EasyPASS - Evaluation of face recognition performance in an operational automated border control system

Markus Nuppeney[1] · Marco Breitenstein[2]

[1]Federal Office for Information Security (BSI)
markus.nuppeney@bsi.bund.de

[2]secunet Security Networks AG
marco.breitenstein@secunet.com

1. Introduction

The technical specifications [ICAO9303-1] [ICAO9303-2] for machine readable electronic passports (ePassports) have been approved by the International Civil Aviation Organization (ICAO) in 2006. More than 60 countries worldwide are meanwhile issuing ePassports according to the ICAO standards equipped with biometric facial images, which are stored in an embedded RF chip. With respect to border control processes, the usage of these ePassports generally allows for benefits regarding the following aspects:

1. Improved security
   - electronic security mechanisms prevent forgery
   - biometrics prevent misuse of real documents by unauthorized persons
2. Increased throughput
   - by using automated checking routines in classical control environments
   - by deploying automated border control systems, so-called eGates (electronic Gates)
3. Ease of use
   - for the holder of the ePassport (self-service scenarios / eGates)
   - for the border control officer (more time for critical cases)

Several countries have already implemented automated border control systems based on ePassports and facial recognition. Smartgate (Australia), RAPID (Portugal) and eBorders (United Kingdom) are currently the most prominent programs or projects in this area.

Besides various operational aspects, there are also crucial technical questions to be considered regarding the biometric performance when introducing eGates and facial recognition at the borders:

1. Is the quality of the ePassport images good enough to recognize people at an adequate level, i.e. are the images good enough to use them for automated facial recognition in a comfortable, reliable and secure manner?
2. If so, is this true for the ePassports of all nations or just for a sub-set of countries spending high effort on quality assurance during the capture process of the facial images resp. photographs?

To answer these questions the German government started the project EasyPASS to deploy an automated border control system at Frankfurt Airport based on facial recognition using the images from ePassports.

Main characteristics and goals of the EasyPASS project are:

- A balancing act between running face recognition systems in a real operational environment at the largest German airport and at the same time operating the systems in a way that allows well-founded biometric performance evaluation.
- Performing an operational evaluation showing the performance as perceived by both passengers and border guards.
- Performing a technical evaluation to be able to assess the biometric performance over the whole operating range.
- Using several face recognition algorithms at the same time and under the same conditions to be able to compare their performance.
- Using several quality assurance algorithms at the same time to evaluate the quality of the face images stored on the ePassports from the particular countries.
- Operating the whole system in a secure way beside the biometric verification. That means complete checking of the documents' optical and electronic security features as well as background checks.
- Using the eGate systems in a self-service mode from the passengers' point of view.
- Possibility to cut off the evaluation functionality to convey the entire system to real operation mode (without extensive evaluation) when the evaluation phase of the project is over.

2. EasyPASS system architecture

In terms of hardware the EasyPASS system is characterized as follows (see Figures 1 and 2):

- Each eGate comes with an entry and an exit door.
- On the right side of the entry door each eGate is equipped with a full-page document reader to perform the optical ePassport checks and to read-out the electronic data from the chip.
- To capture live images of the travellers, an intelligent self-adjusting camera system is embedded into the exit door of each eGate.

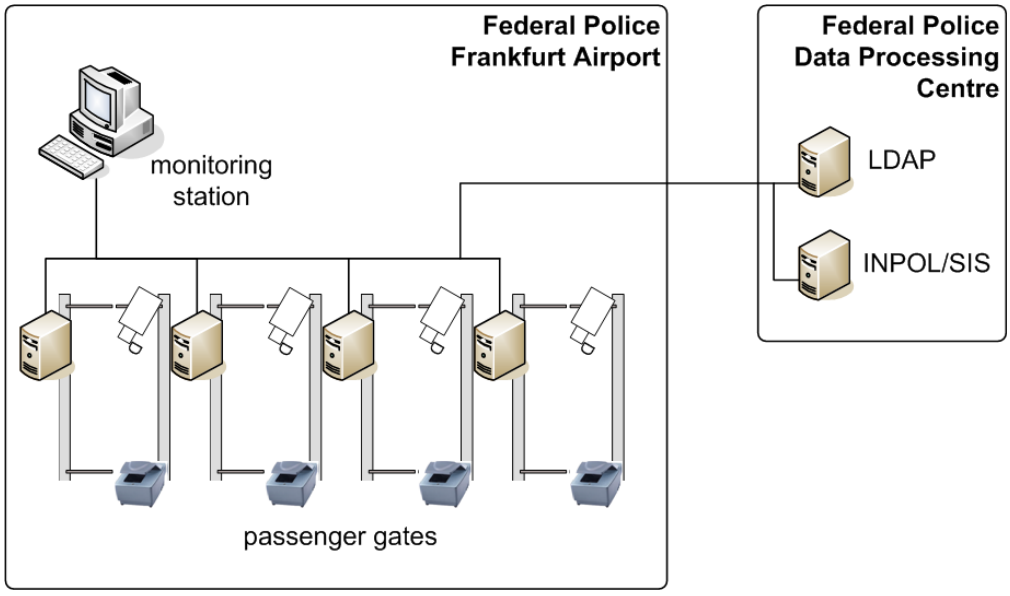

Figure 1: EasyPASS system overview

Figure 2: EasyPASS hardware setup - four operating eGates in parallel

The entire software architecture of EasyPASS is based on the integration platform BioMiddle. BioMiddle facilitates the modular use of biometric system components and document readers within different biometric applications. Standardised interfaces allow for easy replacement of individual components. In particular, biometric hardware and software components are used as encapsulated Biometric Service Providers (BSP) and integrated via an integrated BioAPI 2.0 framework according to the corresponding ISO/IEC standard [ISO19784-1]. The development of the BioMiddle framework was initiated in 2005 by the German Federal Office for Information Security (BSI) in order to be deployed in governmental biometric applications to guarantee modularity and exchangeability.

An overview of the EasyPASS software architecture is shown below (see Figure 3).

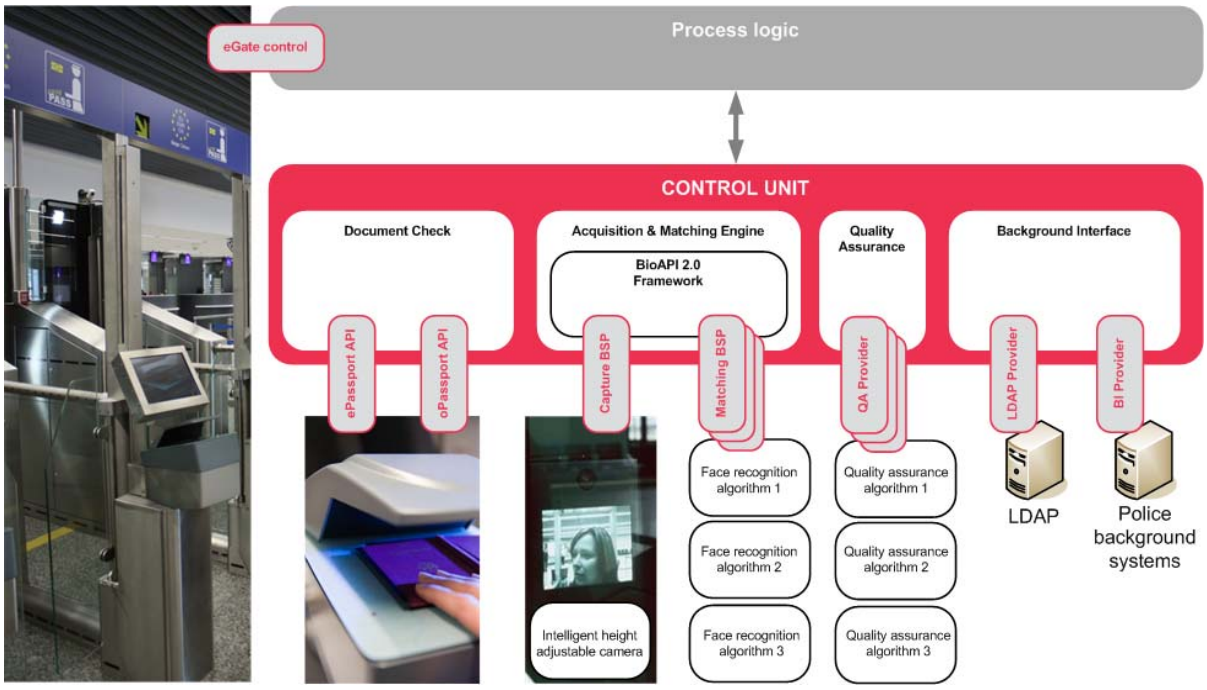

Figure 3: EasyPASS software architecture based on BioMiddle

3. Project schedule

The schedule of the project consists of three main phases:

Phase 0 (Aug. – Sept. 2009):
The system has been operated in "Biometric Data Collection Mode" in order to set up a database of facial images (passport-images and live-images) as the basis for performing the biometric performance evaluation. During "Phase 0" all participating passengers had to sign a declaration of consent regarding the storage of their facial images.

Phase 1 (Oct. 2009 – March 2010):
Since the beginning of October the system is running in "Evaluation Mode", i.e. each passage of the EasyPASS eGates is logged in detail (timestamps, biometric quality characteristics, biometric scores etc.) but the personal and biometric data of the passengers is not stored in a database. From the passengers' point of view the system operates like in "Regular Mode".

Phase 2 (from April 2010):
At the change-over from "Evaluation Mode" to "Regular Mode" it is intended to cut off the evaluation functionality to convey the entire system to regular operation mode (without extensive evaluation). The parameterization of the system for "Phase 2" (biometric point of operation, employed biometric algorithm(s), etc.) depends on the evaluation results from "Phase 1".

4. Test setup and evaluation methodology

The EasyPASS environment is equipped with extensive evaluation mechanisms. This covers mainly the following aspects:

- Logging of events and results in particular to estimate rejection rates regarding
  - Face recognition (comparison scores instead of a simple decision)
  - Electronic security validation
  - Optical security validation
  - Background checks
  - Time measurements

- Calculation of comparison scores with respect to
  - Multiple biometric algorithms (three different state-of-the-art face recognition algorithms are in use)
  - Calculation of comparison scores for genuines (live image of the passenger against the electronic ePassport image)
  - Calculation of comparison scores for simulated imposters (live image of the passenger against ePassports images of different persons stored in the evaluation database).

  This approach enables the calculation of all possible points of operation regarding FRR and FAR for each algorithm within in the real operational environment.

- Performing quality measurements with respect to [ISO19794-5] of the ePassport images using multiple quality assurance algorithms (three different state-of-the-art algorithms are deployed within the system)

All the biometric measurements and evaluations are performed online because of data protection considerations. The mentioned evaluations allow for a profound analysis of the system performance in sense of ROC curves, quality distributions, timing consideration etc. Based on these results the questions stated above can be addressed and answered in detail.

5. Prospect

The very first preliminary evaluation results are really promising. The EasyPASS system is operating in a manner that exceeds the expectations. This covers the performance shown by first analysis, the feedback of the border guards and above all the extremely positive feedback of the passengers. Established and detailed results will be available from April 2010 on, when the evaluation of the project ("Phase 1") is finished.

References

[ICAO9303-1] ICAO Doc 9303, Machine Readable Travel Documents – Part1, Volume1: Passports with Machine Readable Data Stored in Optical Character Recognition Format, Sixth Edition, 2006.

[ICAO9303-2] ICAO Doc 9303, Machine Readable Travel Documents – Part1, Volume2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition, 2006.

[ISO19784-1] ISO/IEC 19784-1, Biometric application programming interface – Part1: BioAPI specification.

[ISO19794-5] ISO/IEC 19794-5, Information technology – Biometric data interchange formats – Part5: Face image data.