

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 II

Automated biometric border
crossing systems based on
electronic passports and facial
recognition: RAPID and
SmartGate

2010

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 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 Agency
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 Citizen (IPSC) of the European Commission's Joint Research Centre.

Frontex wishes to thank the Border and Immigration Service (SEF) of Portugal, Australian Customs and Border Protection Service, Australian Department of Immigration and Citizenship, University of Algarve, Vision Box and airport authorities for cooperation and support extended to the Study Team before and during the visits. Furthermore, Frontex gratefully acknowledges the support of those who contributed text, data and figures.

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

The table of contents

Legal notice.....	2
Acknowledgements.....	3
Summary.....	6
1 Introduction.....	7
1.1 Introduction and objectives.....	7
1.2 Methodology.....	8
1.3 Structure of the study.....	8
2 General background to the study.....	9
2.1 Facial recognition.....	9
2.2 Electronic passports.....	13
2.3 General definition of ABC.....	18
3 Case studies.....	19
3.1 RAPID system.....	19
3.1.1 Airport characteristics.....	19
3.1.2 The RAPID project.....	19
3.1.3 Eligibility.....	20
3.1.4 Biometrics.....	20
3.1.4.1 Technology.....	20
3.1.4.2 Error rates.....	23
3.1.5 Procedures.....	24
3.1.5.1 Enrolment.....	24
3.1.5.2 Verification.....	24
3.1.6 Provider.....	24
3.1.7 Operator.....	25
3.1.8 Difficulties and problems.....	25
3.1.9 Security.....	26
3.1.10 Costs.....	26
3.2 SmartGate.....	27
3.2.1 Airport study – Brisbane.....	27
3.2.2 The SmartGate Project.....	28
3.2.3 Eligibility.....	29
3.2.4 Biometrics.....	29
3.2.4.1 Technology.....	29
3.2.4.2 Error rates.....	30
3.2.5 Process.....	30
3.2.5.1 Enrolment.....	30
3.2.5.2 Verification.....	30
3.2.6 Provider.....	38
3.2.7 Operators.....	38
3.2.8 Conclusions.....	38
4 Conclusions.....	39
4.1 Electronic passports.....	39
4.2 Facial recognition.....	41
4.3 Design of booths.....	41

4.4 Data protection.....	42
4.5 Public acceptance.....	42
4.6 Future	42
5 References.....	44
Annex 1: Acronyms and abbreviations.....	46
Annex 2: Biometric airport control survey	47
The airport.....	47
The users	48
Biometrics	48

Summary

This report describes two automated border crossing systems – RAPID in Portugal and SmartGate in Australia- based on the use of electronic passports and facial image. The two are pioneer systems operational in international airports in Portugal and Australia. In both cases electronic passports are used as the biometric data storage medium and facial recognition is the base for biometric matching.

These two key factors – electronic passports and facial recognition – differentiate RAPID and SmartGate from the other four automated biometric border crossing systems previously studied in the first BIOPASS study¹. The two systems do not require prior registration of the traveller and are interoperable. They rely on the data stored in the passport and have no control over the original registration of biometric data. Face recognition in combination with electronic passports ensures secure checking of travel documents and biometric verification of the identity of the traveller. It can perform as accurately as (or better than) human experts.

The studied systems demonstrate feasibility and compliance with technical and hardware requirements, and are fully accepted by travellers. Despite some limitations, both systems work well and enable the traveller holding an ICAO compliant electronic passport to cross the border in a convenient way.

¹ Frontex studied four systems for registered travellers at the largest European airports namely Amsterdam Schiphol, Frankfurt, Paris Charles de Gaulle and London Heathrow. The PRIVIUM program at Schiphol airport is based on iris biometric modality and uses contact smartcard as a token; ABG system at Frankfurt airport is iris based and uses a passport to enter the gate and locate the relevant record in the biometric database; PEGASE system at Charles de Gaulle airport is based on fingerprints and contactless smartcards; the UK's IRIS system is based on iris biometric modality. Prior enrollment is required for all the systems.

1 Introduction

1.1 Introduction and objectives

In 2008, the European Commission launched an initiative to prepare the next steps in border management [EC08b]. The new ideas raised by the Commission are mainly on facilitation of border crossing for *regular and frequent* travellers through automated border checks, and on the introduction of an entry/exit system to register those entering and exiting the Union. This vision of the future of border management relies to a large extent on technology to improve interoperability, security, convenience and cost-effectiveness. A key enabler is the use of biometrics in travel documents.

Automated Border Crossing (ABC) can potentially be made available to EU citizens holding electronic passports and potentially to third country nationals who are eligible for “Registered Traveller” status. However, ABC for EU citizens is different from the Registered Traveller (RT) concept for third country nationals. For EU citizens, automated gates at the external borders can be introduced under the current legal framework. Access to automated gates can be given to EU/EEA citizens holding EU electronic passports and using facial recognition as the biometric identifier, as already done in some countries today. Third country nationals could be granted Registered Traveller status after appropriate pre-screening on the basis of common vetting criteria i.e. reliable travel history, proof of sufficient means and, potentially, holding an (ICAO-compliant) electronic passport. However, amendments to the Schengen Borders Code would be needed in addition to a separate legislative proposal for Registered Traveller Programme (RTP) to allow such a system to function.

To evaluate the concept of automated border crossing, Frontex has previously studied automated border crossing systems in Europe. The first volume of the BIOPASS study [FRO07] covered systems for registered travellers at the four largest European airports: Amsterdam Airport Schiphol; Frankfurt Airport; Paris Charles de Gaulle and London Heathrow. All systems are fully working and enable the passengers to cross the border in a convenient way, however they are limited to specific airports, offer no interoperability – using different tokens for different systems – and require prior enrolment.

Since ABC systems are being taken up and increasingly tested and used by Member States², and endorsed by the European Commission to improve passenger facilitation and border security, Frontex carried out a subsequent – BIOPASS II – study on two automated biometric border crossing systems which do not require enrolment and are based on electronic passports and facial recognition: RAPID (Portugal) and SmartGate (Australia). The intent of the study is to examine how such systems operate in the EU and outside of it. More specifically, it aims to examine state of the art technology, its performance, strengths, and limitations; and how such systems complement the larger (integrated) border control process.

² Portugal, UK, Finland – ABC systems in operation; Germany – EasyPass pilot; Spain and Netherlands – planned ABC pilots in 2010.

The RAPID and SmartGate systems were chosen as they are fully-functioning, pioneer systems based on electronic passport and facial recognition that have already been operational for a number of years.

1.2 Methodology

To collect information and examine the RAPID and SmartGate systems, the Study Team - comprising of Frontex and JRC staff – visited Faro and Lisbon airport in Portugal and Brisbane airport in Australia. The experts familiarized themselves with two automated border passages and procedures in use in the EU and outside it. They held meetings and carried out interviews with key stakeholders. These interviews covered officials from governments – Border and Immigration Service of Portugal (SEF) in Portugal and Australian Customs and Border Protection Service in Australia – and representatives of the airport authorities (ANA SA in Portugal), system integrators (Vision-Box in Portugal) and research institutions (University of Algarve, Portugal).

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

1.3 Structure of the study

Chapter 2 gives an overview of facial recognition, electronic passports and general description of automated border crossing systems. Chapter 3 presents the two case studies while the conclusions are given in Chapter 4.

2 General background to the study

This chapter gives an overview of facial recognition and electronic passports. The chapter ends with a general overview and definition of systems for automated border crossing, which serves as an introduction to the two case studies presented in Chapter 3.

2.1 Facial recognition

Facial recognition is one of the three biometric modalities chosen by ICAO (the International Civil Aviation Organisation) for inclusion in machine-readable travel documents. Facial images have traditionally been used in border control. Photos appeared in travel documents with the wide spread of photographic technologies. In the digital age, photos are not only printed in passports, they are also stored in chips of electronic passports in digital form as files.

Pictures read from electronic passports can be either displayed to human operators (border guards) or processed by computers. Computer-based facial recognition can even be used for automated border crossing. In such a case, the computer compares the facial image read from the electronic passport with facial images obtained from a camera at the border crossing point.

As in any other biometric system, the quality of reference biometric data is very important and significantly influences performance of the system. ISO/IEC 19794-5 defines requirements for facial images. The specification includes requirements in areas of pose, expression, backgrounds, shadows, glasses. Technical requirements are also prescribed for focus, colours, radial distortion and colour space. In principle both scanned and digital images may be used for storage in the chip, scanned images being more problematic in practice. Biometric software typically uses greyscale information only. Sometimes colour is considered during face localisation.



Picture 2.1: An example of photograph guidelines

In facial biometric systems the source of images for comparison can be a scanner or a digital camera producing still photographs or moving images. At the border, a camera producing moving images will typically be used. A computer system analyses the images from the camera in real time and recognition software processes images if they meet certain quality requirements (e.g. focus or face orientation).

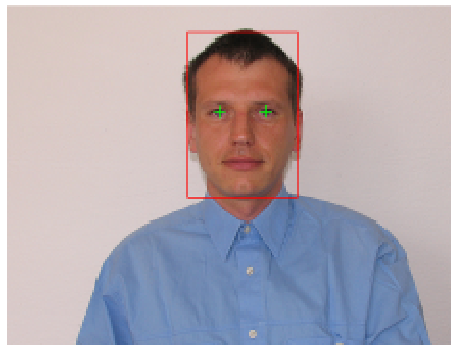
Although some details of the process of the facial recognition differ between various vendors the basic principles are the same. The process of biometric verification based on comparison of two facial images typically includes the following steps [FaceVACS]:

1. Face localisation. First of all the image is analysed for localisation of faces. The image can contain none, one or more faces. At the border it is important to consider only the faces within specified areas (i.e. of the person at the automated gate). If several faces are detected, a unicity detection will trigger an alarm, if no face is detected, the algorithm continues to wait for faces until a timeout is triggered.



Picture 2.2 Locating the face within the image

2. Eye localisation. Within the facial region detected in the previous step the eyes must be localised. From the position of the face the first estimate of the position of the eyes can be made. Further analyses will determine the exact position of the centres of both the eyes.



Picture 2.3 Locating the eye centres

3. Image quality check. Next the quality of the image must be assessed. Images of low quality (e.g. blurred images) would not result in high accuracy matching and therefore must be rejected. In case of images originating from a live camera, poor images are skipped and the following images are processed. In the case of images read from passports, sufficient quality is a consequence of the requirements of ISO/IEC 19794-5 being used at the time of enrolment.



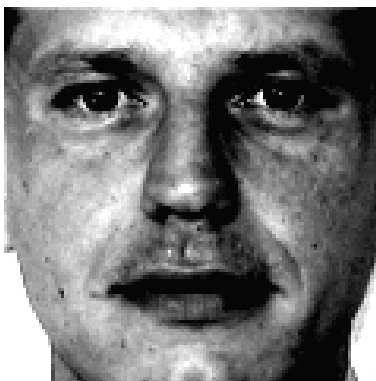
Picture 2.4: An example of a blurred image that is not acceptable for further processing

4. Face normalisation. The image of the face is scaled and rotated to obtain an image of fixed size with a predetermined position for the centres of the eyes. Such an image is also called a 'token image'. To speed-up the process of image-processing at borders, electronic passports may contain images already in the form of token images.



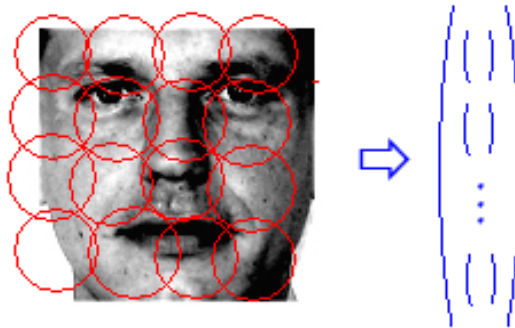
Picture 2.5: Normalized face

5. Image pre-processing. The normalized image is processed with techniques such as histogram equalisation, intensity normalisation. The aim is to remove noise originating in camera and background conditions.



Picture 2.6: Processed normalized image

6. Feature extraction. In this fundamental step the features distinguishing individual persons are extracted from the image (e.g. amplitudes at certain spatial frequencies in a local area [FaceVACS]).



Picture 2.7: Extracting the facial features

7. Reference set. The parameters extracted in the previous step are transformed into a vector to maximize the ratio of the inter-person variance to the intra-person variance. The resulting vector is called the feature set (or the biometric reference).
8. Comparison. The sequence of steps 1-7 is performed both for the reference image read from the electronic passport and for live images. For the reference image the feature set is obtained once only, for the live images the process is performed repeatedly (if necessary). The two feature sets (reference and live) are compared. The result of the comparison is a similarity level (also called a score). The resulting score is confronted with a pre-set (security) threshold to obtain the YES/NO identity match decision. The value of the threshold affects the error rates. A higher threshold is more secure, but less user-friendly (higher False Rejection Rate and lower False Acceptance Rate) and vice-versa. The real-life threshold must reflect a balance between security and usability of the system. If the final result of the comparison is YES, the identity of the traveller is confirmed. If the comparison results in a NO the process of identity verification can continue until the identity of the traveller is confirmed or the time out is triggered.

Exactly which facial features are used in comparisons is vendor-specific. Matching algorithms [FaceRec] are typically based on eigenfaces (based on sets of eigenvectors, Principle Component Analysis (PCA) is used to determine the most discriminating features between images of faces), fisherfaces (trying to maximise the between class scatter, while minimising the within class scatter, uses Linear Discriminant Analysis (LDA) or Fisher's Linear Discriminant (FLD)), the Hidden Markov model (statistical model in which the system is assumed to be a Markov process with unknown parameters) or dynamic link matching (based on artificial neural networks).



Picture 2.8: Illustration of eigenfaces [EF]



Picture 2.9: Illustration of fisherfaces

The accuracy of facial recognition systems has traditionally lagged other biometric modalities like fingerprints or iris. However, recent tests show that latest facial recognition algorithms are nearly as good as their traditional rivals [FRVT2006]. The most difficult subjects from the point of view of false acceptance are close relatives (as faces are genetically determined). False rejects on the other side can be caused by variances in backgrounds, poses, mimics, hair styles, glasses, hats, scarves or illuminations.

To avoid simple spoofing with photographs presented to cameras at the border instead of real faces, biometric systems can be equipped with liveness testing. Liveness testing in facial recognition systems [Liveness] can use multiple cameras to get the 3D image of the face or can assess the dynamics of the face in time (e.g. rotation of the face, blinking or facial mimics). An alternative to liveness detection can be monitoring of the area. Securely designed systems will typically combine both countermeasures.

2.2 Electronic passports

Electronic passports [ICAO9303] combine a booklet with a contactless chip capable of secure data storage. The main driving factor behind the introduction of electronic passports was to increase the security of travel documents. Electronic passports can store biometric data in the form of images and/or templates for three biometric modalities: face, fingerprint and iris. The integrity of stored data is protected by a digital signature of the issuing institution. These institutions are called Document Signers (DS). The public keys of the

Document Signers are certified by the Country Signing Certification Authority (CSCA) in the form of a DS certificate. The digital signature can only be verified if the CSCA certificate of the issuing country is available. The protection of the integrity of the stored data is called the passive authentication. With the help of cryptographic protocols, the authenticity of the document can also be verified (protocols called active authentication and chip authentication). As a result, the passport allows for identity verification of the passport holder using biometric data whose integrity has been secured, read from a document whose authenticity has been verified.

Electronic passports are defined in the 6th edition of the ICAO (International Civil Aviation Organisation) Document 9303 Part 1. Electronic passports in EU countries were introduced by Council regulation (EC) 2250/2004. This regulation mandates EU and associated states (UK and Ireland do not participate, but Norway, Iceland and Switzerland do) to introduce electronic passports with facial images within 18 months and electronic passports with fingerprint images within 36 months (after additional technical specifications are established). These details were specified in Commission decision C(2005) 409 for electronic passports with facial images (also called first generation passports) on 28 February 2005 (therefore the deadline was on 28 August 2006). Commission decision C(2006) 2909 from 28 June 2006 sets the technical specifications of the electronic passports with fingerprint images (also called passports of the second generation). The deadline to introduce passports with fingerprint images therefore was 28 June 2009.

Facial biometric data in the electronic passport is stored as a standard bitmap image as this is currently the only interoperable format. Two image formats are allowed: JPEG and JPEG2000 (both use “lossy” compression algorithms³, JPEG2000 being a newer standard offers better compression rates for comparable image quality). In addition to the image, the position (i.e. coordinates) of certain facial features (e.g. eyes) within the image can be specified. At the moment, however, most of the countries do not store such feature points in their passports. Facial images must meet certain requirements to allow a reliable biometric verification. These requirements are set in the international standard ISO/IEC 19794-5, which specifies properties of three image types: frontal image, full frontal image and token image. Requirements are increasing; token image being the most strictly defined one.



Picture 2.10: The process of forming the token image.

³ A **lossy compression** method is one where **compressing data** and then decompressing it retrieves data that is different from the original, but is close enough to be useful in some way

Fingerprints are (in the EU) stored as images in WSQ images (Wavelet Scalar Quantisation – a lossy compression format optimised for fingerprints). The main reason for using images is interoperability. Whenever possible (and except for children), images of left and right index fingers will be stored in the passport. Fingerprint images constitute sensitive personal data and therefore the reading of fingerprints is protected with an additional mechanism called Extended Access Control (EAC).



Picture 2.11: Sample pictures of left (acquired by Microsoft Fingerprint Reader) and right (acquired by Sagem Morphosmart 300) index fingers.

Extended Access Control [EAC111] introduces two new protocols. Terminal Authentication makes sure that only authorized passport readers get access to fingerprint images. The Chip Authentication protocol verifies the authenticity of the chip.

During the terminal authentication the reader must prove it has been authorised to read the fingerprints. First, the reader presents a set of certificates which show the authorisation of the reader to access the secondary biometric data and then the reader must prove its own identity (via a challenge-response protocol). Because the passport can be also read in other countries – other than the country of issue – the scheme requires a relatively heavy PKI (Public Key Infrastructure).

Each country establishes a CV (Country Verifying) certification authority (CA) that decides which other countries will have the access to fingerprint images in their passports. A certificate of this authority is stored in passports (issued by that country) and it forms the starting trust point (root certificate) for access control. Other countries wishing to access fingerprint data (no matter if in their own passports or in passports of other countries), must establish a DV (Document Verifier) certification authority. This authority will obtain certificates from all countries (i.e. from their CVCAs) willing to grant access to the data in their passports. The DV CA will then issue certificates to end-point entities actually accessing the biometric data – the inspection systems (IS). See figure 2.1.

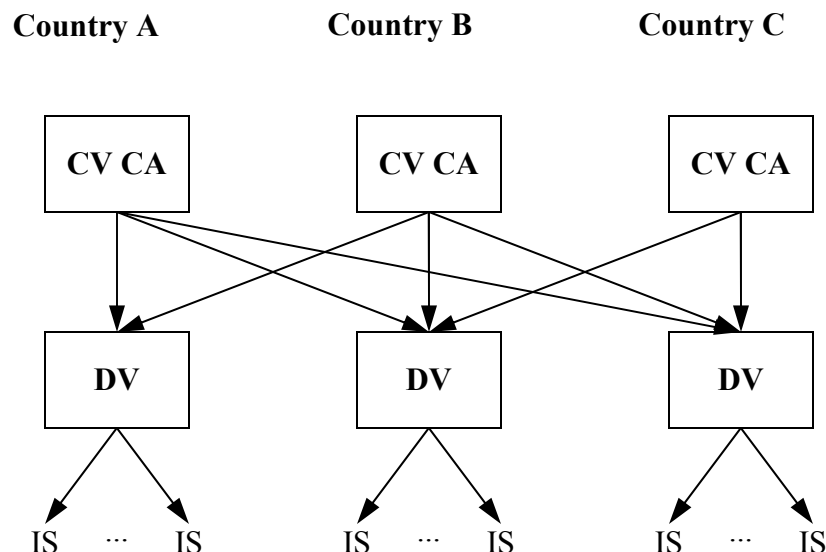


Figure 2.1: A simplified view of an EAC PKI hierarchy.

Each passport stores a CVCA certificate of the issuing country (in our example of a country A e.g. Austria). If an inspection system (in a country B e.g. Belgium) needs to convince the passport that it is authorized to access the fingerprints, it must provide the DV certificate (the Belgian one in our case) signed by the issuing CVCA (Austria) and its own IS certificate (for that particular IS) signed by the DV certification authority (i.e., Belgian in this case). After the passport verifies the certification chain it has to check whether the inspection system can access the corresponding private key. That is performed using a challenge-response protocol. If the authentication succeeds, the inspection system can access fingerprint images (stored in the file DG3).

As the computational power of passport chips is limited, simplified certificates (so called card verifiable certificates) are used instead of the usual X.509 certificates. An interesting point is the verification of certificate validity. As the chip has no internal clock, the only available time-related information is the certificate issue date. If the chip successfully verifies the validity of a given certificate issued on a particular day, then it knows that this date has already passed (or is today) and can update its own internal time estimate (if the value is newer than the one already stored). The combination of storing the internal date estimate in the chip and of short certificate validity should protect sensitive biometric data against stolen inspection systems (i.e. they would be usable only for a short time). This protection is, however, effective only if the passports are frequently read by inspection systems (and therefore the internal date estimate is often updated).

Fingerprint images read from European electronic passports can only be used for identity verification -so called 1:1 matching- and immediately after the comparison must be deleted (privacy protection issue). To facilitate the mutual certification of member states where DVs must be certified by CVCA of other countries, a common -minimal and mandatory- Certification Policy and a protocol for communication between the CVCA (used by single points of contacts in a country) have been developed.

In addition to the terminal authentication, the European EAC also introduces the Chip Authentication protocol. During the chip authentication, a reader can verify whether the chip can access the private key belonging to the public key stored in DG14 (and whose integrity is protected by the digital signature). This cryptographic protocol verifies whether the chip in the passport is genuine and protects against passport cloning. It also improves the encryption level of the following Secure Messaging communication and therefore protects the transmission of the fingerprints against eavesdropping better than by using the keys derived during the Basic Access Control.

Second generation passports can still be read by inspection systems not supporting Extended Access Control (or supporting it but not having the right authorisation), but the fingerprints in the file DG3 will not be accessible. This backward compatibility is also important for worldwide interoperability. Although there are efforts to standardise EAC at the ICAO level, at this moment EAC is an EU-specific protocol.

Reading of second generation passports with fingerprints takes longer than reading passports without fingerprints. The chip authentication and terminal authentication protocols require transmission of cryptographic keys and certificates and non-trivial cryptographic operations are required to be performed by the chip. Additionally the fingerprints stored in DG3 must be read, adding some 25 kilobytes of data. On the other hand, modern chips are significantly faster (and support higher transmission speeds) than the chips available 2-3 years ago. The latest EAC chips (under ideal conditions) can finish the inspection procedure in less than 3 seconds, including the basic access control authentication, chip authentication, terminal authentication and reading of facial and fingerprint images [PRAGUE08].

To summarize the requirements for inspection systems reading electronic passports at the border:

- Inspection systems must be able to read (via optical character recognition – OCR) the machine-readable zone of the passport to be able perform basic access control authentication.
- Inspection systems must be equipped with the list of CSCA (country signing certification authority) certificates of all countries, whose electronic passports are to be validated. Such certificates must be obtained in a trustworthy way (usually via diplomatic channels from the other countries).
- To be able to access fingerprints in electronic passports, inspection systems must have a set of DV and IS certificates authorizing reading of the DG3. For each country a separate DV certificate is required. IS certificates can (but not do not necessarily have to) be shared for several countries if technical parameters allow.
- To increase the security of passport control it is desirable to also perform a check of the physical security features of the passport (e.g. under UV and IR illumination).

2.3 General definition of ABC

Automated Border Crossing (ABC) can be defined as the use of automatic or semi-automatic systems that can verify both the identity of travellers and their authorisation to cross the border at a Border Crossing Point (BCP) without the need for human intervention. ABC systems can be divided into two types: (a) systems based on the use of an electronic travel document and (b) systems based on pre-enrollment which generally take the shape of Registered Traveller Programmes. The former will serve as a basis for this study.

ABC systems – based on the use of an electronic travel document - in case of RAPID and SmartGate use electronic passports as the biometric data storage medium and facial recognition is the base for biometric matching. The automated border crossing process starts with passport scanning. The traveller inserts the datapage of the passport into the passport reader. The reader checks physical security features, reads the MRZ (Machine Readable Zone) and communicates with the chip in the passport to read the data and to verify the authenticity of the document. A facial image of the traveller obtained at the border is then compared with the one stored on the chip. This process is fundamentally the same as in the classical border booth. If the matching is successful, the gate opens and the traveller crosses the border. If a successful match is not obtained, the traveller is referred to a manual booth. Human oversight can be provided by a border guard officer, who supervises the whole process, including the matching of the facial images.

3 Case studies

In this chapter the two case studies are reported.

3.1 *RAPID* system

3.1.1 Airport characteristics

Faro airport (FAO) serves the entire coastal area of Portugal's southern-most province. The airport receives mainly tourist visitors although it is also increasing its share of business travellers. Faro airport serves nearly 6 million passengers a year of which 90 percent are subject to border checks, as most of them arrive from or depart to the UK and Ireland (2008 est.), which are not part of Schengen.

Lisbon (LIS) airport is the main international gateway to Portugal and a major European hub. It is one of the largest airports in Southern Europe. The airport has two main runways. Passenger traffic has grown in the last few years and currently the airport serves around over 13 million passengers a year (2007 est.) of which 45 percent are border checked.

To meet the growing demand in air transportation, Lisbon airport is undergoing expansion. The development plan included the construction of Terminal 2 - operational since August 2007- and the expansion of the current main terminal with new boarding gates, air bridges and parking positions, and a more efficient use of the existing infrastructure.

Both airports are operated by the state-owned company ANA SA (Aeroportos de Portugal).

3.1.2 The *RAPID* project

The *RAPID* project – Automatic Recognition of Passengers with Credentials – has been launched by the Portuguese authorities to (1) facilitate the increasing flow of passengers at the airports, (2) enhance service levels at the airports (speed and convenience), (3) save personnel resources and (4) reduce costs.

The *RAPID* system is based on facial recognition and allows automated border crossing of passengers holding EU/EEA electronic passports. This is the first operational system in Europe to allow automatic border checks of passengers with electronic passports without the need for enrolment.

The system started as a pilot project with ten booths at Faro airport in May-June 2007 and after an evaluation conducted by the University of Algarve, it became operational. Since August 2007, the *RAPID* system has been operational at Lisbon airport and the plan is to deploy *RAPID* at all Portuguese international airports and ports.

Currently, there are 69 *RAPID* e-gates operating at major international airports in Portugal of which Faro airport has 10, Lisbon airport 20, Porto airport 19, Funchal airport 8, Lajes 6 and Ponta Delgada 6. Portuguese authorities are planning to install a total of 110 *RAPID* e-gates at all international airports and ports.



Picture 3.1: The RAPID gates at Faro airport

3.1.3 Eligibility

The RAPID system is designed for citizens of EU/EEA countries entitled to unrestricted freedom of movement who are 18 years or older and hold an EU/EEA electronic passport. Due to restrictions under Portuguese law, no passengers under the age of 18 are allowed to use the system. Therefore, no plans to extend the age group are foreseen in the near future. Citizens of other countries are not accepted at the moment. According to the latest figures 570 000⁴ passengers have used the system so far.

The RAPID system does not have any specific user categorization nor does it have other benefits except for the automation of border crossing.

3.1.4 Biometrics

3.1.4.1 Technology

The RAPID system uses Viisage hardware to read the passport (same as used in the manual booth). The automated border control starts with passport scanning. The traveller inserts the datapage of his/her passport into the passport reader. The reader is an integrated full page reader combining a scanner of the datapage at different wavelengths (visible light, ultraviolet light and infrared light), optical character recognition of the machine readable zone (MRZ) and RF (radio frequency) reader for communication with the electronic part of the passport. The passport reader checks physical security features, scans and recognizes the MRZ and

⁴ From August 2007 to May 2009

then communicates with the chip in the passport. The process is fundamentally the same as in the classical border booth.



Picture 3.2: The passport reader in front of the RAPID gate

When the passport is successfully read and verified, the front door opens and the traveller enters the booth. In the booth there is a monitor displaying instructions and 2 cameras. As soon as the traveller enters the booth, the vertical position of the cameras adjusts automatically according to the height of the traveller. One of the cameras is a standard wide-angle low resolution CCTV camera and is used only for surveillance purposes. The other camera is an industrial quality high resolution -2 megapixels -camera. The output of this camera is used for the biometric verification of the traveller. Two images per second are analyzed and compared with the passport photo of the traveller until a correct match is detected or time runs out after 30s.



Picture 3.3: The inside of the automated RAPID gate

The biometric software used was chosen by the best performance rate. Several biometric matching algorithms were tested during the trial. Real biometric data from the field (images read from passports and obtained by the camera in the booth) was used to compare the accuracy of competing algorithms. The best accuracy was achieved by the Cognitec face matching algorithm which is currently used in the RAPID system. The quality threshold is set to 40 percent.

The passport, biometric and other components were integrated by the company Vision-Box which also developed the supervising software.



Picture 3.4: Screenshot of the RAPID management software

The next version of the system will include several improvements, both at the hardware and software levels. To mention just a few, a second monitor screen will increase the interaction of the user with the system at the point of insertion of the passport into the reader, and an intelligent CCTV monitoring system –fully integrated with the RAPID system – will optimize the automated process based on the processing of the images being captured by the cameras. Finally, a liveness test will guard against the threat of spoofing attacks.

3.1.4.2 Error rates

There are several ways to organize tests of biometric systems and compute error rates. The usual method of calculating False Acceptance Rate (FAR) is to consider so called zero-effort forgeries. In such cases, people do not try to modify their appearance, they only randomly try to match their natural face with the biometric data (facial image) of someone else. Such a test was run by the Vision-Box company by using the test data from real field. The results showed the zero-effort FAR of 0.03 percent (at the matching threshold of 40 percent).

The study of the Algarve University took a more realistic approach and tried to match similar people [Alg07]. It is natural that their success rate was higher. Students managed to find 448 pairs of similar people who could be falsely accepted - a total of 1.25 percent of cases (mainly twins and mothers/daughters). It is also worth noting that after the initial fine-tuning, the security of the system is higher and currently the false acceptance rate would be lower. The study confirmed that for facial biometric systems the most difficult subjects to distinguish between are relatives -genetically related people- like twins or parents and their children.

According to Vision-Box tests, the theoretical False Rejection Rate FRR (for the matching threshold of 40 percent) is 4.25 percent. The study of the Algarve University reports an FRR of 5.2 percent. After the study was performed, the design of the light source was improved and the current false rate is now lower. Reasons for failure by the biometric system to correctly recognize travellers vary. It is estimated that 17% of the false rejections can be attributed to the use of glasses; other factors include wearing hats or occluding the face with hair.

The biometric error rates of the RAPID system based on facial recognition are slightly higher than of comparable biometric systems based on fingerprint or iris, but a strong advantage of the RAPID system is the absence of a need for registration of travellers with electronic passports without secondary biometric data.

3.1.5 Procedures

3.1.5.1 Enrollment

The RAPID system does not require any particular enrollment. Anybody who is eligible to use the system and has an ICAO compliant electronic passport can immediately use it.

3.1.5.2 Verification

The automated border check starts with the passport scanning. The traveller inserts the datapage of the passport into the passport reader. The reader checks physical security features, reads the MRZ (Machine Readable Zone) and communicates with the chip in the passport. This process is fundamentally the same as in the classical border booth and can take as little as 20 seconds.

When the passport is successfully read and verified, the front door opens and the traveller enters the booth. In the booth there is a monitor displaying instructions and 2 cameras. One of the cameras is a standard wide-angle low resolution CCTV camera and is only used for surveillance purposes. The other camera is an industrial quality high resolution 2 megapixels camera. The output of this camera is used for the biometric verification of the traveller. Two images per second are analysed and compared with the passport photo of the traveller. If the matching is successful, the second door opens and the passenger has passed the border. If a successful match is not obtained within 30 seconds, the first door opens and the passenger is referred to a manned booth. Human oversight is provided by a border guard officer in a booth, who supervises the whole process, including the matching of the facial images, for all gates.

3.1.6 Provider

The system was implemented by Border and Immigration Service of Portugal (SEF) and the company Vision-Box.

3.1.7 Operator

Owner and operator of the system is Border and Immigration Service of Portugal (SEF). All the immigration officials at the airport have been trained to work with the system. Training takes one day.

3.1.8 Difficulties and problems

The RAPID system is the first European automated border control system based on facial recognition and electronic passport which does not require prior registration. Having the system based on electronic passports means that the reader must be able to communicate and read electronic passports of several countries supplied by various manufacturers (in contrast with proprietary systems where the readers and cards are supplied by a single vendor). Although all electronic passports are based on the same standard (ICAO Doc 9303 referring to ISO 14443 regarding the low level communication), not all the EU electronic passports are read equally well. Unfortunately no detailed statistics of readability of electronic passports and related issues are available. The only relevant information regarding the various passports with different origins within the EU, being read at the gates, is the time required to fully read the data from the chip (as not all the countries have adopted the same chip manufacturer and also the formats of recorded data). In consequence, the reading time varies between 4 and 10 seconds depending on the country and date of issuance.

An electronic passport can only be considered to be valid when the passive authentication is checked. Therefore passive authentication is one of the basic building blocks of the security of the whole automated system. To be able to perform passive authentication, the Country Signing Certificate of the issuing country must be available. Such a certificate is not a secret, but it is crucial to guarantee its integrity, and therefore the certificate must be obtained using bilateral diplomatic exchange.

Availability of the CSCA certificates is currently a problematic issue and not only the RAPID system has to cope with this fact. As the RAPID system is available only for EU/EEA nationals, the situation is easier than a general worldwide case and the certificate exchange can be facilitated for example by the Article 6 committee on visa requirements. Upgrade of the RAPID system to be able to use also the fingerprint images in the passports, will also require implementation and access to certificates and private keys of the EAC PKI.

For the accuracy of facial biometric systems the light conditions are very important. Non-ideal light conditions increase significantly the false rejection rate. The issue of light conditions was addressed seriously by the integrator of the system. The results have been constantly evaluated and improvements in the position and type of light source have been made.

Relying on electronic passports to provide the link between the individual and his/her biometric data allows omission of the registration process, but also makes the system dependent on the biometric enrollment done in various countries possibly with various requirements. Not all the issued passports fully fulfill the ICAO requirements on facial

images (e.g. the background, pose or size of the head is different). The RAPID system has to cope with scanned images (in some cases only in grayscale), aged photographs and sometimes even with mirrored images. Similar situation might repeat with the second generation passports storing also the fingerprint images

3.1.9 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.

3.1.10 Costs

According to Border and Immigration Service of Portugal (SEF), the system is cost effective and can pay for itself in 2 years. A study on its cost effectiveness is available.

3.2 SmartGate

SmartGate – an automated border processing solution – is being rolled out by Australian Customs and Border Protection Service at Australia’s international airports. It uses the data in the electronic passports and facial recognition technology to perform the customs and immigration checks that are usually conducted by a Customs and Border Protection officer.

The two-step process (involving a kiosk and a gate) is currently operational at Adelaide, Brisbane, Cairns, Melbourne, Perth and Sydney international airports. SmartGate kiosks are also available at Auckland Airport departures enabling eligible travellers to undertake the first step of their entry process into Australia before they depart New Zealand.

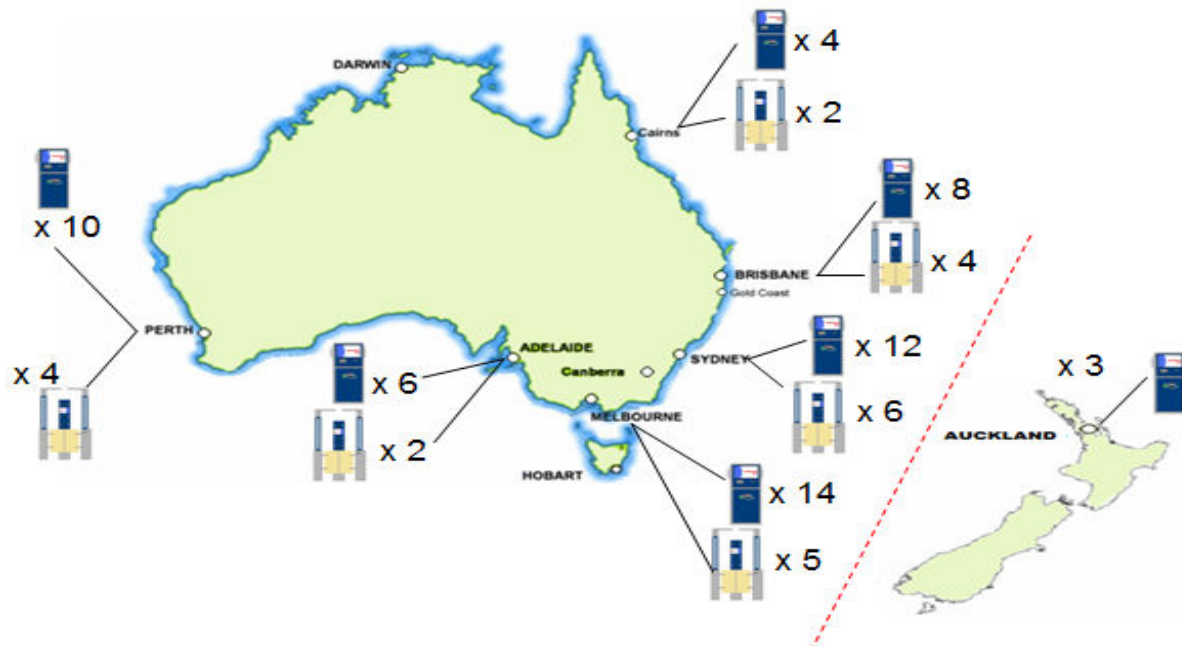


Figure 3.1: Map showing SmartGate current locations with number of kiosks and gates in each.

3.2.1 Airport study – Brisbane

Brisbane International Airport has two terminals - international and domestic – and it serves 3 500 000⁵ passengers a year. Peak times at Brisbane Airport are between 6:30 and 7:30 in the morning.

Brisbane was the first airport to receive SmartGate, selected for the initial implementation due to its lower volume of inbound passengers than the larger airports, high degree of cooperation and enthusiasm demonstrated by both the airport operator and Customs and Border Protection Service staff and a less complex implementation task due to the absence of a trial (or interim) solution that existed in Sydney and Melbourne.

Upon opening in August 2007, a two-week public trial of SmartGate took place encompassing an extensive testing program to ensure that SmartGate was effective and user-

⁵ From June 2007 to April 2008.

friendly. Nineteen hundred Australian electronic passport holders were processed under controlled conditions during the trial period. The trial showed that the face recognition technology worked as expected, that the traveller experience was extremely positive and that the impact on business processes was minimal. Of the 200 travellers who were interviewed as part of the traveller experience assessment: 86 percent rated the solution ‘easy to use’; 99 percent would use it again; 98 percent would recommend it to people they know and 93 percent of previous overseas travellers felt it made the arrivals experience better.



Figure 3.2: SmartGate at Brisbane International Airport

3.2.2 The SmartGate Project

SmartGate allows eligible travellers with electronic passports to self-process through passport control. SmartGate is a two-step process. The first step, at the kiosk, is where the electronic passport is read and a ticket issued to the passenger. At step two, the gate, the passenger inserts the ticket and biometric verification matches the passenger’s live photo with the reference image read from their electronic passport.

SmartGate is now fully operational at Adelaide, Brisbane, Cairns, Melbourne, Perth and Sydney international airports for arriving travellers. SmartGate kiosks are also available at Auckland Airport departures enabling eligible travellers to undertake the first step of their entry process into Australia before they depart New Zealand. SmartGate will be progressively introduced into further Australian international airports.

The following table shows usage statistics of each airport as at 17 January 2010:

	Brisbane (August 2007)	Cairns (January 2008)	Melbourne (September 2008)	Adelaide (December 2008)	Perth (April 2009)	Sydney (July 2009)	Auckland (September 2008)	Total
Number of users	202,657	19,453	352,275	31,475	149,362	282,766	18,055	1,056,043

Table 3.1: Usage figures until 17/01/10

3.2.3 Eligibility

SmartGate is currently available for citizens of Australia and New Zealand, aged 18 years and over. Initially available to Australian electronic passport holders, SmartGate was opened to New Zealand electronic passport holders on 17 December 2007.



Picture 3.1: SmartGate signage

underway to consider extending SmartGate for outwards processing, its application to the sea port environment and to open eligibility to other nationalities that have International Civil Aviation Organisation (ICAO) compliant electronic passports. No prior registration is required for eligible passengers and there is no fee charged for using SmartGate.

Nationals of all countries need a visa for entry into Australia. New Zealand is the only country whose citizens can obtain a visa at the Australian border. The Australian legislation has been changed to enable certain non-citizens arriving in and departing from Australia to have their identity and visas verified in an automated way. The new provisions also enable New Zealand citizens to be immigration cleared via SmartGate and granted a Special Category Visa (SCV).

SmartGate is currently used to process arriving travellers into Australia's airports. Scoping is

3.2.4 Biometrics

3.2.4.1 Technology

SmartGate uses facial biometric technology. The reference image read from the electronic passport (in Datagroup 2 in JPEG or JPEG2000 format) is biometrically compared with a live image of the passenger.

Sagem Australasia is the Australian Customs and Border Protection Service's strategic partner for SmartGate for the facial recognition component. The biometric matching algorithm was supplied by Cognitec and extensively modified by Sagem. The electronic passport reader is supplied by Rochford Thompson and the camera capturing the live image of the passenger is manufactured by Guppy Allied.

3.2.4.2 Error rates

SmartGate is subject to a comprehensive testing program including vulnerability testing. For security reasons, performance figures could not be provided by Australian Customs and Border Protection Service. However, Typical causes of false rejections include people not looking at the camera or poor quality photos stored in electronic passports. During peak times, passenger behaviour tends to be better since passengers can observe other passengers using SmartGate and repeat it. After using SmartGate a few times, passengers become accustomed to the system and can use it with ease.

A public information campaign was launched in November 2008, encompassing an in-flight video, print advertisements and in-airport advertising to educate travellers on eligibility criteria and how to use the solution.

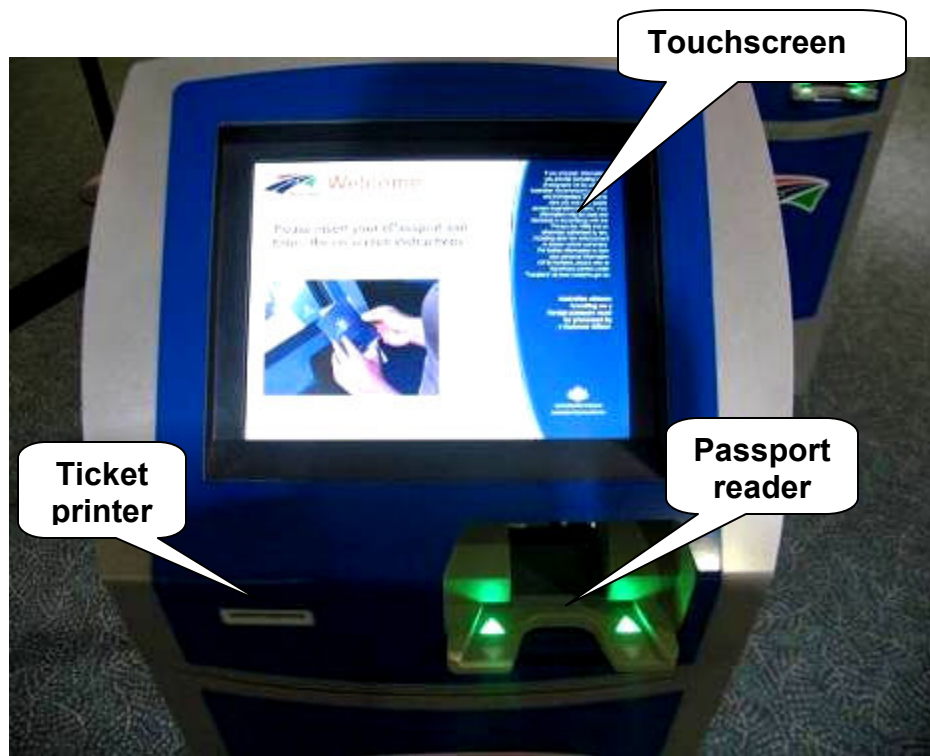
3.2.5 Process

3.2.5.1 Enrolment

No enrollment is necessary to use SmartGate. It is open to all eligible electronic passport holders, currently Australian and New Zealand citizens aged 18 and over.

3.2.5.2 Verification

SmartGate is a two-step process involving a kiosk and a gate. Step 1, the kiosk, checks if a passenger is eligible to self-process and step 2, the gate, verifies identity and final clearance. The kiosk verifies whether the passenger is expected at the Australian border i.e. a database of incoming flights is queried for a record of the passenger with matching passport data. If a record is found, the passenger's eligibility to use the automated option is verified.



Picture 3.2: The user interface of the kiosk



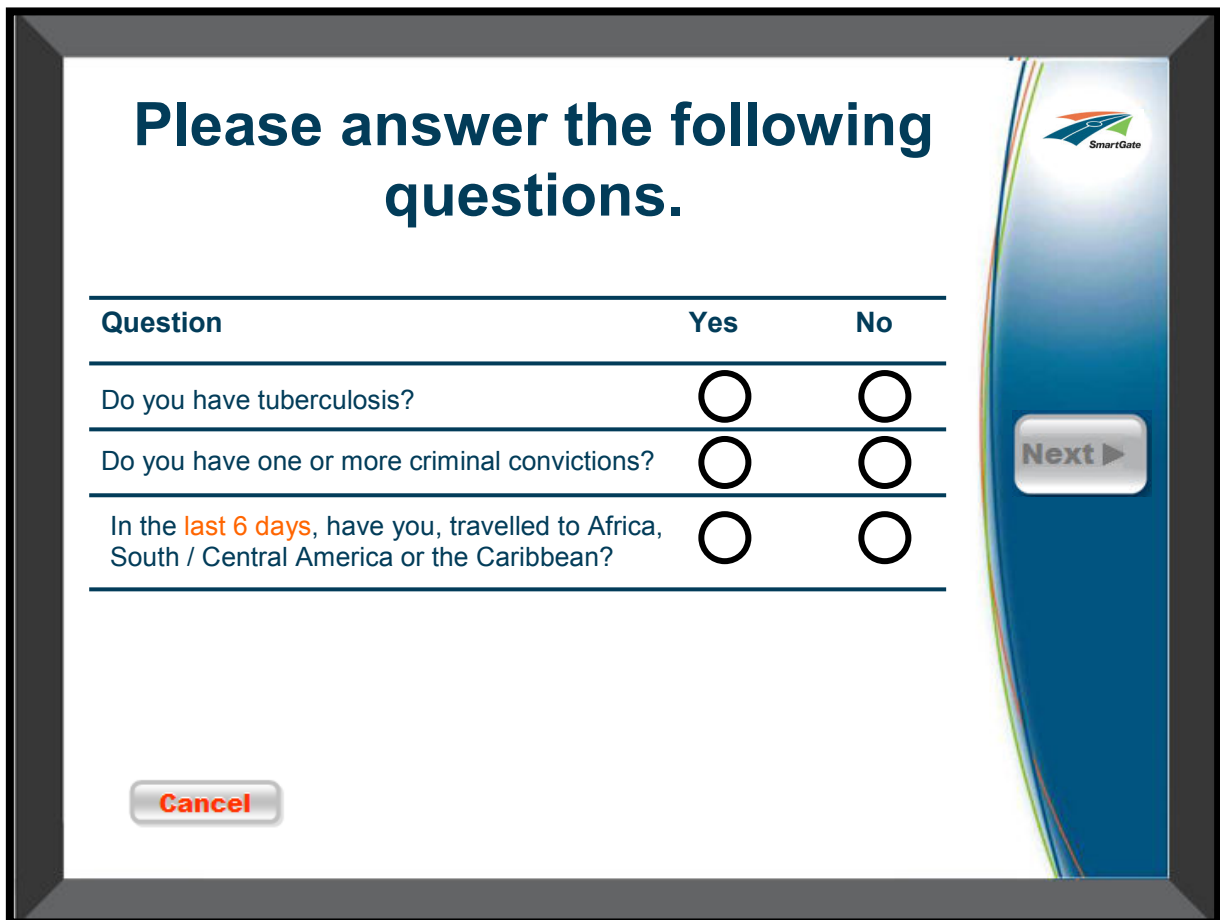
Picture 3.3: A concourse kiosk at Melbourne International Airport

When the electronic passport is inserted in the passport reader, the MRZ data is used to access the passport chip (Basic Access Control) and the kiosk reads the contents of the chip. The data held on the chip is validated against the MRZ data. Passive authentication is performed against Country Signing Certificates, Document Signing Certificates and Document Revocation Lists stored on the Customs network. These certificates are manually

downloaded from the ICAO PKD (Public Key Directory) at present, but planning is underway to connect SmartGate to the PKD through a LKD (Local Key Directory). The passport data is stored in a database which is accessed by the gate.

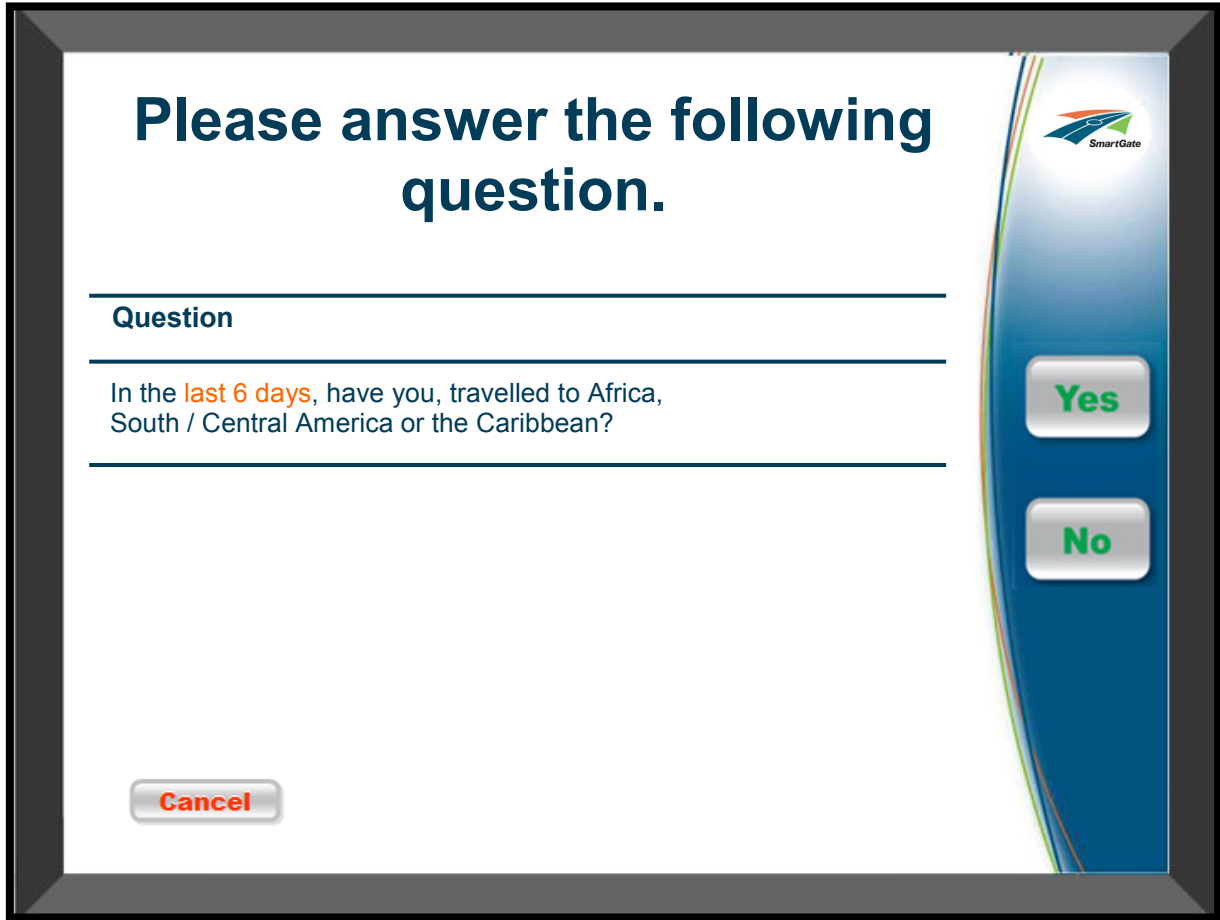
The process at the kiosk involves the passenger answering questions on the touch screen. Currently, Australian citizens are asked one question concerning yellow fever. New Zealand citizens are asked two additional questions about whether they have tuberculosis or a criminal conviction as part of the visa issuance process.

The following images show the question screens:

The image shows a touch-screen interface for the SmartGate system. At the top, the text "Please answer the following questions." is displayed in a large, bold, dark blue font. Below this is a table with three rows of questions. Each row has a "Question" column, a "Yes" column with a radio button, and a "No" column with a radio button. The questions are: "Do you have tuberculosis?", "Do you have one or more criminal convictions?", and "In the last 6 days, have you, travelled to Africa, South / Central America or the Caribbean?". The text "last 6 days" is highlighted in orange. To the right of the table is a large blue vertical bar with the "SmartGate" logo at the top and a "Next" button with a right-pointing arrow. At the bottom left of the screen is a "Cancel" button with red text. The entire interface is framed by a dark grey border.

Question	Yes	No
Do you have tuberculosis?	<input type="radio"/>	<input type="radio"/>
Do you have one or more criminal convictions?	<input type="radio"/>	<input type="radio"/>
In the last 6 days , have you, travelled to Africa, South / Central America or the Caribbean?	<input type="radio"/>	<input type="radio"/>

Picture 3.4: Question screen for non-Australian citizens



Please answer the following question.

Question

In the **last 6 days**, have you, travelled to Africa, South / Central America or the Caribbean?

Yes

No

Cancel

The image shows a digital screen with a dark grey border. The main content area is white. At the top, it says 'Please answer the following question.' in bold dark blue. Below this is a horizontal line, followed by the word 'Question' in bold dark blue. Another horizontal line follows. The question text is 'In the last 6 days, have you, travelled to Africa, South / Central America or the Caribbean?'. 'last 6 days' is in orange. Below the question is another horizontal line. On the right side, there is a blue vertical bar with a 'SmartGate' logo at the top. It contains two large buttons: 'Yes' and 'No', both in green text on a light grey background. At the bottom left of the screen is a 'Cancel' button in red text on a light grey background.

Picture 3.5: Yellow fever question screen for Australian citizens

Did you travel to any of the countries listed?

Africa

Angola	Ghana	Sierra Leone
Benin	Guinea	Somalia
Burkina Faso	Guinea-Bissau	Sudan
Burundi	Kenya	Tanzania
Cameroon	Liberia	Togo
Central African Republic	Mali	Uganda
Chad	Mauritania	
Cote d'Ivoire (Ivory Coast)	Niger	
Democratic Republic of Congo	Nigeria	
Equatorial Guinea	Republic of the Congo	
Ethiopia	Rwanda	
Gabon	Sao Tome and Principe	
Gambia	Senegal	

South/Central America and Caribbean

Argentina – Misiones Province	Guyana	Venezuela
Bolivia	Panama	
Brazil	Paraguay	
Colombia	Peru	
Ecuador (excluding Galapagos Islands)	Suriname	
French Guiana	Trinidad and Tobago	

Buttons: Yes, No, Cancel, Back

Picture 3.6: Part two (if answered yes to part one) of yellow fever question

If the passenger is eligible to proceed to step 2, the gate, the kiosk issues a ticket. The front side of the ticket contains instructions along with the date and time of the transaction at the kiosk and coding which indicates whether the passenger is required to undergo secondary inspection. The back of the ticket contains a magnetic strip encoded with passenger reference information.

IMPORTANT! HOLD ONTO THIS TICKET

Instructions:

- Insert this ticket into the exit
- Hold onto the ticket, along with your Incoming Passenger Card
- Collect your luggage from the baggage carousel
- Hand in your ticket and Incoming Passenger Card to the Customs Officer

Transaction Details:

CHECKED - 27 Jun 2008 - 08:04 - BNEABPIK001
 CLEARED - 27 Jun 2008 - 08:14 - BNEABPIGA25

FCRW

FIRSTNAME MIDDLENAME SURNAME

Labels: Date, time, port of issue and kiosk ID; Date, time, port of issue and gate ID; Traveller name; Code

Picture 3.7: The SmartGate ticket

Eligible passengers at Auckland Airport can obtain tickets before they arrive to Australia. If a traveller is not eligible to use SmartGate, they will be instructed to proceed to an assistance desk for manual processing by a Customs and Border Protection officer.



Once the passenger has a ticket, they can proceed to the gate where the biometric verification takes place. First the passenger inserts their ticket and the magnetic strip on the back of the ticket is read to locate the passenger's record in the database (which includes the biometric data read from the electronic passport). This activates the camera lights and the passenger is instructed to look at the camera.

Picture 3.8: Inserting the SmartGate ticket

The gate camera compares the face with the reference image (passport photo) read from the electronic passport. When the biometric verification succeeds and clearance is verified, the date and time of the transaction is printed onto the ticket and the ticket is returned to the passenger. The glass barriers open and the passenger can proceed to baggage collection and the Customs/quarantine secondary inspection area (no further automation is offered to SmartGate users at this point).



Picture 3.9: The gate consists of the door, ticket reader (on the right side), cameras (opposite the passenger) and light sources

If the biometric verification fails or clearance is not verified, the glass barriers do not open and the passenger is instructed to go to an assistance desk for manual processing.



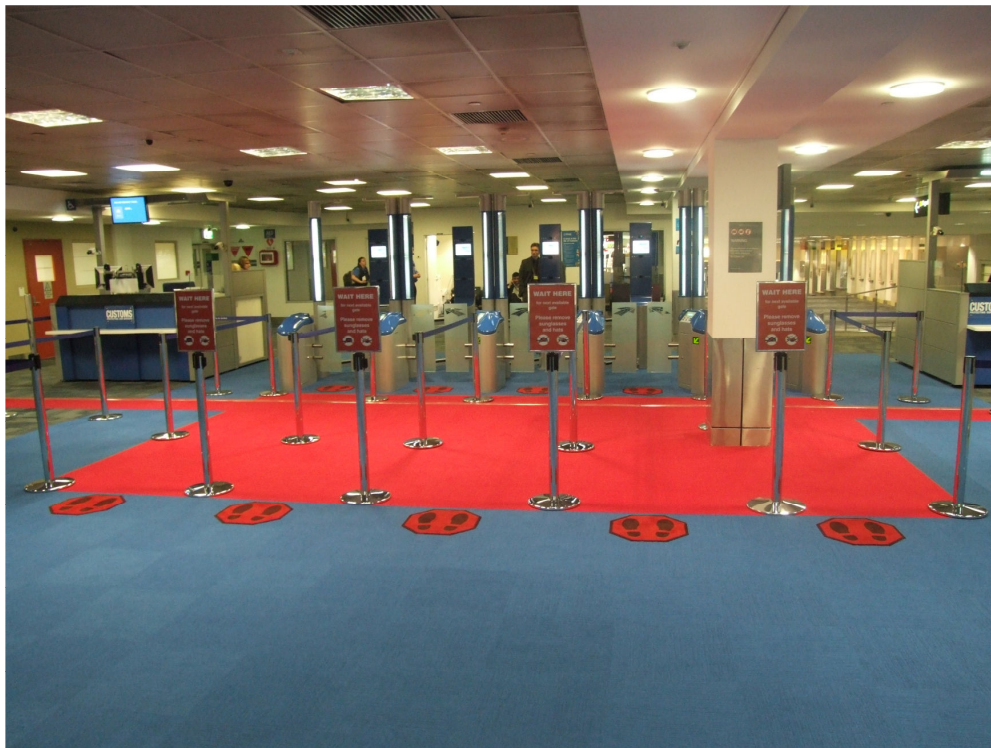
Picture 3.10: To be successfully biometrically verified it is important to stand at indicated place and look straight ahead at the camera

The automated gates do not follow the man-trap or booth design of other systems. They have been designed to offer travellers convenient passage through the process. Infrastructure barriers, such as signage and floor markings, provide a strong cognitive barrier between the queuing and the gate standing points. Moreover, the border area is controlled and the non-automated customs inspection follows thereafter.

The MRZ and images read from the electronic passport and obtained from the live camera are stored in a central database and archived for seven years. SmartGate has a comprehensive logging capability that can be applied at many levels as required.



Picture 3.11: The instructions on the gate are displayed on a LCD monitor opposite the passenger between the first and middle cameras



Picture 3.12: The gates at Melbourne International Airport

3.2.6 Provider

Australian Customs and Border Protection Service owns and operates SmartGate. Sagem Australasia is Customs strategic partner for the facial recognition component. An overarching agreement exists between Customs and Border Protection Service and Sagem Australasia which provides a framework for strategic partnership and development of contracts for specific work packages. The company was chosen through a public tender in 2006.

In 2005, the Australian Government provided funding for the first four years of the SmartGate Automated Border Processing Program for implementation at eight airports.

SmartGate is free of charge to users and there are no plans to introduce fees in the future.

3.2.7 Operators

SmartGate is managed by the Australian Customs and Border Protection Service as part of the border primary line. Customs and Border Protection Service airport staff perform basic maintenance of SmartGate including daily checks, restocking of tickets and incident management.

3.2.8 Conclusions

As of 17 January 2010, almost 1,060,000 travellers had used SmartGate across all airports since opening at Brisbane in August 2007 (with over 650,000 in the period from 1 July to end December 2009). As part of independent research conducted in October 2008 where 200 travellers were interviewed, out of those that used SmartGate, 98 percent agreed that SmartGate made the arrivals process easier, 97 percent agreed that they were extremely likely to recommend SmartGate to people they know and 96 per cent agreed that they were likely to use SmartGate again.

The performance and security of SmartGate is commensurate with requirements of Australian Customs and Border Protection Service.

4 Conclusions

This report describes two automated border crossing system based on biometric verification. In both cases electronic passports are used as the biometric data storage where facial recognition is the base for the biometric matching. The two factors – electronic passports and facial recognition – differentiate RAPID and SmartGate systems from 4 other automated biometric border crossing systems described in the first volume of the BIOPASS study (ABG, Iris, PEGASE and Privium).

4.1 *Electronic passports*

The use of the electronic passport as the data storage of personal data of travellers (including the biometric reference data) means that no additional biometric registration of travellers in the system is necessary. Both systems described in this report are open to all travellers having electronic passports and fulfilling certain basic requirements (citizenship, age etc.).

Although avoiding the need for the registration brings some benefits, they have to be balanced against certain drawbacks as well. The use of electronic passports instead of specific registration into the system means the automated border crossing system has lost control over the original registration of biometric data and the system must rely on the quality and accuracy of the data stored in the passport. Electronic passports offer methods to secure the authenticity of data and document. Requirements on quality of the biometric data stored in electronic passports are also in place.

The integrity/authenticity of the data stored in the passport must be verified by performing passive authentication. The cryptographic hashes of files read from the electronic passport are compared with the hashes stored in the Document Security Object (SOD) and the digital signature of the SOD made by the issuing institution is checked with the help of the Document Signer (DS) certificate attached. To guarantee the authenticity of the data, it is important to check also the signature of the Document Signer certificate with the help of the Country Signing Certification Authority key/certificate and check the DS certificate for possible revocation. This step requires the availability of the Country Signing Certification Authority (CSCA) certificate and a recent Certificate Revocation List (CRL) issued by the CSCA. Therefore, for each country whose citizens (passports) are accepted at the automated border crossing system the CSCA certificate must be obtained in a trustworthy manner (typically via diplomatic exchange). The diplomatic exchange needs to be done only initially. Later trust can be derived from the previous certificates (unless the CSCA key is compromised which would require repetition of the diplomatic exchange). Each CSCA must issue a CRL at least every 90 days. CRL files can be obtained directly by the CSCA (e.g. by downloading from a URL, but not all countries offer this method of CRL distribution) or via ICAO PKD. Again, not all countries issuing electronic passports are members of the ICAO PKD. In the summer of 2009, only 15 countries (Australia, Canada, Switzerland, China, France, Germany, India, Japan, Kazakhstan, New Zealand, Singapore, Nigeria, Korea, United Kingdom and USA) were members of the ICAO PKD.

The RAPID system accepts electronic passports issued by EU/EEA countries. At the time of writing, 27 CSCA certificates⁶ - European and third countries – were available in the RAPID validation component of electronic passport. At the European level, CSCA certificates and CRL files are obtained via bilateral exchange at the Article 6 Committee, however difficulties remain with third countries issuing electronic passports⁷.

The SmartGate system is open for citizens of Australia and New Zealand. CSCA certificates of both countries are available in the SmartGate system and CRLs are regularly downloaded from the ICAO PKD system. Availability of the CSCA certificate and participation of the passport issuing country in the ICAO PKD are basic requirements for the inclusion of a country in the SmartGate system.

As passive authentication cannot prevent cloning of electronic passports, optional active authentication can be implemented to increase security of the document. Both RAPID and SmartGate systems support an active authentication protocol and can check the authenticity of the document when implemented by the issuing country. Australian passports of the N series (issued since June 2009) implement active authentication.

European passports of the second generation implement an alternative protocol to validate their authenticity. At the moment, this chip authentication is not supported by any of the two automated border crossing systems described in the report.

All electronic passports store the facial image in the DG2 file in JPEG or JPG2000 bitmap format. The image can be a scanned photograph or an image from a digital camera (taken at the place of application for passport). Scanned images generally offer lower quality and may be flipped, retouched or replaced with a photo of a similar person. Although the requirements of ISO/IEC 19794-5 apply to all electronic passports, the resulting quality of biometric data in the form of facial images varies significantly from one country to another. Therefore, the biometric system relying on data read from electronic passports must be prepared to handle images of various sources and quality.

In addition to the JPG/JPEG2000 image, the DG2 file can code the position of certain features (e.g. eye centres). Only a few countries store additional feature points in their passports and the biometric software (SW) used at the described border crossing system does not take such information into account.

Biometric data in the form of fingerprint images, which is stored in the European passports of the second generation are not read and utilized in the current versions of the RAPID and SmartGate systems.

⁶ At the moment, Portuguese authorities are waiting for the answer from additional 37 countries.

⁷ Adhesion of Portugal to the ICAO PKD might solve the problem. Portugal intends to join the ICAO PKD in 2010.

4.2 Facial recognition

Recent NIST tests show that facial recognition algorithms can achieve fairly good accuracy [FRVT2006]. In practice it is, however, very difficult to tune the facial biometric system so that it is almost immune from false acceptances (e.g. FAR <0.001%) while the false rejection rate remains acceptable. The accuracy results for the SmartGate system are not publicly available, The RAPID system is configured to a threshold achieving a FRR of 4% at the cost of a FAR of 1% (numbers are dependent on methodology of the error rate calculation). The most difficult subjects from the point of view of false acceptances are twins and close relatives (as faces are genetically determined). Based on experience from the RAPID system, false rejects are typically caused by variances in backgrounds, poses, mimics, hair styles, glasses, hats, scarves or illumination.

To avoid spoofing with printed photographs of faces, a liveness testing must be in place. The details of liveness testing of facial biometric systems deployed at the RAPID and SmartGate are not publicly available. The Cognitec biometric algorithm usually bases the liveness testing on 3D properties of faces and looks at the rotation of the head which would not happen in the case of 2D photo.

4.3 Design of booths

The RAPID booth follows a straightforward design, where the traveller comes to a passport reader and when the passport is successfully read, the first door opens and passenger can be biometrically verified. When the traveller's face matches the photo in the passport, the second door opens and passenger can cross the border. The design is easily scalable and allows for an array of RAPID booths one next to another one.

The SmartGate design is based on a two-step process. At first the passport is read at a kiosk where the passenger answers several questions. At the kiosk a ticket is issued which is used at the gate for the biometric matching. The gates at the border are easily scalable. The kiosks can be located at various places including airports of departure, where travellers typically have enough time before boarding to pick up their tickets. The stop at the kiosk takes on average double the amount of time needed for crossing the border with a ticket, therefore the rule is to install two kiosks per each gate. Furthermore, a two-step process increases throughput and prevents bottlenecks.

Unicity detection is an important feature of the automated system. It makes sure only a single person can cross the border at a time. The system must be able to detect attempts to sneak in another person, no matter whether intentionally or not. In such cases the gate must not open the second door and the extra person must leave the gate. The unicity detection has to be able to distinguish extra persons from hand luggage and also detect small children. Particularly difficult situations are people holding small children in their arms.

Although the process of border crossing using the gates is described as completely automated, the human factor cannot be overlooked. Automated systems can solve the border crossing of low-risk passengers in trouble-free cases. If the person is not eligible to use the system, the passport cannot be read, or the biometrics do not match, human involvement is

necessary. In such cases the passenger cannot pass through the gate, he/she has to return back and head for a classical booth. Automated gates also need to be supervised by humans (typically border control officers) who make sure the rules are followed and the system is not subverted or attacked.

4.4 Data protection

The digital data read from electronic passports and acquired from the traveller during the border check can easily be logged. The storage of the data, however, must be in compliance with local legislation. In the EU, the relevant EU legislation must also be respected. The images of fingerprints obtained from the electronic passports can only be used for identity verification and then must be deleted.

4.5 Public acceptance

Surveys among users of the RAPID and SmartGate systems show that the public acceptance of both is good. Travellers indicate they would use the automated system again and would recommend using the system to their friends as well. Most of the travellers find the system easy to use and convenient. Public information campaigns and traveller education is key to positive public acceptance.

4.6 Future

Automated Border Crossing (ABC) systems will bring positive impact and benefits to the border control process. It will automatically verify the validity of the travel document and then will authorize the document's rightful holder to cross the border. It will also detect signs of falsification or counterfeiting. A biometric check provides enhanced confidence about the authenticity of the travel document. Furthermore, facial recognition can be as accurate (or better) as human verification⁸.

In the future, ABC systems will potentially have a positive impact on airport infrastructure as e-gates take up less space than traditional booths. It will enhance the overall traveller experience by providing faster waiting/processing times. Simplified and fast checks will be cost-effective, more predictable, convenient and user friendly. However, manual checks should always be possible.

Since ABC systems are being taken up and increasingly tested and used in the EU and other countries worldwide, it is important that countries exchange their experience and learn from each other through best practices and recommendations. Key requirements for ABC systems include: security i.e. verification of the authenticity of the travel documents and verification of identity, interoperability, convenience and public acceptance, broad coverage of travellers and cost-effectiveness. Furthermore, the system needs to comply with the rules concerning privacy and data protection.

⁸ Face Recognition Vendor Test, FRVT 2006. NIST

Due to the relative immaturity of the ABC systems and the limited number of operational implementations, further studies should be undertaken to assess the system vulnerabilities (its strength and weaknesses), to derive a set of performance metrics and to conduct a cost-effectiveness analysis. Furthermore, human factors and ergonomics of the systems should be studied well and their effect on efficiency and convenience.

5 **References**

[Alg07]“RAPID – Assessment of the Electronic Control System of the Board”, Presentation, University of Algarve, Department of Electrical Engineering and Informatics, 28 June 2007

[EAC111] Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents (BSI-TR 03110). Version 1.11. <http://www.bsi.bund.de/english/publications/techguidelines/tr03110/index.htm> Accessed Feb 4th, 2009.

[EC08a] MEMO/08/85, European Commission, 13 February 2008.

[EC08b] COM(2008) 69 Final, European Commission, 13 February 2008

[EF] H. Wang, Facial Recognition as a Pattern Recognition Problem, ECE 497NA, <http://www.roading.net/download/graphics/Facial%20Recognition%20as%20a%20Pattern%20Recognition%20Problem.ppt> Accessed June 5th, 2009.

[FaceRec] The overview of image-based and video-based face recognition algorithms. <http://www.face-rec.org/algorithms/> Accessed Feb 4th, 2009.

[FaceVACS] Cognitec: The technology of FaceVACS. <http://www.cognitec.com.br/downloads/pdf/FaceVACS algorithms.pdf> Accessed Feb 4th, 2009.

[FRO07]“BIOPASS – Study on Automated Biometric Border Crossing Systems for Registered Passengers at Four European Airports”, Frontex technical report No1/2007.

[FRVT2006] Face Recognition Vendor Test, FRVT 2006. NIST. <http://www.frvt.org/> Accessed Feb 4th, 2009.

[ICAO9303] International Civil Aviation Organisation, Doc 9303, Machine Readable Travel Documents. <http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx> Accessed Feb 4th, 2009.

[Liveness] G. Pan, Z. Wu and L. Sun. Liveness Detection for Face Recognition. Recent Advances in Face Recognition, Book edited by: Kresimir Delac, Mislav Grgic and Marian Stewart Bartlett, ISBN 978-953-7619-34-3, pp. 236, December 2008, I-Tech, Vienna, Austria <http://intechweb.org/downloadpdf.php?id=5896> Accessed Feb 4th, 2009.

[PRAGUE08] A. Ehre, M. Schlüter, Z. Říha and B. Hofbauer. ePassports EAC Conformity & Interoperability Tests. Results. Prague. September 2008. http://www.e-passports2008.org/download/E-passports_Prague-TestResults_Web_080922.pdf Accessed Feb 4th, 2009.

Annex 1: Acronyms and abbreviations

CA	Certification Authority
CCTV	Closed Circuit Television
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
CRL	Certificate Revocation List
DG	Data Group
DS	Document Signer
DV	Document Verifier
EAC	Extended Access Control
EC	European Commission
EEA	European Economic Area
EU	European Union
FAO	airport code for Faro
FAR	False Acceptance Rate
FRR	False Rejection Rate
FLD	Fisher's Linear Discriminant
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IR	infrared
IS	Inspection System
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
LDA	Linear Discriminant Analysis
LIS	airport code for Lisbon
LKD	Local Key Directory
MRZ	Machine Readable Zone
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
PCA	Principle Component Analysis
PKD	Public Key Directory
PKI	Public Key Infrastructure
RAPID	Automatic Recognizing of Passengers with Credentials
RF	Radio Frequency
SCV	Special Category Visa
SOD	Document Security Object
SEF	Border and Immigration Service of Portugal
SW	Software
TA	Terminal Authentication
UK	United Kingdom of Great Britain and Northern Ireland
URL	Uniform Resource Locator
UV	Ultraviolet
WSQ	Wavelet Scalar Quantisation

Annex 2: Biometric airport control survey

The airport

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 with supervision
- ☐ Automated with supervision
- ☐ Human assisted

Maturity of the system:

- ☐ Trial
- ☐ Final

Since when:

History of the system:

How many people use the airport?

	Average	Minimum	Maximum
Day			
Month			
Year			

Percentage of passengers who are border-controlled:

How many people use the biometric system?

	Average	Minimum	Maximum
Day			
Month			
Year			

The users

For whom is the biometric authentication designed:

☐ Staff

If staff then:

☐ All staff

☐ Selected staff

If staff then for relevant people

☐ Enrollment and use mandatory

☐ Enrollment mandatory, but use only optional

☐ Enrollment optional, but if enrolled then use mandatory

☐ Enrollment optional, use optional

☐ Passengers

If passenger then:

☐ All passengers

☐ Passengers not requiring the visa

☐ Only passengers from the following countries

☐ Closed only for a selected group of people. Please specify:.....

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:

Camera/reader manufacturer type:

All readers the same?

☐ No

☐ No, describe:

Everywhere the same SW used?

☐ Yes

☐ No, describe:

Integrator:

Enrollment (if relevant)

How many and which finger/eyes enrolled:.....

What documents are necessary for enrollment?.....

What data is required at enrolment?.....
How long does the enrollment 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 enroll a person if there are problems?
What is the FTE (fail to enroll) rate?
Is the enrollment 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 enrollment SW verify the person has not already been enrolled (as someone else)?

Passports

Passport accepted for automated system:

- ☐ Non-electronic with MRZ
- ☐ Electronic without BAC
- ☐ Electronic with BAC
- ☐ Electronic with EAC

Support of security features:

- ☐ Passive authentication performed
- ☐ Active authentication performed
- ☐ Chip Authentication (as a part of EAC) performed
- ☐ SW is ready for Terminal Authentication (as a part of EAC)

Public Key Infrastructure:

- ☐ System is connected to ICAO PKD
- ☐ System requires DS certificates to be stored in ePassport's EF.SOD file
- ☐ CSCA certificates bilaterally exchanged with the following countries

How do you handle situations when the CSCA certificate of a country is not available?.....
Do you have any experience with a fake of the electronic part of the passport?.....

Do you have problems with reading of passports of certain countries?.....
Do you have any statistics on readability or speed of reading of ePassports?.....
What are you experience with OCR of the MRZ (to run the BAC)?.....

Biometric 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?
Typical causes of false rejections.

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 / data privacy

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?.....
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?

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.... ..

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?