, the candidate must visit one of the enrolment rooms in person. There is no application form to fill in.

Heathrow

Terminal 1	The enrolment room is on right hand side before reaching the shops. This enrolment room is open between 06:30 and 18:30.
Terminal 2	The enrolment room is near gate 1. This enrolment room is open between 07:00 and 21:00.
Terminal 3	The enrolment room is before reaching the Duty Free shopping area opposite the BAA Security desk. This enrolment room is open between 08:00 and 18:30.
Terminal 4	The enrolment room is between gates 3 and 4. This enrolment room is open between 07:30 and 19:30.

Table 4: Heathrow terminals

Gatwick

North Terminal	The enrolment room is in the departure lounge and is located at the bottom of the spiral ramp near gates 59-63. The enrolment room is open between 07:30 and 13:30.
-----------------------	---



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA

South Terminal	The enrolment room is in the departure lounge and is located at Gate 90. This enrolment room is open between 07:30 and 13:30.
-----------------------	---

Table 5: Gatwick terminals

Manchester

Terminal 1	The enrolment room is near gate 20. This enrolment room is open between 06:00 and 14:00
Terminal 2	The enrolment room is on the right in the shopping area. This enrolment room is open between 06:00 and 14:00

Table 6: Manchester terminals

Birmingham Terminal 1

The enrolment room is located on the left of the departure ramp before gate 56. The enrolment room is open between 08:00 and 20:00.

3.4.1.6 Training of staff

Each immigration officer working on IRIS enrolment receives 1 day IRIS training and 2 days extra forgery training. Each camera operator receives 1 day IRIS training. Every chief immigration officer receives half a day Podium Manager training (overview of the system and what to look for on the Podium Manager screen). Local Cascade Trainers at each Port deliver the training. The IRIS Project trainers give 3 days training on the IRIS training packages to each Cascade Trainer and they then sit in on the first few training sessions to give assistance if required. Based on experience from the two pilot airports, laptops were used to train the staff at places where the system was not yet operational.

Number of IRIS Cascade trainers	20
Number of Immigration Officers	235
Number of Camera Operators	93
Number of Chief Immigration Officers (basic + barrier faults)	94

Table 7: Trained staff statistics

3.4.1.7 Price of the system

The contract cost for IRIS system is 2.8 million pounds (ca. 4.2 Million Euro). Of this, 1.6 million pounds (ca. 2.4 Million Euro) covers development, hardware and software plus installation at 10 sites, iris license fee, and initial training by supplier. The remaining 1.2 million pounds (ca. 1.8 Million Euro) is for maintenance and support over 5 years.

3.4.1.8 Maintenance of the system

The contract is in place for 5 years with SAGEM (prime contractor), who have subcontracted the service & maintenance to SERVICETEC. 1.2 million pounds (ca. 1.8 Million Euro) for support and maintenance for 5 years (includes training for the 2 pilot ports (Heathrow Terminals 2 and 4 but does not include human operators).



3.4.2 miSense and miSense^{PLUS}

miSense and miSense^{plus} were trials carried out in Heathrow Airport to test the Ideal Process Flow – which was developed by IATA's⁹ (International Air Transport Association) Simplifying Passenger Travel Programme¹⁰. SPT aims to test a series of new technologies and processes designed to help make air travel easier, quicker and more secure. SPT covers over 70 airports, airlines, government authorities, travel agents and technology suppliers working together to implement new systems that are complementary and provide for international interoperability.

The original idea of the miSense^{plus} project was to use interoperable systems for automatic border control between three airports using an eToken: Dubai, Hong Kong, and London Heathrow. During the negotiations, Dubai airport withdrew from the trial and time delays led to interoperability problems between Heathrow and Hong Kong, although fast paths through immigration were put in place to expedite arrivals in Hong Kong for trial members. The miSense trial was limited to passengers travelling with Cathay Pacific to Hong Kong and with Emirates to Dubai. The miSense^{plus} system was limited to UK and EEA passengers flying from London Heathrow Terminal 3.

3.4.2.1 miSense

The miSense element of the trials was a system that used biometric recognition technology to simplify the journey from check-in to the plane while maintaining high levels of security. miSense was a single journey use of a “disposable” biometric captured at check-in and used as an identifier at ticket presentation (security) and on boarding the plane. The trial began on 19th October 2006 in London Heathrow Terminal 3 and lasted for 4 months.

Enrolment

The enrolment is limited to passengers flying with Cathay Pacific to Hong Kong and Emirates travelling to Dubai. A dedicated miSense CUSS (Customer User Self Service) kiosk was positioned in the check-in zone in London Heathrow Terminal 3 of each airline.

Check-in

At the miSense kiosks (Cathay Pacific and Emirates) instructions appeared on an active screen. The passenger was asked to scan their passport photo page and an image of a fingerprint was recorded on a single digit reader (Sagem MSO 301). The fingerprint taken is normally of the right index finger but any digit worked just as well. This information is stored on a dedicated miSense server by the United Kingdom Immigration Service in accordance with the UK Data Protection Act 1998. Biometric authentication is used to identify passengers on entering the passenger restricted area (PRA) and on boarding for selected flights from Heathrow Terminal 3.

⁹ IATA - The International Air Transport Association - was founded in Havana, Cuba, in April 1945. It has over 270 Members from more than 140 nations in every part of the globe.

¹⁰ The Simplifying Passenger Travel (SPT) Programme is an initiative that focuses on the passenger and facilitating their journey while emphasising the security benefits of processing 'known' passengers automatically, thereby freeing-up resources to concentrate on 'unknown' passengers.



Biometrics

The miSense system used fingerprint modality for clearing the gates. Sagem provides biometric matching /verification software.

Security control

Before the entrance to security and PRA in Terminal 3, an automatic security gate was installed (QBG – quick boarding gate). The passenger scanned their chosen finger on the Sagem rapid ID scanner and inserted their boarding pass to gain access. The details are checked against the record made at check-in. If the boarding pass was valid for the flight on that day and if the fingerprint matched, then the gate opened and the passenger was allowed to proceed to the PRA.

Aircraft boarding

The final verification check was carried out at the boarding gate for specific flights to Hong Kong and Dubai. miSense passengers were called to board in advance of normal travellers. They were asked by airline staff (Cathay Pacific and Emirates) to scan their chosen fingerprint on a hand held wireless device (Sagem rapID scanner) and the details were again checked against the database. This portable device was used as the gate the aircraft arrive at cannot be easily determined. Under legal requirements, passengers are still obliged to show their boarding pass and passport. For the trial group, the advantage was gaining experience with different biometric technologies at every stage of the end-to-end journey.

Data issues

Participants in the miSense trial agreed to submit passport details and an image of a fingerprint. The United Kingdom Immigration Service, in accordance with the UK Data Protection Act 1998, stored this information. After the completion of the trial, all personal information was deleted in accordance with the Act. miSense personal data is deleted after 24 hours; only personal enrolment data for miSense*plus* is saved and logged (see 3.4.2.2)

By the end of the trial on 28th February 2007 over 2000 passengers had successfully had their disposable biometric captured at the miSense check-in kiosks and made use of the miSense system.

3.4.2.2 miSense PLUS

miSense*plus* was a traveller registration scheme; meaning when the passenger registered in the system, they received a miSense*plus* membership card which can be used for all miSense services listed above and enables use of automated arrivals gates at UK Immigration on arrival from any destination. The system was available in London Heathrow Terminal 3 and the trial began on 15th November 2006 and finished on 28th February 2007.

Procedures – Enrolment - Verification

Enrolment took place in Heathrow Terminal 3 (the enrolment room is located between security and the Duty Free shopping area in the IRIS enrolment room). For miSense*plus*



only UK and EEA¹¹ citizens over 18 years were allowed to enrol. The passenger must hold a valid passport with an MRZ. An Immigration Officer performed an extended forgery check of the document and normal immigration procedures to ensure the passenger was eligible to use an automated immigration control. Then the person was directed to the *miSenseplus* enrolment area, where they were instructed to read and sign a “terms and conditions” form, which gives consent of personal and biometric details to be stored and used for background and watchlist checking.



Picture 19: miSense PLUS enrolment

The photo page of the holder's passport was scanned on to the *miSenseplus* system and their Biometric data was then captured (a facial image using a digital camera JPEG format), ten fingerprints (SAGEM scanner), and a detailed image of both Irises (IRIDIAN). Checks were carried out against the passenger's passport details and their fingerprints to ensure that the identity or the person had not been enrolled before. Additional information of the person was also taken: email, phone number, flight information. A personalised *miSenseplus* membership card (eToken) was then produced (including a three line MRZ) and their biometrics written onto the chip contained

¹¹ European Economic Area national are from: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxemburg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden and the United Kingdom. Switzerland is not a member of the EEA, but its citizens are treated as such for immigration purposes in the UK.



within (in line with ICAO ePassport guidance). At this stage the person was enrolled on to the scheme and received their card, but it was not activated immediately. This was done after background checks were complete (normally 24-36 hours later).

Background checks were initiated in batches on a daily basis (biographic data and fingerprints were checked against criminal and other databases). Enrolment processes took on average 7 minutes to complete though could be as quick as 3 minutes, from passport data capture to printing and testing of the miSenseplus card. A delay in activating the card meant the passenger could not use the automated immigration control until all background checks were complete. Any problems were communicated to the passenger by e-mail. There is no statistical information on how many people failed to enrol (FTE) – but some people did not want to finish the registration because of a delay and they were in a hurry.

Immigration Control

At the automated immigration control barrier the miSenseplus card was scanned and the data on the chip read (along the ICAO guidelines for ePassports). The passenger placed their right or left index finger onto a fingerprint scanner (SAGEM) and this was verified (1:1) against that held on the card. Verification against the miSenseplus system was also carried out to ensure the card was genuine and activated. There is no specific number of authentication attempts a passenger can make but if the person was unsuccessful, the gate would not open and they would have to proceed to manual border control. The gate could only be used once a day by the same passenger to ensure multiple crossings using one card did not take place. The whole procedure at the miSenseplus barrier took approximately 15-20 seconds

Data storage

The miSenseplus membership card was BAC-protected and contains encrypted images of the two index fingers, two iris codes, a JPEG of the face and MRZ. (Template format: Proprietary SAGEM for fingerprints, IRIDIAN for irises, JPEG for face). At the end of the trial, all personal data are destroyed in accordance with the UK Data Protection Act 1998 [DPA98].

By the end of the miSenseplus trial 1007 passengers had been enrolled in the 13 weeks the enrolment system was available.

How and where miSenseplus can be used

With the miSenseplus membership card the person could use all miSense services without having the necessity to register every time if travelling with Cathay Pacific to Honk Kong and Emirates to Dubai. Other difference/advantages to the miSense services are:

- The registered traveller can check-in at a miSense kiosk putting the miSenseplus card on the check-in scanner instead of the passport;
- The registered traveller can also use any boarding pass from any airline to use the QBG and enter the PRA (boarding passes with magnetic strip only);
- The registered traveller has the advantage of using the automated immigration barrier to enter the UK on arrival from any destination.

miSenseplus membership card could also be used to "fast track" through immigration on arrival and departure at Hong Kong International Airport. At the moment this type of



card cannot be used at an automated barrier as under Hong Kong law it is obligatory to stamp the holders passport. When entering the Hong Kong Immigration area, the person must look for the miSense sign positioned above the dedicated Immigration desk and present the membership card to the Immigration Officer.

Security

Fingerprint scanning devices used incorporated live finger detection (liveness test by Sagem). Physical security of the HW and networks access to the database was provided via a dedicated airport LAN. A host/presenter for IRIS gates and the miSense gate was responsible for supervision and monitoring within the Immigration Hall in Terminal 3. For detection and control of the system, employees performed a series of security tests.

Altogether there were seven enabled points/gates in London Heathrow Terminal 3: 2 at Check-in, 2 at entrance to the PRA and portable units at 2 boarding gates, along with 1 gate at border control – miSense*plus* only. All the systems were automated, except the portable units at aircraft boarding which are human assisted (boarding pass and passport still need to be shown).



4 Conclusions

FRONTEX
LIBERTAS. SECURITAS. IUSTITIA

Four case studies are presented in this study. These four systems are the European pioneers in the area of automated border crossing. All four systems are fully working and enable the registered passengers to cross the border in a convenient way.

4.1 Biometrics

One of the presented systems is based on fingerprints, while the remaining three are based on irises. Although biometrics is an important part of the whole concept and many questions were raised before such border crossing systems came to practice, it turns out that biometrics is the least problematic component at the end. With the false rejection rate between one and two percent (while still keeping false acceptance rate sufficiently low) biometric technologies show their maturity and usability. Both iris-based and fingerprint-based systems operate well without significant differences. Surveys in the UK show that iris based systems are no longer seen as dangerous for your eyes and the younger generation even finds them trendy. Fingerprint systems have very low FTE rates and can register virtually every traveller. The security of the biometric systems is considered high. The liveness testing of the biometric scanners was tested by relevant authorities. No details about the liveness tests or their evaluations are, however, publicly available.

4.2 Booths

The border crossing booths can be of various designs and in fact do not necessarily have to be booths at all. What is important that the entry is on one side of the border, exit is on the other side of the border, you cannot leave to the other side of the border without biometric verification/identification and that the booth/lane can only be used by a single person at a time.

At the European airports there are principally two kinds of booths/lanes: with side door and without side door. In the case of booths with side door if the passenger cannot be biometrically verified or if there is any other problem the side door opens and the passenger proceeds to the classical border check. That implies that there must be a classical border booth next to each automated booth (see figure below).

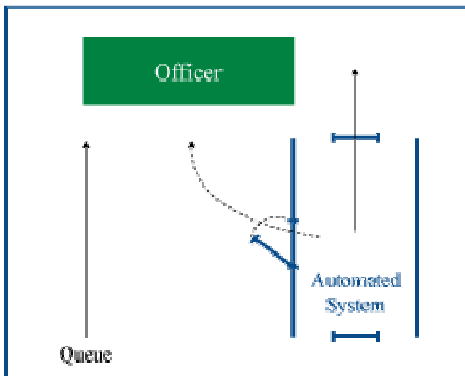


Figure 14: Design with a single automated booth



Another option, the border officer serves two automated lanes like the figure below.

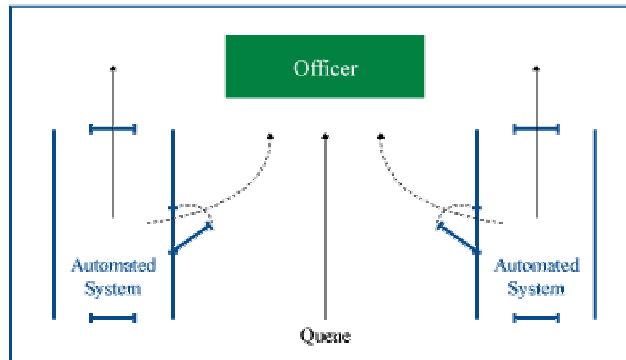


Figure 15: Design with two automated booths

The advantage is that the passenger does not have to wait in the queue and gets directly to the classical border check and that the classical border booths have a good overview/supervision of the automated booths. The disadvantage is the need of one classical booth for each one or two automated booths which limits the boom of the new technology.

The booths without the side door (see Figure 16) cannot direct passengers to the classical border check. Instead the front door opens if something goes wrong and the passenger must go to the classical border check and wait in the queue if necessary. The advantage of such booths is their easy scalability as many of them can be located next to each other.

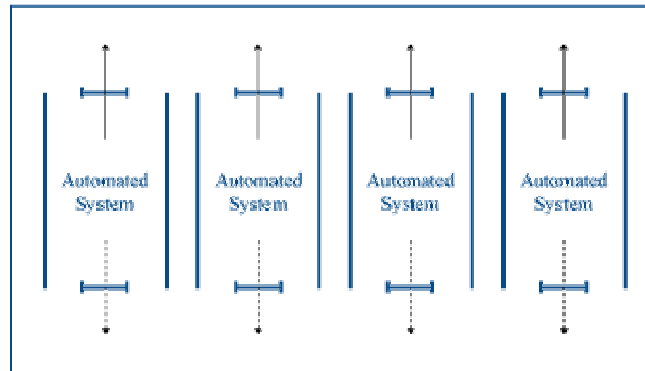


Figure 16: Multiple booths without a side door

4.3 Privacy

Unless based on electronic passports (and none of the four cases is) the registration / enrolment under supervision of a border police officer to a registered traveller system requires an additional storage of personal data including biometric data. The data can either be stored in a central or local database, in a token given to user or in the combination of the two.



In any case the European and national legislation of personal data storage and processing must be taken into account. We cannot address all the details here but would only like to emphasize that generally it is necessary to allow the passengers to review the stored data, rectify the data and delete the data if they decide to opt-out.

The privacy aspects are defined by the voluntary participation of the passengers. Therefore, such systems can be seen in different light than for example the video surveillance, where individuals are verified and possibly identified without their explicit consent.

4.4 Future

Biometrics will likely revolutionise many aspects of border crossing. Automated border crossing has proven a viable concept and it is likely that the use of automation will increase in this area. However, the human border officers are not completely replaceable neither today nor in the near future. No computer systems can currently detect nervousness and suspicion as well as experienced border officers. Therefore the aim of the automated border crossing systems is not to replace humans on border completely, but to make their work more efficient. If the low risk passengers can be handled by the automated systems, the border officers will have more time to focus on problematic cases.

The studied systems are more or less only pilot projects handling about one percent of the border crossings. Although not yet applicable for mass border control, the studied programmes are an intermediate step proving the concept and providing experience for the design of future systems.

A serious disadvantage of the four studied systems is the need of multiple registrations. The registration in Frankfurt will not help one crossing the border in Paris and so on. However, the introduction of electronic passports provides the means for a more universal system. Currently European passports only include facial photographs which might not be good enough for automated systems. At the latest from June 2009 European electronic passports will also include fingerprints. As their integrity is protected by the digital signature of the issuing authority, these can be trusted and interoperable biometric data usable for the automated border crossing systems. The clear advantage is no need for registration. Any passenger having an electronic passport and fulfilling additional requirements (like the EU citizenship) could use the automated system directly. The system would read the data from the passport and compare it against the freshly captured data. In the future, automated border crossing systems using electronic passports or electronic visas could handle the vast majority of travellers to and from Europe.

4.5 Summary

At the end we present a short summary of some important features of the automated border crossing systems. The aim of this study is not to evaluate and compare the systems but to present different working solutions.



System	Privium	Frankfurt	PEGASE	IRIS
Modality	Iris	Iris	Fingerprint	Iris
Biometric mode	Verification	Verification	Verification	Identification
Biometric HW	LG	OKI	SAGEM	Panasonic/SAGEM
Biometric SW	Dartagnan Middleware SW, LG SDK	Iridian	SAGEM	Iridian
Biometric FRR	< 0.01 %	Confidential	1.5 %	n/a
Operational FRR	1.5 %	Confidential	Not available	n/a
Biometric FTE	0 %	Confidential	0 %	0 %
Unicity test	No	Yes	Yes	Available
Unicity FRR	n/a	Confidential	3-5 %	n/a
Side door	Yes	Yes	Yes	No
Man trap	Yes	Yes	Yes	No
Owned by	Schiphol Group	Bundes- polizeiamt	SAGEM	Home Office
Supplied by	Dartagnan	BOSCH	SAGEM	SAGEM
Financed by	Schiphol Group	Bundes- polizeiamt	Air France	Home Office
Operated by	Koninklijke Marechaussee	Bundes- polizeiamt	Police Aux Frontières	Home Office
Price for passengers	99,00 Euro	0	0	0
Registered passengers	36 000 (end of Q1 2007)	20 900 (end of 2006)	10 000 (end of 2006)	80 000 (end of April 2007)
Crosses a day	1850	100	100 - 150	1600
Token	Contact smartcard	Passport	Contactless smartcard	None
Stored on token	Member number, iris templates, 'query string'	MRZ	Card number	n/a
Stored in DB	Name, surname, place and date of birth, nationality, document number and expiry date, home address, billing details	MRZ, biographic information from the passport and iris templates	First name, surname, date and place of birth, nationality, address, fingerprint minutiae; number, validity date and type of passport	MRZ, category, registration date, expiry date of IRIS, iris templates, facial photo.



5 References

[BWG00] Biometrics Working Group: *Best Practices in Testing and Reporting Performance of Biometric Devices*, 2000. <http://www.afb.org.uk/bwg/bestprac.html>

[CCC04] Chaos Computer Club: *How to fake fingerprints?*, 2004. http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en

[DAUG98] Daugman, J.: *Phenotypic versus genotypic approaches to face recognition*, Face Recognition: From Theory to Applications, Heidelberg, Springer-Verlag, 2004. ISBN 3-540-64410-5.

[EZO05] G. M. Ezovski: Biometric Passports: Policy for International and Domestic Deployment. Journal of Engineering and Public Policy. vol. 9, 2005.

[FRVT06] Large-Scale Results, March 2007, P. Jonathon Phillips, W. Todd Scruggs, Alice J. O'Toole, Patrick J. Flynn, Kevin W. Bowyer, Cathy L. Schott, Matthew Sharpe - National Institute of Standards and Technology, Gaithersburg, MD 20899

[ICAO04] ICAO, MRTD: PKI for Machine Readable Travel Documents offering ICC Read-Only Access

[ICAO04_2] ICAO TAG MRTD/NTWG: Biometrics Deployment of Machine Readable Travel Documents, version 2.0, including annexes A-J, <http://www.icao.int/mrtd/download/documents/>

[ICAO04_3] ICAO: Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, V 1.7, <http://www.icao.int/mrtd/download/documents/>

[ICAO05] ICAO: ICAO 9303 specification; including Supplement – 9303, 2005-4 V3.0

[ICAO07] Strategic Objectives of ICAO http://www.icao.int/icao/en/strategic_objectives.htm

[JRC06] Vakalis, J., Hosgood, B., Chawdhry, P.: *Biometric for Border Security – an Overview*, Technical Report, IPSC-JRC, 2006.

[MATS02] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: *Impact of Artificial 'Gummy' Fingers on Fingerprint Systems*, SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, January 2002. <http://cryptome.org/gummy.htm>

[NPL01] Mansfield, T. et al.: *Biometric Product Testing – Final Report*, National Physical Laboratory, 2001, <http://www.npl.co.uk/>

[UK05] UK Passport Service: *Biometrics, enrolment trial*, Management Summary, 2005.



[WIKI07] Wikipedia: RFID, <http://en.wikipedia.org/wiki/RFID>



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA.

Annex 1: Acronyms and abbreviations

ABG	Automated Biometrics-Supported Border Control
AMS	Amsterdam Airport Schiphol in the Netherlands
BAA	British Airport Authority
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CCTV	Closed Circuit Television
CDG	Charles de Gaulle airport in Paris
DB	Database
DG	Data Group
DLL	Dynamic Link Library
DPI	Dots Per Inch
EEA	European Economic Area
EER	Equal Error Rate
EU	European Union
FAR	False Accept Rate
FI	False Identification
FMR	False Match Rate
FNMR	False Non Match Rate
FRA	Airport Frankfurt / Main – Fraport in Germany
FRR	False Rejection Rate
FTA	Fail to Acquire
FTE	Fail to Enrol rate
HW	Hardware
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ID	Identity
ISO	International Standardisation Organisation
KLM	Koninklijke Luchtvaart Maatschappij
LDS	Logical Data Structure
LED	Light Emitting Diode
MAC	Message Authentication Code
MRZ	Machine Readable Zone
NIST	National Institute of Standards and Technology
NPL	British National Physical Laboratory
OCR	Optical Character Recognition
PEGASE	Programme d'Expérimentation d'une Gestion Automatisée et Sécurisée
PKI	Public Key Infrastructure
PRA	Passenger restricted area
QBG	Quick Boarding Gate
RAPID	Automatic Identification of Passengers Holding Travelling Documents
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristics
OPS	Opsporing Personen Systeem



SDK	Software Development Kit
SIS	Schengen Information System
SW	Software
UK	United Kingdom
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
WSQ	Wavelet Scalar Quantization



Annex 1: Biometric airport border control survey

The site

Airport code: Airport name:

Relevant terminal and/or gates:

Biometric authentication is used for:

- Border control
- Check-in
- Entering PRA
- Boarding
- Entering other restricted areas
- Other use:

How many biometric-enabled points/gates at airport?

Automation of the gates/points:

- Automated
- Human assisted

How many enrolment points:

Are there any outside airport?

Maturity of the system:

- Trial
- Final

Since when:

How many people use the airport?

How many people use the biometric system?

	Average	Minimum	Maximum		Average	Minimum	Maximum
Day				Day			
Month				Month			
Year				Year			

The users

For whom is the biometric authentication designed:

- Staff
- Passengers

If staff then:

- All staff
- Selected staff

If passenger then:

- Airline FF. Which airlines:
- Airport FF. How do you evaluate?
- Anybody
- Other; please specify

If staff then for relevant people

- Enrolment and use mandatory
- Enrolment mandatory, but use optional
- Enrolment optional, but if enrolled then use mandatory
- Enrolment optional, use optional

If passenger then the system is

- Open for anybody to enrol
- Closed only for a selected group of people. Specify:.....



FRONTEX
LIBERTAS. SECURITAS. IUSTITIA

Are there any categories of users: like staff/passenger and/or standard/luxury?

Are there other benefits other than automated gates offered to users?

Biometrics

Modality used:

- Fingerprints
- Iris
- Face
- Other:

Reader manufacturer type:

All readers the same?

- Yes
- No, describe:

Biometric matching/verification software

Everywhere the same SW used?

- Yes
- No, describe:

Enrolment

How many and which finger/eyes enrolled:

What documents are necessary for enrolment?

What data is required at enrolment?

How long does the enrolment take in average?

Are there any background checks done/required?

How data is stored:

- Database (what and where)
- Card (protection, encryption and digital signature, key management)
- Database + card (what and where)

Template format:

- Proprietary
- Standard – image
- Standard – processed template

How many times do you try to enrol a person if there are problems?

What is the FTE (fail to enrol) rate?

Is the enrolment finished at the place and card issued to the user (or delivered later)?

How many unsuccessful biometric tries are allowed at authentication points?

What happens if all the authentication attempts are unsuccessful?

Is verification or identification used at the biometric points?

Does the enrolment SW verify the person has not already been enrolled (as someone else)?....

Is the biometric data from biometric checks kept?

What information is logged and how the logs are processed?

What's the design of the verification points? Man-traps?



Error rates

FTA (fail to acquire):
FNMR (false non/match rate):
FMR (false match rate):
FAR (false acceptance rate):
FRR (false rejection rate):
Any difference in error rates with and without the liveness tests?

Other errors

Are there serious technical problems?
And minor ones?
Are there serious organizational problems?
And minor ones?
Any problems with the user interface, ease of use, user satisfaction? Any surveys?.....
What about speed? Average and minimum/maximum per check.
Is it really faster than normal procedures?
Are you addressing the real bottleneck?

Security

What about liveness test of the biometric sensor?
What about physical security of the HW and networks?
What about human supervision/monitoring?
Any experience with “hackers”/”attackers”?
How do you know that no detected incidents imply perfect security? Do you run your own tests?

The provider

Who operates the system?
What are the key points of the agreement with the border control authorities?
How long-term is the contract?.....
How was the company chosen?

The people

How many people are present at a time and in general employed to support the automated system?
Who are these people? Border control officials, system maintenance technicians, cleaners?
What kind of training do these people have?
How is the system maintained/cleaned etc.?

Costs

What were the investments? Numbers and structure.....
People vs. technology.....



FRONTEX
LIBERTAS SECURITAS IUSTITIA

How expensive is the maintenance/operation?.....

What are the costs per passenger?

And when compared with a classical system?.....

What are the costs for users?



FRONTEX

LIBERTAS SECURITAS JUSTITIA

European Agency for the Management of Operational Cooperation at the External Borders
of the Member States of the European Union

Rondo ONZ 1, 00-124 Warsaw, Poland
Telephone +48 22 544 95 00 Fax +48 22 544 95 01