Frontex Perspectives on Biometrics for Border Checks

Erik Berglund, Rasa Karbauskaite

Frontex
Rondo ONZ 1
00-124 Warsaw
Poland
erik.berglund@frontex.europa.eu
rasa.karbauskaite@frontex.europa.eu

Abstract: The European Union is developing new concepts for border management. Biometrics is seen is a key technology to facilitate more secure and convenient border management. Biometric information in the form of the facial image is already stored in the electronic passports, and from 2009 fingerprints will also be stored. Also from 2009, biometrics will be introduced in the Visa Information System (VIS). The VIS will store facial images and fingerprints of all visa applicants and a check against the stored data will be performed at the border crossing. The use of biometrics makes the concept of automated border crossing feasible. Frontex has studied such systems and found them to perform well. There are, however, several design issues that need to be addressed to make the systems more user friendly.

1 Background

The European Union (EU) has a combined population close to 500 million and about a third of the global GDP. The Union has gradually developed along the lines of the fundamental ideas of freedom of movement of people, goods, services and capital. To facilitate the free movement of people, the Schengen Agreement of 1985 has created open borders without passport controls between those states adopting it. Today, most EU member states and some non-member states have adopted the Schengen Agreement, which, after its integration into European Law, is referred to as the “Schengen acquis” [EC06].

The EU external borders are annually crossed by about 300 million people – 160 million EU citizens, 60 million third country nationals not requiring visa, and 80 million third country nationals requiring visa [EC08a]. To facilitate these large flows while keeping a high level of security requires efficient border management. The EU border management policy aims to strike a balance between on the one hand promoting movement of people and goods, and enabling cross-border collaboration, and on the other hand providing a high level of security.

In the conclusions of the Justice and Home Affairs ministerial meeting of 4-5 December 2006, the Council of the EU adopted the concept of Integrated Border Management. This concept consists of the following dimensions:

- border control (checks and surveillance) as defined in the Schengen Borders Code, including relevant risk analysis and crime intelligence;
- detection and investigation of cross border crime in coordination with all competent law enforcement authorities;
- the four-tier access control model (measures in third countries, cooperation with neighbouring countries, border control, and control measures within the area of free movement, including return);
- inter-agency cooperation for border management (border guards, customs, police, national security and other relevant authorities) and international cooperation;
- coordination and coherence of the activities of Member States, institutions and other bodies of the Community and the Union.

The abolishment of the internal borders of the European Union has underlined the need for the Member States to collaborate in managing the external borders. As a part of the Integrated Border Management policy, Frontex has been created as a European agency tasked to coordinate such collaboration.

While there is an increasing coordination at a European level, border control remains the responsibility of the Member States. However, the Schengen Borders Code [EC06] and the Schengen Handbook give detailed regulations for border checks and border surveillance along all external borders of the states that apply the Schengen acquis. At present it is applied by all EU Member States with the exception of the UK and Ireland. Furthermore, Norway and Iceland apply the regulation despite not being EU members.

The regulation lays down, amongst other things, the requirements for entry and exit control. However, it is important to underline that these requirements were written at a time when biometrics was not a common good as it is today. This means that up to now all developments related to the use of biometrics for border control have to comply with the existing legal framework (Schengen acquis).

2 EU initiatives on the use of biometrics

The European Commission has recently launched an initiative to prepare the next steps in border management [EC08b]. This vision of the future relies to a large extent on technology to improve security, convenience and cost-effectiveness. A key enabler is the use of biometrics in travel documents.

Electronic passports using biometrics have already been introduced. Since 2006, EU passports have been issued with the facial image stored in a chip and from 2009 fingerprints will also be included [EC04]. Germany has already started issuing second generation passports with fingerprints, while the other EU states are preparing themselves.

Starting from 2009, also visa for foreign citizens will use biometrics. As part of the application process, a facial image and the ten fingerprints will be captured and stored in the Visa Information System (VIS). Both biometric features can subsequently be used for verification purposes, e.g. at the border.

The VIS gives the border control officers a powerful tool for border checks. Not only will the border guards be able to check the reason the visa has been issued and verify that against the declaration of the person standing in front of them, but they will also be able to check whether the person standing in front of them actually is the one the visa was issued to. Additionally, inside the EU states, the VIS will make it easier to identify persons lacking documents and not willing to cooperate, facilitating the detection of so called “overstayers”.

The regulation on the Visa Information System (VIS) and the exchange of data between Member States on short stay-visa will be formally adopted in 2008. The regulation covers the exchange of data between the states that apply the Schengen acquis on applications for short stay-visa and on the decision taken thereto. The goal of this exchange of data is to facilitate the examination of such applications and the related decisions, to prevent so called visa shopping, to facilitate the fight against fraud, to facilitate the checks at the external border and within the territories of the Member States, to assist in the identification of persons, and to prevent threats to the internal security of any of the Member States.

The new ideas raised by the Commission [EC08b] are mainly on facilitation of border crossing for *bona fide* travellers through automated border checks, and on the introduction of an entry/exit system to register those entering and exiting the Union. Automated border crossing could be made available to EU citizens and to third country nationals who have been awarded the status as “Registered Travellers”. An entry/exit system could become operational by 2015.

As the mentioned systems will handle large amounts of personal data, data protection is one of the main concerns expressed by the Commission. The systems must, of course, comply with all rules on data protection. The data stored in the VIS will be automatically deleted after 5 years. Sharing these data with others (more concretely with other states or international organisations) is forbidden, the only exception being if certain data are needed to prove the identity of a third country national in relation to returns.

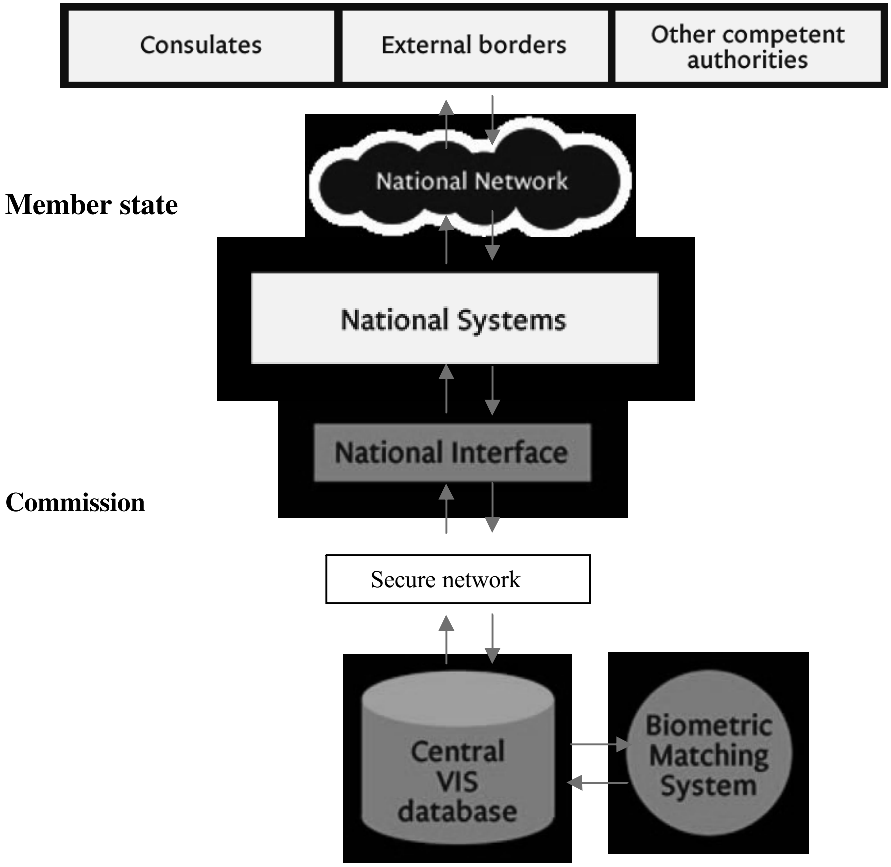

Figure 1: The VIS covers Member State authorities in third countries as well as in the Member States, and the central parts that are operated by the Commission. The central part of this system will become operational in 2009, while the system is to be fully operational at all sites by 2012.

3 Biometrics for border checks

Biometric information has traditionally been used at border checks in the form of a photo in the passport. In the digital age, biographic information is not only printed in passports, but also stored in digital form in a chip.

The international standard for electronic passports has been developed by the International Civil Aviation Organization (ICAO). The ICAO standard [ICAO06] recommends face as the primary biometric for inclusion in machine readable travel documents, while finger and iris are recommended as secondary biometrics.

The choice of face as the primary biometrics is natural, as it offers an automatic compatibility with the classical border checks and as it is commonly accepted to use facial images to verify peoples' identities. However, the accuracy of facial recognition systems has traditionally been behind the top biometric modalities like fingerprints and iris. Recent tests [NIST07], however, show that the latest facial recognition algorithms are nearly as good as its traditional rivals. Furthermore, the tests included comparisons with trained humans, where the algorithms performed better than the humans. Most difficult subjects from the point of view of false acceptances are twins and 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 illumination.

4 Frontex studies on automated border crossing

The use of electronic travel documents based on biometrics facilitates the introduction of automation. Automation offers possibilities to make border crossings more convenient and secure as well as more efficient. To evaluate the concept of automated border crossing, Frontex has studied different systems. The first 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. A subsequent study [FRO08] has covered the Portuguese RAPID and the Australian SmartGate, both using facial recognition. All systems are fully working and enable the passengers to cross the border in a convenient way.

The system at Charles de Gaulle is based on fingerprints, while the systems at Schiphol, Frankfurt and Heathrow are based on iris. The study [FRO07] shows that biometric technologies are mature and usable, with false rejection rates of a few percents. The encountered problems do not concern the biometrics, but rather the practical design of the checkpoints and the human-machine interfaces. However, all four systems require specific registration and offer no interoperability.

4.1 RAPID system

The RAPID project – Automatic Recognizing 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 the costs. The RAPID system is based on facial recognition and allows automated border crossing of passengers holding EU electronic passports. This is the first system in Europe to allow automatic border checks of passengers with electronic passports.

The system started as a pilot project with ten booths at Faro airport in May-June 2007 and after the evaluation conducted by the University of Algarve [Alg07] it became operational. Since August 2007, the RAPID system has become operational at Lisbon airport and the plans cover the employment of RAPID at all Portuguese international airports and ports.

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.

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 ten gates.

An important performance parameter indicating the provided security of an automated border crossing system is the False Acceptance Rate (FAR). The usual way of calculating the 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 test data from real field use. The results showed a zero-effort FAR of 0.03%.

The study of the Algarve University took a more realistic approach trying to match people with similar looks. It is natural that their success rate was higher. The FAR for the 448 pairs of similar people that could be found amongst the passing travellers turned out to be 1.3%. This trial confirmed that for facial biometric systems the most difficult subjects to distinguish between are close relatives like siblings or parents and children.

Another important performance parameter indicating the provided convenience is the False Rejection Rate (FRR). According to Vision Box, the supplier, the theoretical FRR at the chosen performance level is 4,25:‖ . The study of the Algarve University reports the FRR as 5,2:‖ . However, after the study, the design of the light source has been improved, which has lowered the FRR.

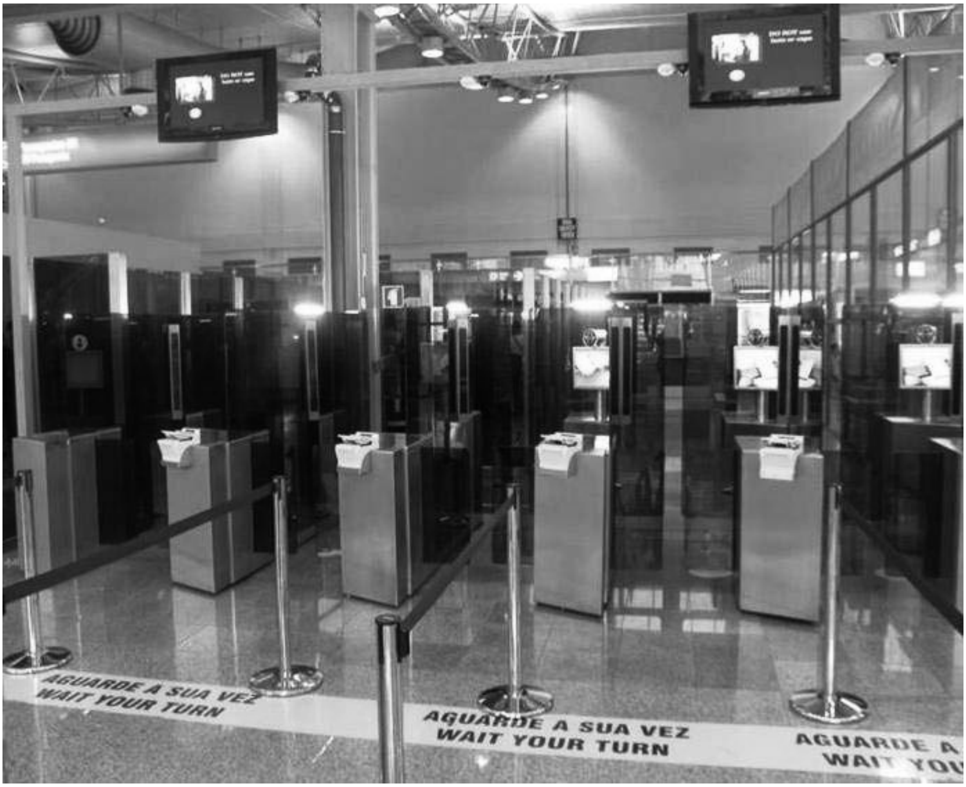

Figure 2: The RAPID gates at Faro Airport.

The performance of the system, in particular the false rejection rate and the time to reach a satisfactory match, depends to a large extent on the quality of the facial image stored in the passport. This quality varies and not all passports fulfil the ICAO requirements on background, pose or size of the head etc. Furthermore, some countries, e.g. the UK, allow passport applicants to bring photographs that are scanned, which can result in outdated low-quality images being stored in the passport

Furthermore, many travellers experience problems with the man-machine interfaces. These problems include how to enter the passport into the reader and where to stand. Further refinements of signs and instructions are likely to reduce these problems.

As could be expected, 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. However, RAPID has verified that facial recognition is good enough for border checks. Furthermore, a major advantage of the RAPID system is that it uses the standard electronic passport and consequently offers interoperability with other manned and automatic systems.

4.2 SmartGate system

Smartgate is an automated border processing system being introduced by the Australian Customs Service. It has been in operation at Brisbane Airport since the conduct of a public trial in August 2007. The trial showed that the face technology worked as expected, that the traveller experience was extremely positive, and that the impact on the further business processes was minimal. Of the 200 travellers who were interviewed as part of the traveller experience assessment: 86% rated the solution ‘easy to use’; 99% would use it again; 98% would recommend it to people they know; and 93% of previous overseas travellers felt it made the arrivals experience better.

The use of SmartGate is currently limited to Australians and New Zealanders with ICAO compliant electronic passports. However, the system will gradually be opened for other nationalities.

5 Conclusions

The European Union is developing new concepts for border management, where technology will play an increasing role. Biometrics is seen as a key technology to facilitate more secure and convenient border management. Key requirements for biometrics in border check applications include: security, i.e. verification of the authenticity of the travel documents and verification of identity; convenience and public acceptance; broad coverage of travellers from the EU and elsewhere; interoperability; and cost-effectiveness. Furthermore, the systems need to comply with the rules concerning privacy and data protection.

The studied systems for automated border crossing prove the concept of using automation based on biometrics for this application. Furthermore, the overwhelming results from the user satisfaction surveys indicate that the public is more than ready to accept automated processes for border crossing.

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.

[EC04] Council Regulation (EC) 2250/2004.

[EC06] Council Regulation (EC) 562/2006.

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

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

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

[FRO08] "Automated Border Crossing Based on E-passports and Facial Recognition", Frontex technical report to be published.

[ICAO06] "Machine Readable Travel Documents", Doc 9303, Part 1, Volume 2, ICAO, 2006.

[NIST07] "FRVT 2006 and ICE 2006 – Large-Scale Results", NISTIR 7408, National Institute of Standards and Technology, March 2007.