COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 – Consensus building, experience sharing
on internet evolution and security

ICT PSP call identifier:	ICT PSP 2nd call for proposals 2008
ICT PSP Theme/objective identifier:	3.2 Trusted information infrastructures and biometric technologies
Project acronym:	**BEST Network**
Project full title:	**Biometrics European Stakeholder Network**
Grant agreement no.:	**238955**

Deliverable D6.2

Mapping Selected Applications Scenarios to their Respective Standards and Evaluation Schemes

FINAL (vs 1.0)

Classification: —

Dissemination level: PU

Date of submission: March15th, 2012

Table of Content

1 Introduction

As biometrics become more ubiquitous the number of people using specific biometric-based applications continues to surge. Biometrics have been pioneered in government applications, before being more widely accepted for enterprise use, and are now emerging in the retail space. The many different and varied application scenarios have been studied in detail within the BEST Network and presented in the earlier deliverables [1, 2, 3, 4].

In this document two key applications have been selected: the e-passport enrollment process and Automated Border Control (ABC) systems at airports. The reason for this choice is that these two scenarios are currently the only ones for which testing, evaluation and certification is of crucial importance at this very moment because of the large scale of their roll outs. For each one, the relevant standards and evaluation schemes, which may be applied within the context of that scenario, are investigated. These testing schemes and standards stretch from conformance, to performance, to usability, and beyond.

A number of other popular application scenarios were excluded from this study, as they were found to be unsuitable for detailed analysis. Such scenarios included new emerging applications, closed proprietary biometric systems, or those lacking sufficient application requirements.

The application scenarios selected for investigation include the passport enrolment process, automated border crossing (ABC) systems and border control equipment. The passport enrolment process paves the way for every European citizen to obtain a biometric e-passport, and thus has an unprecedented scale. Once issued, these e-passports may be used to pass smoothly through airport electronic gates, in an automated border crossing system. For those not passing through electronic gates, they may encounter other border control equipment used to capture biometric data, confirm identity, and perform background checks.

For each selected application the scenario is described and evaluation objectives (including quality, interoperability, and security) are compiled. A survey is then performed of relevant available standards and existing testing and certification schemes for that specific scenario.

It was found that, within a European context, the development of a number of new standards or evaluation schemes, could be recommended in order to stimulate wider acceptance of the application. On the other hand, it can generally be concluded that uniform testing and evaluation of biometric components and systems in Europe still have way ahead:

- The requirements and specifications of the two selected scenarios are not uniformly and sufficiently defined across Europe, making them a moving target for testing and evaluation.
- Some basic characteristics of biometric testing make it difficult to develop common testing, evaluation and certification schemes and tools.
- There are security issues regarding the biometric capturing process during the passport application process, which might be transported to ABC system that are based on that passport.
- For both scenarios counts that testing and certification will increase the overall level of trust and performance

References:

[1] BEST Network D1.1 “Inventory of biometrics enabled registration processes for immigration purposes”, July 2010

[2] BEST Network D2.1 “Survey of existing and emerging commercial biometric applications”, September 2010

[3] BEST Network D3.1 “Inventory of best practices biometrics at airports”, February 2010

[4] BEST Network D4.1 “State of Art: Biometrics in eID systems”, April 2010

2 Passport Enrolment Process

The most relevant biometrics roll out currently without any doubt is the installation of the enrolment procedures as part of the passport application process. The innovative aspect of it is that the data subjects form an open group of participants at an unprecendented scale. At the same time the enrolment process is the very basis of any national identity scheme, which puts a large burden on the quality and integrity of that process. Until now we have learned that many issues with respect to the processes and procedures, as well as the validation and certification of the used biometric technologies leave some significant gaps on both national as European level. In order to improve the reliability and integrity of any subsequent usage of the biometric verifiers for border control purposes (such as ABC), the enrolment process is of crucial importance. The level of quality and integrity of the enrolment process has a direct impact on citizens because of different standards, requirements, quality, availability of and usability of e-passports and ABC.

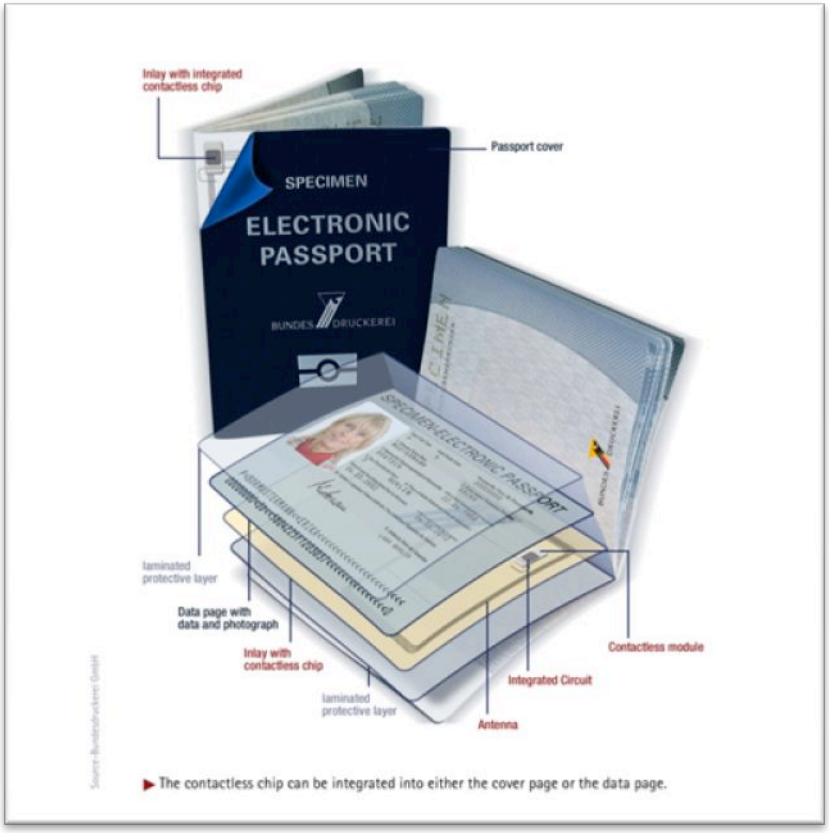
Without European harmonization on these issues second class passengers will be those whose travel documents (issued by some of the EU27) not only do not meet the 2019 standards of two 'old' biometric data sets in principle, but also fail to meet quality requirements thereby forcing the passenger into the manual checking lane or maybe even into lengthy fall back procedures. Educating them about the advantages of ABC will cause greater frustration, once the biometric verification process has proven unreliable. The administrative differences in renewing stolen passports between different member states already effectively deprive some citizens of their right to cross border mobility as it takes so long to get a travel document renewed or replaced. This is about more than trust in the technology, or its cost.

The overall effect could be to erode public trust in the ICTs (and biometrics in particular) and in the agencies responsible for border controls and migration issues.

2.1 Application description

2.1.1 EU e-passports

Passports are identity documents, issued by a national government, which are used to prove identity and citizenship while travelling across country borders. The last decade has seen the introduction of machine readable passports containing biometric identifiers stored on a contactless smart chip (e-passports) by approximately seventy countries.



Specimen: e-passport (source: BundesDruckerei)

Within Europe, there has been legislation [1] which specifies which biometric identifiers should be enrolled and stored within EU e-passports. These requirements are based on the ICAO recommendations for Machine Readable Travel Documents (MRTD) [2,3]. The first generation e-passport contains a digital face photo of the owner. Second generation e-passports require two index fingerprint images in addition to the face image. Iris images may also optionally be included, but typically have not been used to date. There is no current EU legislation specifying how biometric e-passports should later be used for verification at a border control.

Within Europe a new e-passport is usually issued when an old legacy passport has expired. Each Member State is responsible for enrolling and issuing its citizens with e-passports, and deciding whether to maintain a central national database of the captured biometrics. There is no central EU database for all issued e-passport data.

Within the EU both 1st generation (face only) and 2nd generation (face & 2-fingers) e-passports are currently being issued. The enrolment process varies largely across Member States. These variations are due in part to the different:

- Enrolment environment
- Capture devices
- Device ergonomics
- Biometrics captured
- Quality of the biometrics
- Biometric algorithms employed
- Feedback provided to the citizen or operator
- Conformance testing
- Verification of the biometrics

For example, in some Member States it is sufficient to submit a face photo which has been captured in a public photograph booth or at home. Some citizens even edit these photos, to remove blemishes, before submitting them. In other States the citizen must present themselves to an enrolment office in order to allow both fingerprints and face biometrics to be captured. As there is no specification of the minimum quality to be stored on the chip of the passport, there is a large variety of the quality of the stored biometric data. This includes both the facial image as the fingerprint images. In addition to these discrepanties there is no international unified standard that can determine if the image quality is high or low.

2.1.2 Enrolment verification

The quality of the captured biometrics are tested during enrolment in order to estimate if they will be suitable for later use at a border control. In some cases a verification comparison may also be made with these samples.

The verification may be performed against additional biometric presentations captured during the same visit. For example, if two or more multi-presentation captures of the same biometric are performed, then a comparison between these may be made to ensure matching is feasible. Captures may be separated by other tasks during the enrolment session to help confirm that sufficient quality can be obtained repeatedly.

As e-passports expire, after five or ten years depending on Member State, a renewal process will be performed. This will involve capturing and enrolling a new set of biometric identifiers from the holder, in order to allow for changes to the biometrics that may have occurred over the life of the e-passport, such as caused by aging or damage. At re-enrolment the issuing country may wish to verify that the newly enrolled biometrics correspond to the biometrics on the expired e-passport, and a verification could be performed between these two sets. In cases where Member States do not maintain a central record of the issued biometrics, the expired e-passport would be required in order to obtain these.

E-passports are usually issued and delivered to the holder's home address at a later date. However, one scenario might allow the e-passport to be collected in-person and a biometric verification against the issued e-passport could also be performed at that time, although the primary purpose would be to prove the identity of the person collecting the e-passport rather than checking the quality of the enrolled biometrics which would already have been issued onto the document.

2.1.3 Identification search

Furthermore, in some enrolment scenarios, it is desirable to perform a 1:n biometric identification search against a database of enrolled biometrics. This can be for de-duplication or law enforcement purposes. The choice for such identification facility, which requires central storage of the biometric data of all citizens, depends on national legislation and is not regulated at a European level. This 1:n identification can be done against the entire enrolled e-passport population in order to prevent duplicate e-passports being issued for a single individual by a single Member State. While there is no central EU database for this purpose, some Member States do store all biometrics captured. Alternatively identification may be performed against a smaller set of individuals that have been added to a watch list. In addition, depending on the population size and accuracy required, it may be necessary to enroll additional biometrics beyond those required for issuance on the e-passport itself. For example, ten fingerprints or two iris images might be captured in order to allow a more accurate identification search.

After the biometric images have been captured, formatted, and deemed to be of sufficient quality for enrolment, they are written securely onto the e-passport chip. The face image is protected on the e-passport by the ICAO Basic Access Control (BAC) mechanism. The fingerprint data is protected by a more sophisticated ICAO Extended Access Control (EAC) scheme where Member States can control which other countries have access to the data through the use of cryptographic keys.

2.2 Evaluation objectives

The goal of the e-passport enrolment process is to collect genuine biographic and biometric data from an individual and issue an e-passport that can later be used to prove identity at a border control. The process should ensure that the captured biometrics are suitable for later use at a border control post. However, suitability will depend on how the biometrics will be utilized at the border.

It is noted that there are no current standards specifying how biometric e-passports be used for verification at a border control. However, it is expected that they will be used to perform some form of one-to-one verification, by comparing the e-passport enrolled biometrics against biometrics captured from the holder at the border. The verification capture could be performed manually by an operator or in an automated fashion. The application scenario using ABC gates, described in an earlier section, is an example where the enrolled biometrics will be utilized.

If one-to-N identification is to be performed against a watchlist or other population subset, then the biometrics may need to be of better quality than those used for simpler 1:1 verification. In either verification or identification scenarios, the quality and correctness of the captured biometrics will impact the accuracy attainable.

Based on the potential use of the biometrics at the border the e-passport process needs to be evaluated to ensure that the biometrics:

- are of sufficient quality to be usable for all of the envisioned border control scenarios (quality)
- are usable at the border of any country enabled to process e-passports (interoperability)
- originate from the correct identity enrolled (security)

The evaluation objectives for these areas of quality, interoperability, and security are now examined in turn.

2.2.1 Quality

E-passport biometrics need to be of sufficient quality and yield sufficient accuracy to be usable for all the envisioned border control applications. For EU passport holders this will involve the use of face and/or two fingerprints. For example, the face needs to be captured to a standard that is of sufficient quality to use for automated facial recognition in a reliable, accurate, and secure manner.

The quality of the biometrics and their suitability for biometric matching will depend on the quality assurance processes at e-passport enrolment. There are several components of the quality assurance processes which will need to be evaluated, beyond a simple biometric quality algorithm score. The components to be evaluated should include:

- Environment control
- Information and guidance material for enrolees
- Operator training
- Capture devices
- Ergonomics
- Capture protocol, including number of attempts & data selection from those attempts
- Capture feedback
- Quality algorithms and thresholds
- Handling of modality-specific factors
- Verification test (see earlier section)
- Conformance to e-passport biometric data standards (see next section)

There has already been some work to evaluate some of these components for generic applications. For example, in EU BEST D6.1 [5], schemes to certify capture devices, or white lists, are described. A white list of biometric devices is a list of accepted products, which have been tested and analyzed by a certification organization, confirming that the product is acceptable according to established criteria. A white-list for biometric capture devices for EU e-passports would be very helpful for EU countries to select suitable enrolment equipment from the large choice available.

Currently there are many different practices and choices for the e-passport capture protocol. For example, with data selection sometimes the best image according to a proprietary quality algorithm is selected. In other cases a composite record based on data from multiple captures may be used. While some guidelines have been formulated for electronic visa biometric capture, the e-passport enrolment process would also benefit from European-wide guidelines and evaluation in this area.

The quality evaluation process will have some modality specific parts, since different factors are known to affect biometric performance for different modalities [6].

2.2.2 Interoperability

E-passports are currently issued by over seventy independent countries, and it is expected that eventually every country will migrate to these from legacy paper-only passports.

As an e-passport holder travels across the world, entering and exiting different countries, their enrolment biometrics may be utilized at a number of independent border controls. Similarly, each nation will need to be able to process biometrics for every e-passport issuing country. In order to ensure that the e-passport based biometric border systems work to the same high level of accuracy, not only do high quality biometrics need to be captured but these need to be evaluated as being interoperable across all the different countries.

For example, different issuing countries may follow very different capture protocols, use different capture devices, and operate in very different environments. Even if the biometrics are considered high quality for one nation's enrolment process and subsequent border control environments, they are not guaranteed to be suitable and interoperable with other countries border control environments.

The enrolled biometrics need to be evaluated for interoperability across the range of different border control scenarios. While use of e-passport standards, described in the next section, will form the foundation of this interoperability, it will not guarantee it.

2.2.3 Security

The purpose of introducing biometrics into e-passports is to link the person presenting the passport to the document itself through their biometric identifiers. Biometrics can provide an important security feature for passports.

At enrolment it must be confirmed that the data subject is presenting genuine live biometric samples that uniquely belongs to him/her, and not synthetic or other fake biometrics. Many e-passport enrolments are supervised and part of the process could include a manual inspection of the person's biometrics at capture. However, enrolment of face photos for first generation e-passports may take place remotely through the post or online. In such scenarios it may be possible to compare the submitted photo with one from an older e-passport belonging to the same person, as mentioned earlier, and is performed sometimes for other government issued documents such as a driver's license.

It is also desirable to confirm that the person presenting themselves for enrolment, either in person or remotely, is the same person for whom the passport is being issued. Mechanisms, such as use of breeder documents and references, are often already in place for this.

As part of the enrolment process evaluation it needs to be confirmed that procedures are in place to ensure the liveness of the captured biometrics and the link between the person presenting these biometrics and the identity for which the passport is issued.

2.3 Standards

While there are no international standards yet specifying how to conduct and certify the enrolment process for e-passports, there are standards specifying the format of the data on the e-passport including biometrics, biographics, and security data. There are also standards covering the RF chip and communications protocols, and the layout and dimensions of the document itself. We present these existing e-passport related standards both at an international and country-specific level. Relevant standards that could be developed in the future are then discussed.

2.3.1 Existing international standards

E-passports must conform to number of existing standards, which are now examined. The enrolment process must gather and format data in a way that conforms to these standards.

ICAO 9303 – Machine Readable Travel Documents, Part 1 – Machine Readable Passports

Volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format

This part provides the core specifications for machine readable passports with both human readable and machine readable data. It specifies the data page layout, the visual inspection zone, and a machine readable zone (MFZ) contained in two lines of text. Security features and verification of those features are also covered.

ICAO 9303 – Machine Readable Travel Documents, Part 1 – Machine Readable Passports

Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability

This second volume provides specifications for electronically enabled machine readable passports, e-passports. It includes face biometrics as mandatory data to be stored on the e-passport, and fingerprint and iris biometric data as optional data. The biometrics must be high-resolution images stored on a high-capacity contactless RF chip. ICAO 9303 specifies the use of the ISO/IEC 19794 data interchange format standards for the face [16], finger [15], and iris [17] images for e-passports, and these are described below.

The MRZ data and other optional data is also stored on the e-passport chip. A secure data container, the logical data structure (LDS), is defined to hold the biometrics and other data on the chip. Public key cryptography and key management is specified to control access to the e-passport contents. An e-passport page displays a face photo, since this can be manually verified by a non-expert, but does not show the fingerprints or iris images as these require specialized experts and are typically verified by a biometric algorithm.

ISO/IEC 7501-1:2008 – Identification cards – Machine readable travel documents – Part 1: Machine Readable Passports

This standard is a short endorsement of specific content of ICAO Doc 9303 Part 1 – Machine Readable Passports [2, 3]. It defines the specifications for biometric e-passports. It also provides guidance and specifies the form that the e-passport should take to allow details about the holder to be both readable by humans and machines.

Data format standards (ISO/IEC 19794)

ISO/IEC 19794-5, Information technology – Biometric data interchange formats – Part 5: Facial image

data

This part of the ISO/IEC 19794 standard defines the data format for face images as well as the scene and photographic settings to use. The format uses a JPEG/JPEG2000 image. It describes how a photograph should appear and provides some best practices as to how it should be captured, especially for travel documents such as e-passports. Additional metadata such as gender and eye colour may be included in the format. ICAO 9303-1 volume 2 specifies that a full frontal or token face type should be used, and that they can be compressed to a size of 15 to 20 Kbytes for an e-passport.

A token image where the face image has been rotated if necessary to ensure that a horizontal line drawn through the centres of the eyes would be parallel to the top edge of the photo. For e-passports, the centres of the eyes should be approximately 90 pixels apart.

ISO/IEC 19794-4, Information technology – Biometric data interchange formats – Part 4: finger image data

Part 4 of this standard specifies the data format for finger images. It includes compressed or raw images, reader and scanning characteristics, and supplier-specific information. ICAO recommend compressing the finger image with WSQ to a size of approximately 10 Kbytes.

ISO/IEC 19794-6, Information technology – Biometric data interchange formats – Part 6: Iris image data

Part 6 of this standard describes iris image data formats. The rectilinear format may use a raw, uncompressed image or a compressed format. It also included a polar format that requires segmentation and pre-processing of the original image but results in a more compact format. For e-passports, ICAO recommend using a rectilinear image which is compressed to approximately 30K.

Conformance testing standards

For each of the three parts of the ISO/IEC 19794 data interchange standard above, there are also conformance testing standards which include methodologies for testing conformance to each data interchange format. The conformance testing standards for face image [19] and finger image [18] are published, while the iris image version [20] is still under development:

- *ISO/IEC 29109-4:2010, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 4: Finger image data*
- *ISO/IEC 29109-5:2011, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 5: Face image data*
- *FCD ISO/IEC 29109-6, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 6: Iris image data*

These standards should be used to check that the e-passport face, finger, and optional iris data conforms to the specified standards.

Sample quality standards

Biometric sample quality standards have been developed to allow easy exchange of sample quality information. The ISO/IEC 29794 standard [21, 22, 23] specifies methods for defining and interpreting quantitative quality scores for different modalities. Standardization of actual quality algorithms are outside the scope of the standard. This standard should be considered in the design of quality assurance processes for an e-passport enrolment.

ISO/IEC TR 29794-4:2010, Information technology -- Biometric sample quality -- Part 4: Finger image data

This part [21] pertains to aspects of quality specific to the finger image format. It defines the interpretation of finger image quality scores. It also addresses the development of statistical methodologies for characterizing quality metrics to aid interpretation of quality scores and their relation to matching performance.

ISO/IEC TR 29794-5:2010, Information technology -- Biometric sample quality -- Part 5: Face image data

This part [22] pertains to aspects of quality specific to the face image format. It specifies terms and definitions that can be used in the specification, use and testing of face image quality metrics. As with the finger sample quality part, it defines the purpose, intent, and interpretation of face image quality scores.

ISO/IEC NP 29794-6, Information technology -- Biometric Sample Quality Standard -- Part 6: Iris Image

The part [23] of the quality standard relating to iris is still under development, but includes methods used to assess the quality of iris images. It also specifies requirements for both software and hardware that capture iris images and measure their quality.

2.3.2 EU country specific standards

Within the EU some countries have created their own standards and guidelines which are relevant to e-passports. The German Federal Office for Information Security (BSI) has published technical guidelines relating to the e-passport process [24, 25, 26, 27, 28], and these are now briefly examined.

BSI TR-03104, Technical Guideline for production data acquisition, quality testing and transmission for official documents

Provides mandatory specifications for technical systems involved in acquiring application data of sufficient quality at enrolment service providers such as municipal registration offices or embassies. The technical guideline is in German.

BSI TR-03105 Conformity Tests for Official Electronic ID Documents

This guideline specifies the tests which should be performed to check the interoperability of e-passports and the associated readers. It includes a test plan for testing the different security protocols and for testing the application layer logical data structure.

BSI TR-03118, Test Specifications for the Technical Guideline for production data acquisition, quality testing and transmission for passports

This guideline defines test cases for the evaluation of hardware and software components used in the capture, quality assurance, and transmission of e-passport enrolment data. The technical guideline is in German.

BSI TR-03121, Technical Guideline biometrics for public sector applications

Public sector applications include e-passports and e-visas. This technical guideline provides guidelines for a common architecture for public sector applications allowing consistent and comparable quality. It specifies standardized quality and security requirements. It also provides guidance for certification methods, which should be considered in design of an e-passport enrolment service certification process.

BSI TR-03122, Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications

This guideline further addresses quality assurance and is related to TR-03121. It specifies conformance testing for both hardware and software, including BioAPI software. Test cases are provided for conformance testing of capture, compression, quality assurance and formatting of biometric data for electronic identity documents, which would include e-passports.

2.3.3 Standards to develop

As examined in the previous section, there are existing standards for the format of the data on an ICAO e-passport including biometrics, biographics, and security data. There are also standards covering the RF chip and communications protocols, and the layout and dimensions of the document itself.

However, there are no European-wide standards covering other aspects of the e-passport enrolment process. As examined in an earlier section, there is a need to evaluate the quality, interoperability, and security of this process.

This leads to a requirement to develop best practices for an e-passport enrolment process that ensures high quality. It should include finger capture guidelines as there is less guidance in this area. It should also provide iris capture guidelines, since this is an optional e-passport biometric modality that may be more widely adopted in the future as iris recognition gains popularity. The document should incorporate lessons from existing standards (previous section) and the best practice guidelines and evaluation schemes mentioned in both this section and the next.

There is also a need to develop a standard for certification of the e-passport enrolment service. This certification would ensure that it produces biometric enrolment data that reaches a minimum level of quality, interoperability, and security assurance. It could include certification of some or all of the processes that affect e-passport biometric quality, as detailed in an earlier section.

ISO are developing a technical report, draft ISO/IEC TR 29196 [14], with guidance for biometric enrolment. The report will provide guidance for the collection and storage of biometric enrolment data and the impact of enrolment on later verification and identification. The guidance will be generic in nature and applicable to many types of application, including e-passport biometric enrolment. However, differences in operation dependent on different types of application will be noted. Guidance relating to specific modalities, including face, finger, and iris will be provided. The components of a successful enrolment will be presented from the different perspectives of users, enrolment authorities, developers, and enrolment operators. While it is expected that the technical report will provide useful general guidance for e-passport biometric enrolment, it is not intended to provide the specifics for e-passport enrolment or enrolment certification standards.

2.4 Related evaluation schemes

In this section we reference existing evaluation and enrolment schemes and research, parts of which might be adapted for an e-passport enrolment process evaluation. While there are a large number of countries issuing e-passports there is still no standardized process for performing this across Europe.

All kinds of biometric systems use enrolment. The success of these enrolment processes is often measured through later biometric performance testing, as specified in ISO/IEC 19795 [13] test standards, rather than by evaluating the actual enrolment process itself. Evaluation parameters reported typically include failure-to-enrol rates and enrolment quality score distributions.

Many countries produce guidelines for passport photographs, which aim to produce a high quality face photo that is compliant with ICAO recommendations and ISO/IEC 19794-5. Similarly, several countries produce capture guidelines for electronic visas (e-visas), which may include capture procedures for both face and finger biometrics.

The EU BioDev II project [12] investigated how to produce high quality finger enrolments for use in the European Visa Information System. The focus was on fingerprint enrolment, verification, and identification and the interoperability of devices, processes and software. BioDev II found that quality assurance has a large impact on the overall process, but obtaining high quality images increased the enrolment time. The project also

noted the need to specify best practices for high quality enrolment processes. Lessons learned from BioDev II were incorporated into the design of the German BSI specifications for biometric visas and e-passports, listed in the previous section.

Within Europe, Germany is one country which enrolls two fingers and face for their 2nd generation e-passports, and an overview of the enrolment workflow is presented in [10]. Each single finger is captured three times and the best image for each finger is selected based on a quality score. The three images of a finger are matched against each other to avoid substitutions. If an index finger is not available then a thumb, middle, or ring finger is selected instead in that order. Within Germany, there are also enrolment standards for electronic visas, listed in the previous section.

NIST investigated how face capture at US borders using the US-VISIT biometric system could be improved [7], and some of these lessons might also be reusable for e-passport face enrolment. In [8] the same NIST group investigated the optimal height and position of 10-print finger capture. While current EU passports only store 2 fingerprints, there may be lessons from this study that can be applied to e-passport enrolment or identification at enrolment. NIST have also produced a handbook [9] on usability and biometrics aimed at ensuring successful biometric systems. It presents a user-centred design process for biometric systems aimed at increasing usability and user satisfaction.

The communications between e-passports and the physical readers, used at a border control, have been regularly tested by the manufacturers at special e-passport conformance and interoperability testing sessions. While these tests did not examine the interoperability of the enrolled biometrics, they did aim to ensure that the passport readers were capable of electronically reading all ICAO-compliant e-passports. Tests included RF chip interface interoperability, communications protocol interface interoperability, and e-passport application-level interoperability. ISO/IEC 10373-6 [11] defines low-level test methods for proximity cards including e-passports. BSI TR-03105, described earlier, defines conformity testing for e-passports.

The e-passport capture best practices and enrolment certification work should review and re-use lessons learnt from these related evaluation schemes.

2.5 References

[1] Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (13 December 2004)

[2] ICAO 9303 – Machine Readable Travel Documents, Part 1 – Machine Readable Passports, Volume 1, Passports with Machine Readable Data Stored in Optical Character Recognition Format

[3] ICAO 9303 – Machine Readable Travel Documents, Part 1 – Machine Readable Passports, Volume 2, Specifications for Electronically Enabled Passports with Biometric Identification Capability

[4] ISO/IEC 7501-1:2008 – Identification cards – Machine readable travel documents – Part 1: Machine Readable Passports

[5] EU BEST Deliverable 6.1, Inventory of Testing & Certification Institutions in Europe, version 1.0, 30th June 2010.

[6] ISO/IEC TR 19795-3 Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing, December 2007

[7] M. Theofanos, B. Stanton, C. Cheppard, R. Michaeals, J. Libert, S. Orandi, “Assessing face acquisition”, NISTIR 7540, September 2008

[8] M. Theofanos, B. Stanton, C. Sheppard, R. Micheals, N. Zhang, J. Wydler, L. Nadel, W. Rubin, “Usability testing of height and angles of ten-print fingerprint capture, NISTIR 7504, June 2008.

[9] NIST, “Usability and Biometrics: Ensuring successful biometric systems”, June 2008.

[10] O. Bausinger, U. Seidel, "Next generation e-Passport fingerprint enrolment – Quality vs. Time", NIST Biometric Quality Workshop 2007, Gaithersburg, October 2007.

[11] ISO/IEC 10373-6:2011, Identification cards – Test methods – Part 6: Proximity cards.

[12] F. Rahmun, "Towards Best Practices for Biometric Visa Enrolment – Experiences from pilot project BioDEVII", BioSIG 2010, Darmstadt, Germany, September 2010

[13] ISO/IEC 19795-1:2006, Information technology – Biometric performance testing and reporting – Part 1: Principles and framework.

[14] ISO/IEC 3rd WD 29196 Technical Report on "Guidance for Biometric Enrolment"

[15] ISO/IEC 19794-4, Information technology – Biometric data interchange formats – Part 4: finger image data

[16] ISO/IEC 19794-5, Information technology – Biometric data interchange formats – Part 5: Facial image data

[17] ISO/IEC 19794-6, Information technology – Biometric data interchange formats – Part 6: Iris image data

[18] ISO/IEC 29109-4:2010, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 4: Finger image data

[19] ISO/IEC 29109-5:2011, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 5: Face image data

[20] FCD ISO/IEC 29109-6, Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 6: Iris image data

[21] ISO/IEC TR 29794-4:2010, Information technology -- Biometric sample quality -- Part 4: Finger image data

[22] ISO/IEC TR 29794-5:2010, Information technology -- Biometric sample quality -- Part 5: Face image data

[23] ISO/IEC NP 29794-6, Information technology -- Biometric Sample Quality Standard -- Part 6: Iris Image

[24] BSI TR-03104, Technical Guideline for production data acquisition, quality testing and transmission for official documents

[25] BSI TR-03105 Conformity Tests for Official Electronic ID Documents

[26] BSI TR-03118, Test Specifications for the Technical Guideline for production data acquisition, quality testing and transmission for passports

[27] BSI TR-03121, Technical Guideline biometrics for public sector applications

[28] BSI TR-03122, Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications

3 ABC

3.1 description of application: ABC systems based on e-Passports

Despite the economic downturn the world is still suffering, air traffic business still forecasts a steady growth for the upcoming decade. As passenger numbers continue to rise while the number of international airports remains constant, the pressure to process large volumes of people as quickly and securely as possible grows. But this increased throughput at international air border crossing points cannot come at the cost of additional hassle for passengers or reduced security. New approaches are thus needed to make air travel an enjoyable experience for the law-abiding majority while keeping borders effectively closed for the unlawful individuals.

ABC systems at border crossing points allow passengers holding electronic passports to pass smoothly through airport electronic gates, leaving border security personnel to concentrate on second-line controls, managing of possible rejections, and manual screening of ineligible travellers. Frontex is rather clear about the purpose of an ABC system:

> *"The primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met."*

Source: Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems vs0.7, Warsaw, October 2010

The common identifier for ABC systems is the electronic passport, which are complying with guideline ICAO DOC9303 and the European implementation of that guideline EC2252/2004. The biometrics are being used to verify whether the person who presents the passports (and with that claims a certain identity) is the rightful owner of that passport. As most of current European best practices apply only the facial image as biometric identifier, this document only addresses ABC systems based on the e-passport and facial biometrics.

As there are no significant experiences yet with Registered Traveller schemes (EU-NEU) nor with biometric visa control (VIS/BMS), the ABC system is being considered as a standalone system. If in the future other functionalities are being coupled to the ABC-gates infrastructure, each of these functionalities need to be assessed on it's own and in combination with each other. It seems clear that a combination of functionalities will certainly complicate such assessments and will be out of scope of this document.

3.2 objectives of this paragraph

The objectives of this chapter is to investigate which testing schemes and testing capabilities are needed to properly assess the conformance of ABC systems to the Frontex Best Practice Guidelines with applicable standards, guidelines and legal frameworks. Also this chapter tries to understand which standards are applicable to ABC systems conform the frontex Best Practices Guidelines

3.3 what is needed to test and evaluate

Testing and evaluation only makes sense if the object to be tested is clearly defined and specified. The landscape on ABC gates shows a strong diversity of implementation at a European and global level (ref. BEST Network D3.1).

This lack of common specifications and requirements for ABC gates leads to de facto vendor dependency, which is not beneficial for interoperability, performance and competitiveness of the industry. This has been noticed by the European Commission, who has addressed this issue in its latest FP7-SEC 2011 call on ABC gates. Also the Smart border initiative (25.10.2011 COM(2011) 680) focuses on this matter.

So common requirements on European do not exist, nor do common specification exist, despite the efforts of Frontex on their best practices document. Is can be read in BEST Network D3.1, Frontex best network document was not established in consultation with the airlines industry (IATA), which immediately raises the question how much common agreement exists on the requirements and specifications it describes.

As there are no clear specifications yet fr ABC gates in Europe, one can list the specifications of gates already deployed in Europe, while trying to think of some way to develop a benchmark. Given the sometimes large differences between the various ABC-versions that might be a challenge:

Country	**Programme Name**	**Biometrics Technology**	**Status** (reported Feb. 2010)
Austria	ABC System	Face	Planned pilot
Czech Republic	ABC System	Face	Planned Pilot : Technical study available. Fall 2009 pilot
Finland	ABC System	Face	Pilot start: July 2008. Operational since April 2009.
France	PARAFES	e-Passport Fingerprint	Pilot since August 2007. Entry and exit. For EU/ EEA and CH.
Germany	ABG	Databank Iris	Entry and exit. For EU/ EEA and CH, and permanent residents.
Germany	EasyPASS	e-Passport Face	Pilot since October 2009. Entry and exit. For EU/ EEA and CH.
NL	PRIVIUM	Iris Smartcard	Introduced October 2001. Entry and exit. Targets frequent flyers with an EU nationality.
NL	No-Q	e-Passport Face	Pilot Q1 2010. Exit.
Portugal	RAPID	Face e-Passports	Introduced May 2007. For EU/ EEA and CH. Entry and exit.
Spain	ABC System	Face Fingerprint	Planned pilot. 2009 finalizing technical solutions. 2010 pilot.
Switzerland	Augreko	Face e-Passport	Planned pilot from mid 2010.
UK	ABC System	Face	Pilots.
UK	IRIS	Iris Databank	Operational since January 2006. For EU/ EEA and CH, permanent residents and Visa holders. Entry only.
USA/ NL	FLUX -Alliance	US: Databank Fingerprint NL: Iris SmartCard	Pilot until April 2010. Combination of existing GlobalEntry and PRIVIUM programmes. Pre-registration & vetting (extensive background checks).

As already stated in D3.1, the airline industry has hardly been involved in most of these efforts. This is rather interesting, as from the passengers perspective the airlines is the one who they will take accountable for delivering the overall service. Therefore it would be rather natural from a client/provider perspective that airlines would be directly involved in matters that involve the travel experience of their passengers.

3.4 which standards are applicable

ABC Gates systems are already deployed in many countries. Some of them are solely based on a facial recognition system, where others are iris or fingerprint based. The ISO (SC37/WG4) is currently working on a report named "*Traveller processes for biometric recognition in automated border crossing systems*" to express best practices and processes for automated biometric border crossing systems. This reports shows the requirements related to many of the different types of biometric application implementations. It intends to indicate topics and issues which organisations will need to address during the design process, deployment and operation. This report is not a standard per say, it just provides guidelines. We can only hope that this effort will lead to a convergence of requirements and specifications.

Then, the CEN TC224/WG18 is also working on a Technical Specification (TS) "*Personal identification — Recommendations for using biometrics in European Automated Border Check*" dedicated to European Member States. This TS document focuses on automatic border check (ABC) systems and is aiming to help ensuring a continuous, comprehensive and harmonized level of security throughout Europe. Furthermore, the best practice recommendations given in this document focus on helping to make processes for border control authorities more efficient by speeding up border clearance, while delivering an improved experience to travellers.

As ISO/IEC already published a series of standards dealing with biometric data coding, interfaces, performance tests as well as compliance tests (SC37). But it is essential for the global interoperability of the worldwide passport system that all these standards are applied in European deployments. Once applied, they needs to be tested and certified.

However, those standards do not consider national or regional characteristics and differences; in particular, they do not consider European Union privacy and data protection regulation as well as accessibility and usability requirements. This TS shall amend the ISO standards with respect to special European conditions and constraints, and shall propagate best practice experiences made in the first European and international deployments.

Finally, the TS systematically discusses issues to be considered when planning and deploying ABC systems and gives best practice recommendations for those types of systems that are or will be in use in Europe. The document deals with personal identification which also includes ergonomic aspects that reflect the acquisition of biometric data.

3.5 what are the existing/missing testing schemes and capabilities

3.5.1 Document authentication

Document authentication devices for ABC gates have to provide the following functionality:

- Optical capabilities
  - OCR detection
  - Image acquisition in UV, IR, and visible light
- Electronic capabilities
  - RFID communication based on ISO/IEC14443
- Verification of optical security features
- Verification of ePassport data
  - Security protocols BAC, AA, CA, TA
  - ICAO Logical Data Structure
  - Passive Authentication

The following schemes are applicable for testing of document authentication devices for ABC gates:

Scope	*Existing testing schemes*	*Testing schemes missing*
OCR detection	[ISO1831]	X
Image acquisition in UV, IR, and visible light	(internal test schemes of operating agencies)	X
RFID communication based on ISO/IEC14443	[ISO10373] [ICAO_RF-4] [BSI03105-4]	X
Verification of optical security features	(internal test schemes of operating agencies)	X
Verification of ePassport data	[BSI03105-5.1]	X

3.5.2 Biometric verification

Depending on the biometric modality that is used in the ABC gate capture devices for face or fingerprints and corresponding verification units are used.

The following schemes are applicable for testing of face and fingerprint capture devices and verification algorithms for ABC gates:

Scope	*Existing testing schemes*	*Testing schemes missing*
Face capture unit	[BSI03122-3] (Modules “AH-PH-VID”, “AS-PH-VID”, “BIP-PH-VID”, “QA-PH-VID”, “COM-PH-VID”)	Image quality assessment
Face verification unit	[BSI03122-3] (Module “CMP-PH-VID”)	Image quality assessment
Fingerprint capture unit – Hardware	[BSI03118-1] (Section 3.1) [EBTS/F]	Life detection
Fingerprint verification unit		Life detection Vendor independent quality assessment

3.5.3 Background checks / Clearance

ABC gates for EU/EER/CH nationals have to check if the document is known as lost or stolen. For that purpose no common European approach exists. That’s why there are just proprietary internal test schemes of the operating agencies.

3.5.4 Physical equipment

The physical equipment (gate, kiosk, mantrap) has to meet the requirements of several European directives (e.g. Machinery Directive 2006/42/EC, Low Voltage Directive 2006/95/EC, EMC Directive 2004/108/EC).

The compliance to these EC directives is claimed by the CE label.

3.5.5 European testing and evaluation capabilities

The following passage is directly derived from the presentation of Raul Reillo Sanchez during the European Biometrics Symposium on 17th February 2012. It is a summary of earlier discussions during the BEST Network workshops from September and November 2011 about testing and evaluation, as well as a collection of earlier findings through projects like MTIT and BioTesting Europe.

The matter of testing and certification of biometrics based ABC systems can not be specifically address, without first making an assessment of the State of the Art of testing and evaluation of biometric components and systems in general. The problem is that not only the lack of common requirements on ABC systems that make the test subject like a moving target, the biometrics testing industry itself is struggling with various fundamental challenges, that are closely related to the nature of the technology itself.

First we will look what the general requirements are for having a mature testing industry.

One of the main advantages in using an accredited laboratory is that they provide evaluations that are interoperable, traceable, repeatable. If this is all the case, a certificate can issued by an accredited laboratory. However, for an accredited laboratory in order to maintain its accreditation it shall demonstrate periodically its technical capability and evaluation quality. To keep its evaluation quality the lab needs to make sure that:

- all its testing tools maintain calibrated based on common accepted criteria
- perform auto-analysis (i.e. repeat an evaluation and reach the same results)
- perform intercomparisons with other laboratories (i.e. the same test is given to another laboratory, as to see if they reach the same results)

We see that with the testing of biometrics these requirements are poorly met. For that we can not speak about mature testing capabilities for biometric components and systems.

There are currently few Labs that carry on Evaluations of Biometric products, although large roll-outs such as the biometric passport did take place. As soon as society, industry and/or administrations will start requesting certified products, there will be the need of more labs to start business. The fact that there are so few testing labs in Europe capable of testing biometric components and systems might be an indication that the end user (mostly being national governments) doesn't see the benefits of requiring certified tests and products.

There are several types of evaluations can be carried out in Biometrics, such as:

- Conformance testing
  - BioAPI Conformance (ISO/IEC 24709-x)
  - Data format Conformance (ISO/IEC 29109-x and rev.19794-x)
- Performance Testing (ISO/IEC 19795-x)
  - Technology Evaluations
  - Scenario Evaluations
  - Operational Evaluations
- Security Testing
  - Following Common Criteria

At first sight, Biometrics does not seem to present too much of a difference from other technologies

We have currently published many standards that can be used as basis for certifying products. So what is the problem? Why don't we just start testing based on those standards?

Unfortunately there are major differences to other technologies, that make it difficult to have accredited labs for biometrics:

- Testing databases are key to almost any biometric testing, but they are not interchangeable unfortunately. That means that each testing lab has its own references. Previous experiences have shown that the same algorithm can perform differently depending on the database used.
- Data protection laws make it difficult the exchange of biometric data in many countries.
- Variability in human properties makes it difficult to create "standard databases". That means that test databases are needed that are generally accepted and being used as THE reference. For that these databases need consensus on the quality of every single image (if quality of images needs to be tested) and on the features' placement and definition (if the performance/interoperability of feature extractors and matchers is to be tested).
- Scenario and operational evaluations require end-users to interact. That means that data sets will be different for auto-analysis and intercomparisons.
- As it is a rather new technology, there are no certified tools to be acquired, meaning that each test lab takes its own tools. A generally accepted and validated Test Database should be one of such tools.

So what can / should we do?

With **conformance evaluation** problems arise regarding intercomparisons in Data Format

Conformance. For this there are two approaches:

- Send data records to be analyzed by the other laboratory. This requires specific agreements between labs as to comply with data protection laws as well as with audit requirements
- Use certified conformance testing programs. Are there any available?

Unfortunatly with **security evaluations** based on Common Criteria we encounter the problem of two worlds that are not getting a common understanding:

- security experts deny the fact of the enormous differences at the front-end
- biometrics experts do not think (at least at this moment) on CC as needed for evaluating its security level

Than we have **technology evaluations**. This needs a clear defined and detailed methodlogy, which is commonly accepted. Still than we run into the problem of test databases. Not too much helps come from ISO/IEC 19795-1, which says:

> *"For technology testing, a **generic** application and population may be envisioned, ensuring that the tests are neither too hard nor too easy for the systems being evaluated"*

This leaves several questions:

- Due to variability of human properties, how can we find an interoperable definition for ***generic***?
- How can we measure the difficulty of a database? Work is currently being carried out under ISO/IEC 29198 SC37 for fingerprints, but no final solutions are ready yet.

In case we build a Standard Test Database, we run into the following issues:

- How can we use public/privately available databases?
- How can we deal with Data Protection Laws?

Given al these obstacles, why don't we change our approach? For example by establishing a network of distributed data sources made available securely to accredited labs. A similar approach was already proposed by the project BioTesting Europe in 2008 (www.biotestingeurope.eu).

Than we have **scenario and operational evaluation**. Here we encounter some really difficult points:

- Not possible to exchange the "data set" as these data are proprietary and confidential
- In real life applications it often is not even possible to "save" the "data set" used, also not for investigation purposes.

Methodologies are still needed to evaluate the impact at the front-end, caused by:

- Environmental conditions (already under development on SC37)
- Ergonomics
- Usability
- Accessibility
- Processes and procedures
- Etc.

These non-technical factors strongly depend on matters like training and eduction of operating personnel, appropriate Service Level Agreements, the business case as driver for investments etc.

Especially with operational evaluations we run into legal and operational issues that can cause barriers for recording operational data of the system, as these data might not directly be linked with the business process of the application itself. In addition, tools are needed for the analysis of those recorded data, such as video's and large amounts of photos and images.

In Europe the situation is that there are several specialized, highly capable and well recognized testing laboratories and institutions. However, they are not linked to each other (no laboratory network available) and most of them are not accredited. In addition, there seems not be a strong demand for the services of these labs. The latter seems to be rather contradictive, if we take large projects into account such as the e-passport and the European Biometric Matching System. Given these large scale multi national system one would expect at least a European convergence towards common test capabilities. Unfortunately that didn't happen (yet).

The issue of testing and evaluation of biometric components and systems has not been unnoticed by the European Commission. We had the MTIT Project in 2005/2006, followed bio BioTesting Europe in 2007/2008. In 2010 the FP7 security track launched a call with the topic: SEC-2011.5.1-1 *Evaluation of Identification technologies, including Biometrics.* This call was targeted to citizen services and e-passports. Fortunately a significant project was awarded that addresses this call:

The expected impact of a project under this call is:

"To support the development of the proper legal framework (if needed) without endangering the EU legal privacy framework; to increase the industry's competitiveness by allowing them to compete using common standards, to demonstrate to the law enforcement agencies the added value of using common certified systems within the EU (international) operation; to show to the EU citizens that action/progress in this area is possible without building "a priori endangering privacy" systems."

The recently awarded project **BEAT** (**B**iometrics **E**valuation **A**nd **T**esting, starting March 2012 and ending February 2016) seems to be able to deliver on these objectives as its output will include:

- A framework of standard operational evaluations
- Evaluation of the performance, vulnerabilities and privacy preservation mechanisms
- Integration and deployment of the BEAT testing platform
- Dissemination and exploitation of the results
- Legal aspects

More information about **BEAT** can be found at www.beat-eu.org.

The main conclusions regarding the situation of testing and evaluation in Europe are:

- Certification of Biometric products are about to be requested, the real demand is still from unclear requirements

- Certification shall be done by trustable, auditable and independent third parties (i.e. accredited laboratories)
- Tools are still needed:
    - Certified tools for conformance testing
    - A network of accredited labs with sharable tools such as distributed data sources where data is never released from the lab that is in custody
- Common Criteria and Biometrics are two worlds that shall come to a common understanding
- Quality of Scenario and Operational Evaluations can only be audited by the procedure followed, not by the results obtained
- Europe is aware of this situation and working towards building solutions, although funding and interest (both by government administrations and by industry) are still needed.

3.5.6 Privacy Impact Assessment

As already has been stated in BEST network D6.1, only very little consideration has been given in the discussion about ABC gates regarding privacy and data protection. This is partly due to the fragmentation of requirements, which has been discussed in the previous chapters. However, it is without any doubt that the proposed revision of the European Data Protection Directive will have a strong impact on requirements of ABC systems regarding the management of personal data. This doesn't start and end with the passport verification at the ABC gates. In fact, it is the beginning. As soon the ABC gates are introduced and widely deployed – that is the trend we see – new applications will be build on the principle that the ABC gates now can deliver a validated id-credential, which can be used for additional processes and services, such as profiling based on destination (a merge of id-information and flight information) or automated boarding based on biometrics.

All signs point into the direction of a development into the direction of smooth and transparent passengers ground processes at airports. Check Point of the Future of the IATA shows a vision of separating travelers into three different categories, based on the risk profiles of every individual. The automated (or better: machine assisted) border crossing systems like the ABC gates will certainly a core element or even a key enabler for that process.

Fur sure we do not have a common accepted Privacy Impact Assessment, as we do have a variety of ABC that would need to be assessed. Fortunately there are some relevant activities in this area that can be of significant support, such as the European PIAF project: the Privacy Impact Assessment Framework Project, funded by the European Commission (www.piaf-project.eu).

These PIA off course will be built on the Data Protection Directive 95/46/EC, the Regulation (EC) No 45/2001 addressing personal data processing by the institutions and other relevant bodies of the Union, such as the European Parliament and the European Commission. It should also be noted that the Article 29 Data Protection Working Party has adopted some specific recommendations with regard to biometrics in its working document of 1 August 2003.

More information about the Proposal for a revised European Data Protection Directive and for more in depth information about Privacy Impact Assessments in Europe BEST Network D0.6 can be consulted, as this contains relevant information on these matters provided by EDPS Peter Hustinx and PIAF coordinator Paul de Hert. For a general overview on the legislative, regulatory, legal and ethical aspects of biometrics at a European level reference is made to BEST Network deliverable D7.1, D7.2 and D7.3.

3.6 perspectives/issues/recommendations on privacy and data protection

The passage below is a contribution of by WG7 regarding the privacy aspects of ABC systems.

As mentioned in the previous chapter, there has been little consideration of privacy and data protection issues in the Deliverable D3.1 or the Frontex Best Practice starting point documents. In one document, reasons have been given ('lack of expertise and time' – Frontex), the other devotes half a page (of 17) to data protection considerations and remains very general. The lack of focus on this major issue is concerning. Data protection considerations have thus possibly not been as incorporated as other considerations.

ABCs and e-passports present, of themselves, a range of data protection concerns both as to their own security and as to their potential social impact. These issues are part of a wider series of debates regarding the security imperative, automation of security networks, government surveillance, legitimacy of collection of biometric data etc. These discussions and concerns must be considered as a background in the development or analysis of any certification or testing. The FRONTEX document states 'the primary goal of ABC systems MUST be facilitation without disregarding security. Facilitation is thus the main objective to maximize, and security a boundary condition that has to be met'. Data protection and privacy considerations are the rights predominantly harmed by encroaching security and as such should be accorded due consideration.

It would be necessary to elaborate exactly what is to be certified and tested and to clarify what data collection and processing acts in combination with which external processing acts and by whom are required in practise. Only with a greater degree of certainty would it begin to be possible to clarify the data protection and privacy issues involved.

All testing and certification requiring the processing of personal data (with the exception of data already anonymized or not identifying an individual) should be obliged to follow the principles of Directive 95/46 (laid out in article 6) and supporting legislation. The privacy rights of the individual must also be borne in mind laid out in article 7 of the Charter of Fundamental Rights of the European Union and article 8 of the European Convention on Human Rights. Pure privacy concerns may not be so relevant here, but should be borne in mind with the development of any more invasive systems.

Each data processing operation potentially engages the framework in a different and potentially unique way. The following factors may influence the specifics of engagement; specific ABC design, the location of the ABC and the national legislative issues its operation touches on, the purpose of the operation, to whom the data is distributed and who the data controller is, what data is being distributed, which external/other systems are involved in processes and how they interact with these processes. The principles of the framework must thus be applied to each operation with the specifics of the above issues in mind.

ABCs operate differently depending on design and incorporate novel technologies. Their specific qualities must be considered when considering the privacy and data protection in testing and certification. The practicality of their setup and background layout may also be important although are probably not key concerns.

The data protection framework is transposed differently in various countries and under certain circumstances this can lead to different engagement in different states. The potential for this must be considered as must the difference across states in the interplay of the data protection framework and relevant local non-harmonized legislation. The data protection framework may also overlap or interact with other relevant European or international legislation. Legal boundaries and interaction should be clarified

The collection of data necessary for each operation should be kept to the minimum necessary for that operation and data should be stored only for as long as necessary. If possible data should be anonymized (for example in statistics collection). The reality of the possibility of anonymizing biometric data must be considered. The difference between different types of biometric data must also be considered. Different types of biometric data may contain different information about the individual and alone or in combination with other categories of data this may demand their consideration under the more strenuous considerations required by article 8 (processing of special categories of data).

Data may be collected toward different aims, for instance toward improving the operational effectiveness of the system, toward statistics collection or toward developing the business model. Following this, data may be transferred to different types of bodies. The legitimacy and justification of each entity's collection and

processing of data must be carefully considered. Data collection, distribution and storage processes must be tailored with the status of likely recipients and future use in mind.

In testing and certification the interaction of ABC mechanisms with other external databases must be safeguarded. There must be particular care when considering interoperable systems in which data may be dispersed across networks. Where data is captured it must be considered where this data will be stored, and whether it will be stored with or will be easily accessible alongside other data or data sets which together may constitute a breach of the principles of the framework. It must be borne in mind that the ABC system will work in tandem with systems which themselves raise considerable data protection issues and this must be borne in mind when considering testing and certification.

When data must be shared out or dispersed among systems or operators, designations such as controller and processor and the consequent responsibilities should be considered beforehand, otherwise risk getting lost amongst the dispersion.

Where possible it must be made clear to the data subject how and why the data is being processed although, due to clear legal and practical reasons there are limits to this. This has been recommended in the FRONTEX best practises.

3.7 References

[ISO1831] ISO/IEC 1831:1980, Printing specifications for optical character recognition

[ISO10373] ISO/IEC 10373-6:2011, Identification cards -- Test methods -- Part 6: Proximity cards

[ICAO_RF-4] ICAO Machine Readable Travel Documents, Technical Report, RF protocol and application test standard for e-passport – part 4: e-passport reader tests for air interface, initialisation, anticollision and transport protocol, Version 1.01, 20.02.2007

[BSI03105-4] BSI TR-03105 Part 4, Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4, Version 2.2, 17.03.2010

[BSI03105-5.1] BSI TR-03105 Part 5.1, Test plan for ICAO compliant Inspection Systems with EAC, Version 1.2, 11.09.2009

[BSI03118-1] BSI TR-03118-1 (PS Biometrie I), Version 2.1, 17.10.2007

[BSI03122-3] BSI Technical Guideline TR-03122-3, Conformance Test Specification for Technical GuidelineTR-03121 Biometrics for Public Sector Applications, Part 3: Test Cases for Function Modules, Version 2.2

[EBTS/F] FBI Electronic Biometric Transmission Specification (EBTS), Appendix F, Version 9.0, 19.112008

PIAF Project www.piaf-eu.org

BEST D0.6 contributions by Peter Hustinx (Proposed Revisions to the Data Protection Directive), Paul de Hert (Privacy Impact Assessments) and Raul Sanchez-Reillo (testing and evaluation in Europe)

BioTesting BioTesting Europe, Biometric Testing and Evaluation of Biometric Components and Systems in Europe – www.biotestingeurope.eu

BEAT **B**iometrics **E**valuation **A**nd **T**esting – www.beat-eu.org