JRC Scientific and Technical Reports

Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats

James Goldstein, Rina Angeletti, Manfred Holzbach, Daniel Konrad, Max Snijder
Editor: Paweł Rotter

EUR 23564 EN - 2008

JRC EUROPEAN COMMISSION

ipts Institute for Prospective Technological Studies

The mission of the IPTS is to provide customer-driven support to the EU policy-making process by researching science-based responses to policy challenges that have both a socio-economic and a scientific or technological dimension.

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, s/n. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

http://ipts.jrc.ec.europa.eu
http://www.jrc.ec.europa.eu

JRC48622

EUR 23564 EN
ISBN 978-92-79-10657-6
ISSN 1018-5593
DOI 10.2791/5941

Luxembourg: Office for Official Publications of the European Communities

Printed in Spain

FINAL REPORT

Biometrics Deployment Study

Identifying challenges and threats facing large-scale biometrics deployment in Europe

SEVILLE, October 2008

Authors:
James Goldstein *Cybion Srl (Italy)*
Rina Angeletti *Cybion Srl (Italy)*
Manfred Holzbach *Secure Information Technology Cente r(A-SIT) – Austria*
Daniel Konrad *Secure Information Technology Cente r(A-SIT) – Austria*
Max Snijder *European Biometrics Forum – The Netherlands*

Editor:
Paweł Rotter *Institute for Prospective Technological Studies (IPTS) - Spain*

Produced by Cybion Srl
Commissioned by:
European Commission, Joint Research Centre

Acknowledgements

The leaders of the Biometrics Deployment Study would like to thank the following experts who provided their much appreciated support during the timeframe of the study, including the Expert Meeting and Final Conference in Brussels:

- Günter Schumacher – *EC / JRC – IPSC*
- Klaus Keus – *BSI (Germany)*
- Nicolas Delvaux – *Sagem (France)*
- Max Snijder – *European Biometrics Forum (Netherlands)*
- Alessandro Alessandroni – *CNIPA (Italy)*
- Peter Hanel – *Motorola (Austria)*
- Waltraut Kotschy – *Data Protection Commission (Austria)*
- Jan van Arkel – *CEN eAuthentication, Porvoo Group Troika (Netherlands)*
- Christoph Busch – *Fraunhofer IGD (Germany)*
- Bart Preneel – *KU Leuven (Belgium)*

In addition, we are also very grateful for the particular support from Max Snijder and Will McMeechan from EBF for their collaboration with our study in the final conference organisation, Alessandro Alessandroni for his assistance and helpful input and Professor Reinhard Posch and Reinhard Schmid from the Austrian Ministry of Interior for their contributions.

Finally, we would like to thank our study coordinators from IPTS, Ioannis Maghiros and Paweł Rotter, for their continued support during the project.

All their insight into the topic of biometrics deployment helped strengthen the results of the study and we are grateful for their overall support.

Preface

This report, entitled *"Biometrics Deployment Study: Identifying challenges and threats facing large-scale biometrics deployment in Europe"* was commissioned by the Institute for Prospective Technological Studies[1] and produced by Cybion Srl (Italy) in collaboration with A-SIT (Austria). The report is a compilation of the final deliverables of three related studies on implementation challenges for biometrics deployment in Europe.

More specifically, this report includes: (a) the outcome of a year-long investigation (2006-07) on the status of large-scale biometric deployments in Europe; (b) an extract of the outcome of a brief study focusing on the security and privacy challenges of large-scale installations which was validated at a one-day workshop (September 2006); and (c) an extract from the outcome of the European Testing and Certification of Biometric Components and Systems Project which was funded by the Preparatory Action for Security Research (PASR) 2006, the final report of which was presented in June 2008. The aim of the overall study was to feed into the discussions of a European Expert Group on Biometrics which would consider issues related to security/privacy, testing and certification procedures and implementation challenges.

The aim of the Biometric Deployment Study was to point out the common challenges and threats experienced by the most important biometric deployments in Europe. The study concentrated on solutions originated from governmental contractors which involved at least 10,000 users and large-scale solutions developed by the private sector. The aim of the report, "Security and Privacy in Large-scale Biometric Systems," was to present results and discuss open issues regarding data security, protection and privacy of large-scale implementations of biometric systems such as: proportionality and compliance to regulations, standards, best practices and the European attitude to Biometrics. The aim of the "Bio Testing Europe" study, commissioned by the IPSC,[2] was to feed discussions among the members of a European Network for the testing and certification of biometric components and systems, so as to facilitate the creation of testing and certification capabilities at a European level.

The main impact of the study was achieved when the study results and conclusions were presented to the 3rd EBF Research Conference in October 2007. Approximately 100 industry experts, academics, biometric consultants and policy makers, including representatives from the European Parliament, European Commission and Data Protection organisations, gathered for a two-day conference to debate research, industry and end-user challenges for large-scale biometrics deployment. All three study components were well received and thoroughly debated. However, due to the phased development of the three components included in the above study, some of the information presented is no longer (at the time of publishing) up-to-date. While the editors have made every effort to ensure that the material is current, they are aware that factual data in relation to the status of implementation may have changed. However, it has been decided to publish the work as the challenges presented and the conclusions drawn are still believed to be very valid; especially in view of the continuing widespread interest on biometric-based identity services and applications.

The three reports are presented in Chapters 2, 3 and 4 respectively and Chapter 5 summarises the main conclusions of the high-level conference where the results of the studies were debated. Chapter 6 introduces identified challenges and recommendations and conclusions.

---

1 The Institute for Prospective Technological Studies (IPTS) is one of the seven research institutes that make up the European Commission's Joint Research Centre.

2 The Institute for the Protection and Security of the Citizen is another of the seven research institutes that make up the European Commission's Joint Research Centre.

Table of Contents

List of Tables

List of Figures

Executive Summary

The current status (February 2008) of large-scale biometric deployment in the EU is at a critical juncture. EU Member States have been compelled to strengthen their border controls, law enforcement activities and policies, by introducing much debated biometric technology into passports, so as to comply with both EU and US policy requirements. As a result, the large-scale deployment of biometric technologies in identification and authentication applications has rapidly matured. Law enforcement, border control and access control are the three major applications where large-scale biometric systems have been heavily adopted; for instance, in national biometric passports and identity cards, registered traveler systems at airports, Automatic Fingerprint Information Systems (AFIS), visas and driving licenses.

Biometric technologies involve the collection of human traits, such as fingerprints, facial and palm structure, iris, retina and DNA, their transformation into digital representations unique to the owner and their storage. Biometrics may be used to accurately verify that a person's identity is the one indicated on a secure travelling document (i.e. a visitor entering a country at a border control point with his passport), or even identify a person by matching their biometric data to previously-stored identity data (i.e. an individual being checked against a criminal watch –black– list). Hence, the use of biometric technologies, in such large-scale scenarios, may successfully address today's most relevant security challenges.

In the last few years, major projects have been launched within the EU, deploying large-scale biometric systems on both national and EU levels, with a view to enhancing security and protecting the safety and freedom of EU citizens. However, in several cases problems have emerged concerning, for instance, system security threats and vulnerabilities, privacy infringements, lack of experience of border control staff and loss of end-user convenience at checkpoints or enrolment stations. But as EU needs grow, with some of the systems involving millions of individuals as target users, so do the complexities of the challenges that recent EU large-scale biometric deployment projects have to face. Moreover, such concerns may lead to diminishing confidence in the systems and, more importantly, to a lack of trust of citizens in their governments. Therefore, these large-scale biometric deployment challenges need to be appropriately dealt with, so that the benefits of these systems for both EU Member State public institutions and society are positively appreciated. All three components of this report specifically try to address such large-scale biometric challenges. An integrated picture of all related topics, such as technical issues, standards, legal frameworks, data protection and policy implications has been drawn and used to produce the following set of recommendations.

1. Biometric systems **enrolment process:** For interoperability purposes, the enrolment process must be standardised and certified at least Europe-wide. This must include data quality control (biometric and non-biometric), usability for the enrolment application and operator training for service personnel. The individual to be enrolled must be made aware of, and understand, the purpose and range of the application and – except in the case of criminal prosecution – have an opportunity to view and verify whether the identity data the system collects is correct. There must be equivalent and acceptable fallback solutions to prevent discrimination against people not able to enrol (i.e. in case of failure to acquire biometric traits). There must also be EU-wide certified procedures for "un-enrolment" or data modification, operated by strictly authorised and strongly supervised intermediaries and transparency must be offered to the data owner. This must include mandatory data removal when an application or feature expires.

2. Biometric **data storage**: Although important benefits arise from the use of centralised databases, these should be avoided where possible. In case centralised databases are implemented, within the current legal framework for data protection, the data quality must be very high and certified. A legal framework and practical procedures should be defined that enable enrolled individuals to have their identifying stored data revoked or corrected when the data are flawed or of poor quality. An EU-wide standardised complaint collection process should be put in place to guarantee democratic processes. Moreover, biometric data should never be stored in their raw format (e.g. a high definition photo of a fingerprint). Instead, encrypted templates should be used which achieve the same matching result but reduce the risk of identity theft and the likelihood of "function creep". Biometric data should not automatically lead to the connected personal data. This must be restricted to implementing applications with a clear purpose and as few users as possible should be authorised to use such applications. Also, outsourcing the processing of identification data including biometrics to third parties should be avoided when strong regimes to regulate authorised access and functionality cannot be guaranteed.

3. Appropriate **matching** procedures: There is need to define[3] and implement a standardised EU-wide matching algorithm, calibration process, and flexible user interface administered by well-trained, certified and suitably supervised operation personnel. Biometric matches should – wherever possible – only be based on biometric-only matches, excluding the possibility of linking with related personal data. Widely accepted and enforced legal regulations and best practices should limit the number of biometric inquiries to those strictly necessary for the purpose intended. Overall, appropriate implementation of biometric testing standards, facilities and certification schemes are necessary prerequisites for large-scale deployment efforts.

4. Biometric **data security**: Since biometric technologies attempt to address security-relevant challenges, security requirements need to be defined in detail and at an international level where possible. For instance, the following security practices may be implemented: (a) when using biometrics for a secure identification process, the complete security cycle should be considered (i.e. enrolment, storage, acquisition, matching and the entire back-end system); (b) enrolment and matching should be performed using 'live and wellness' detection, especially in unattended environments and/or the process should be appropriately supervised wherever possible; (c) multi-modality (meaning more than one biometric identifier - e.g. facial recognition and fingerprint) is recommended to help prevent spoofing and encrypted templates should be used, rather than original samples, for storing and matching; (d) matching against tokens yields the highest security level and is therefore preferable; (e) implementing an effective key management process is necessary to protect personal data, as is for example the use of the Extended Access Control (EAC) protocol to the e-passport.

5. **Privacy and data protection** issues: There is consensus among stakeholders that there is not enough common agreement on what functionality biometrics should support and how the data should be managed. A common European approach would prove beneficial in overcoming implementation differences among Member States in the handling of privacy and data protection issues. A degree of harmonisation is required to enable a more effective communication of European values to other parts

[3] A European Biometric Matching System has been announced

of the world when debating international data exchange and data handling in connection with privacy and data protection issues, thus providing stronger protection of EU citizens' interests.

6. Biometric systems **purpose and use:** There is a need for initiatives leading to widespread public awareness amongst EU citizens as to the purpose and use of biometric technologies in large schemes such as e-passport and public administration applications. If the purpose of the system is clearly explained to the citizen, and also the way the citizen is expected to interact with the system, and if the safeguards are in place with their resulting benefits, all stakeholders involved would be in a better position to understand their role in biometrics deployment. A fair and open debate could then commence with discussions on costs/benefits, purpose of systems, potential impacts, in the long run ensuring system take-up and use. More specifically, there is consensus that the following issues ought to be clearly communicated to involved citizens whenever new large-scale biometric system deployment takes place:

   i. What are the system security objectives and how should they be incorporated within large-scale biometric technologies?

   ii. What are the envisaged deployment scenarios and how will these address security targets?

   iii. In what way, and based on which options, are decisions made when identifying an appropriate level of trade-off that involved citizens would have to make in relation to values that may need to be sacrificed?

   iv. What regulations need be defined to guarantee that all the processes enabling and controlling the biometric system will work properly and what would an appropriate level of supervision be?

   v. What are practical implications for citizens (and travellers) and how are these likely to evolve in the short and long term?

   vi. What are the expected costs for taxpayers in both the short and long term?

7. **Open dissemination** on implementation phase results: Finally, and as a result of the difficulties encountered in completing the survey due to responsible public institutions citing confidentiality reasons, one overall recommendation for EU policy-makers is to create consensus among the Member States and implement a procedure that would facilitate the open dissemination of all information on biometrics systems in the implementation phase. This lack of information concerning EU Member States large-scale projects does not bode well for biometrics deployment in the future as keeping this data secret could suggest that the systems are not secure, may hide poor error rates, be behind schedule or conceal unsatisfactory roll-out results. If the public sector is considered as a "test-bed" for large-scale biometrics deployment with the eventual transition to industry as the next target, the process is stalled by the lack of information. It is expected that an open dissemination process would create a more fluid communication flow between the major stakeholders (i.e. research, industry and government) and result in more effective systems in the near future.

Structure of the Report

This report is structured as follows:

- Chapter 2 (Large Scale Biometric Deployment Study) presents facts, figures, best practices and analyses open issues in relation to biometric systems actually deployed or under development.

- Chapter 3 (Security and Privacy in Large Scale Biometrics Systems) analyses open issues in relation to proportionality and compliance to regulations, standards, best practices and European mentality regarding data security, protection and privacy.

- Chapter 4 (Bio Testing Europe) presents results and analyses open issues in relation to EU-wide testing standards ensuring that the technical functions produce comparable and certified results under different technologies, vendors and environments.

- Chapter 5 includes the conclusions of the debate that took place during the conference where results from all 3 studies were presented.

- Finally, overall conclusions emerging from the analysis of the various challenges that were identified through out the entire study are presented in Chapter 6.

Some of the projects/systems that were monitored during the study that will be discussed in this report are:

- EU e-passports (both first generation - i.e. those using facial technology, and second generation - i.e. those where fingerprints are inserted to comply with 2009 deadline made by ICAO).

- National ID card initiatives that plan to use, or have implemented, biometrics such as those in Portugal, Spain, Italy, and the much debated ID initiative in the UK, where delays in the rollout of the scheme have recently been reported.

- Registered traveller systems at Schiphol (Amsterdam, Netherlands), Frankfurt and London's Heathrow Airport.

- Access control systems, such as an ID card for the Italian Ministry of Justice.

- Various internationally interoperable EU Member State AFIS deployments

- Databases such as EURODAC, Visa Information System (VIS), Schengen Information System (SIS), SIS II

- BioDev I and II projects, serving as pilots for the VIS

1 Biometrics Deployment Study Objectives and Activities

1.1 Background

The importance of biometrics related research and development has significantly emerged worldwide with the threat of terrorism. At European level, the ever increasing immigration into the EU has also led to consider biometrics as a mean to prevent identity fraud. Two Council Regulations on biometrics enhanced personal documents have been presented, a proposal which deals with visas and residence permits for third-country nationals[4] and a regulation which sets out guidelines for a EU citizen's passport.[5] Moreover the building process of the Visa Information System (VIS) has been launched by a Council decision[6] and the technical specifications on the standards for biometric features related to the development of VIS have been laid out.[7] It is perceived that knowing who is entering the European territory is one of the key elements of an area of freedom, security and justice. Further, it has been understood that preventing visa overstaying for longer times also will prevent correlated crimes. These initiatives define a tight schedule for the implementation of appropriate biometrics enhanced personal documents in each of the Member States. However, major parts of those initiatives are in a preliminary or planning stage and not all of the Member States are prepared currently at the same level.

As a result of the U.S. Enhanced Border Control Act, standardisation and development of biometrics in travel documents has been **mainly U.S. driven**, such as within ICAO.[8] Europe was lagging behind concerning this topic and had to adopt the ICAO developments. As a result, the U.S. has positioned its industry even though there is a strong European biometrics research community and industry. Moreover, aspects which are strongly European-specific such as their high data-protection standards have not yet been solidified.

Finally, the **societal aspects** of biometrics have been discussed even more controversially than technical issues. The nightmare vision of "Big Brother" poses the necessity to balance the relinquishing of privacy with the security benefits that technology promises and therefore has become an obstacle for larger scale deployment of biometrics. The term "trust" is also used in the context of relying on only one single technical solution or one single technology supplier. Therefore, future European-wide solutions have to provide interoperability across Europe on one hand while respecting the individual national or cultural concerns regarding the use of a specific technology.

In **economic terms** the biometrics market is growing and placing a greater demand on the national and international biometric industry, biometric system developers, researchers and end-users to work together. There are numerous issues that require cooperation among the major stakeholders:

- Privacy,
- testing and evaluation,
- infrastructure,
- cost,
- scalability,
- open system interoperability,

[4] COM (2003)558, COM(2006)210
[5] Council Regulation (EC) 2252/2004
[6] Council Decision 2004/512/EC
[7] Commission Decision 2006/648/EC
[8] International Civil Aviation Organisation (www.icao.int)

- data interchange,
- conformance to existing standards.

As we will discuss in the following sections of this report, many of these relevant issues have not yet been satisfactorily resolved. Eventually, the Automatic Border Control concept analysed further in this report requires a very large investment of funds by European taxpayers.

Although the relatively lengthy experience of biometrics in law enforcement and discussions of using biometrics for border control purposes in Europe have begun in Europe before 9-11, the **triggering drivers were launched from the U.S**., not only by the traumatic national experience but also by claiming European security measures as being too weak – which has been understood as a request for immediate action by European policy makers. This claim and the U.S. request for biometric passports to conform to its Visa Waiver program produced political pressure on the implementation of biometrics into the passports within a shorter period than originally planned. Therefore the principle of proportionality has not been properly assessed before embarking on implementation of biometrics in travel documents. ICAO recommendations and existing European directives leave much freedom on the implementation, which makes it difficult for a proper EU wide assessment on proportionality and standards.

Although some large biometric implementations are moving forward, the European Commission and other public funding entities are concerned about the lack of experience with this relatively new technology to be deployed at such a large scale with high costs, since the potential for irreversible impact on society is possible.

Therefore, generic concerns can be summed up with the following questions to consider:

- Will the systems work as promised by the industry?
- Will the investment, effort and possible inconvenience be proportional to the goals to be achieved?
- Can political control over the necessary personal data and therefore trust be obtained?
- What further actions will be required?

To properly address these issues, this report combines results consolidated from various sources such as surveys, expert meetings, thematic conferences and events that originate from three projects commissioned by the Institute of Prospective Technological Studies (IPTS) and funded by the European Commission.

1.2 IPTS Biometrics Deployment Study Objectives

The IPTS Deployment Study was initiated in November 2006 to investigate the current status of large scale biometric deployment in Europe and to gather relevant information regarding the challenges and threats faced by the various deployments on both a national and European level. Cybion and A-SIT have collaborated together in carrying out the different phases of the study which are detailed later in this section.

It is the aim of the present study to **point out the common challenges and threats** that are faced within the most important biometric deployment experiences taking place in Europe. This study concentrates on solutions originated from **governmental contractors**[9] and

[9] While private sector initiatives are not excluded, the major large scale roll-outs are mainly driven by the public sector.

involving **at least 10,000 users**. Large-scale solutions developed by the private sector were also considered as a secondary target.

The objectives of the project are detailed as follows:

- to collect information on and summarise the present **state of biometric deployment** in Europe
- to distribute and analyse a **questionnaire** to be sent to major European players and stakeholders active in the biometric field
- to identify the major **challenges and current problems** for biometric deployment in Europe
- to **propose areas that should be explored** in order to solve or alleviate existing or potential problems that may flow from the large-scale implementation of biometrics systems
- to consolidate results obtained and **options for policy making** flowing from the study, from projects on testing and evaluation and on Security and Privacy
- to organise a **conference at European level** to present the study results and disseminate biometrics deployment related information stimulating dialogue among stakeholders.

The Study is also intended to be a further update of the current situation in Europe since the publication of a study by IPTS in February 2005, "**Biometrics at the Frontiers – Assessing the Impact on Society."** This report therefore provides an update on the progress made or not achieved in the time since that publication.

Overall, the study should assist in understanding the **major challenges** that real biometric deployment solutions are facing and the commonalities between the different solutions and in identifying those areas that require further research. The eventual goal is to **shape public policy making** in the EU Member States starting from the results from the study.

One of the most important outcomes from the study is the **prioritisation of the challenges** faced by large-scale biometrics deployment and the production of a number of recommendations be used at political level. A breakdown of these challenges and recommendations are discussed in full at Chapters 5 and 6 in this report.

The study has been organised in **three macro-phases**:

1. Set up and launch of a survey on at least 50 biometric deployments in Europe
2. Organisation of an expert meeting in Brussels that was held in March 2007 to focus on preliminary survey results and elicit experts opinions on existing biometric deployments and future challenges
3. Organisation of a European Conference held in Oct. 2007 to present to a wide audience the survey and expert meeting results and addressed policy making options.

1.2.1 Phases of study

Part I – Survey on biometrics deployment

The initial task dealt with the identification of European stakeholders in biometrics and the creation of a detailed European map of large scale biometrics solutions with contact information of institutions involved. This activity was carried out starting from background knowledge coming from Cybion and A-SIT and at the same time the information was retrieved, monitored and analysed starting from specialized European Internet sources, such as: articles, surveys and studies, institutional web sites, specialised portals.

Following this identification process, in close consultation with IPTS, a survey has been conducted towards European deployers of biometric systems. The aim was to understand the actual status in large-scale deployment of biometric systems in Europe. Specific characteristics of systems to be analysed concern the size of applications (at least 10.000 users enrolled) and the type of deployers involved (main target is public sector, second step commercial solutions). The first step consisted in the definition of the profile of the requested information to be acquired with the survey, then the selection of deployment cases, the definition of the questionnaire content, questionnaire distribution, and collection of results. Based on the material collected, the relevant information on biometrics solutions and activities was analysed and structured appropriately.

Results: The first analysis output was provided in the **Background Report** for the Expert Meeting. *Project documents:*

- *Deliverable 2 – Preliminary survey results background paper.*
- *Deliverable 3 – Survey results.*

Interviews and participation to external events were also carried out as complementary methods of receiving relevant information from public institutions. They are detailed here:

Austrian Ministry of the Interior – about AFIS and Prum Treaty
To complement the statistical and shorthand information given in the questionnaire, A-SIT had the opportunity of an interview with officials from Austria's Ministry of the Interior. This discussion helped to understand the basic features, methods and experiences with the Austrian AFIS and DNA database network used for law enforcement, which is compliant to the Prum Treaty. It can be concluded that many of those principles and experiences will apply to other countries running Prum-compliant systems.

Interviews with CNIPA (ITALY)
Cybion has had several meetings with CNIPA, the Italian public institution responsible for providing consultancy to all Italian public administration on IT issues and developments including the adoption of biometrics solutions. Study participants remained in contact with the relevant department at CNIPA to keep up to date to the latest large scale biometrics developments in Italy. They have been reported in Chapter 2 in further detail.

10th Conference on Information Security in Berne, Switzerland at Nov 27th,
The conference in German language titled "Sein oder Schein" (which translates into "To be or seem to be") focused on IT ethics and the question **"How much security can a human being suffer?"**

Some presentations and discussions covered developments in Switzerland concerning law enforcement and airport security versus the difficulty for data protection authorities to keep the right balance.

An interesting experience with EU-compliant security checks at Zurich airport is that the official opinion is that most passengers accept the strict regulations, but conflicts with the reality. For example, the latest requirement that bans certain liquids in hand-baggage and forces passengers to place them in plastic bags when going through airport security has actually caused more problems than solutions. The number of items taken away from the passengers did not decrease and security personnel experience an increased amount of both verbal and even physical assaults. Data protection officials claimed that blind faith into security technology will lead to a threat to citizen's freedom caused by errors or mistakes which can not be proven by individuals confronted with an omnipresent "system". Such development was named "Technology Totalitarianism". On the other hand, they made it clear that it is not the purpose of data protection to protect unlawful information or such that keeps criminal action undisclosed.

Part II – Organisation of expert meeting

Starting from the results obtained in the previous phase, biometrics experts were invited to participate to a restricted meeting to discuss the intermediate results achieved. Experts from universities, industry and governmental institutions as well as Commission staff analysed and discussed the collected information. The aim was to provide insights and experts' opinions on the status of biometrics deployment and identify challenges for further deployment and uptake.

Study coordinator Cybion with the support of A-SIT invited a group of experts (see Annex II for the meeting agenda and expert list) to participate in the meeting at the beginning of March in Brussels. The aim of the meeting was to present the preliminary results of the survey and to stimulate discussion and experts' vision focused on the following topics:

- actual status of biometrics deployments,
- existing common challenges and threats,
- roadmap for future deployments.

The preliminary results were presented during the meeting and the study's Background Report (Deliverable 3) was sent to the experts prior to the meeting giving them a preview of the initial results of the survey.

Results: The results from the survey together with relevant findings from the Expert Meeting have been elaborated together to be published in the present document.
Project documents:

- *Deliverable 4 – Expert meeting organisation.*
- *Deliverable 5 – Expert meeting minutes.*
- *Deliverable 6 – Deployment Status Report.*

Phase III – Organisation of a European conference

Once relevant information on biometrics deployment solutions has been collected to a sufficient extent, it was made available to the anticipated experts audience and continuously

kept updated. The two-day event to a wide audience took place on the 2 and 3 October 2007 in Brussels.

The aim of the final conference was:

- to present the results of the survey to IPTS, European Commission officials based in Brussels and to major EU public and private stakeholders in biometrics deployment;
- to learn about experiences gained from various EU public sector institutions in the implementation of their biometrics deployment projects;
- to stimulate a discussion among the participants concerning the conclusions, recent developments and factors that could assist further policy development in large scale biometrics deployment in Europe.

The event, titled the 3rd EBF Research Seminar, brought together major stakeholders from the governmental, research, industrial arenas to discuss the latest developments, challenges and recommendations for biometrics related topics. It also provided findings from two more EC funded biometrics projects mentioned above (focusing on Security and Privacy and Testing). The full agenda of the event can be found in Annex I.

Results:
The results of the survey, the outcome of the expert meeting and of the conference have been consolidated into the present **Final Report** that aims to:

- present an overview of biometric deployment solutions in Europe,
- identify major problems linked to large scale deployment of biometrics solutions,
- gather proposals for policy makers to overcome the identified difficulties and facilitate for the future the deployment of biometrics technologies and applications in Europe.

Project documents:

- *Deliverable 7 – Conference organisation.*
- *Deliverable 8 – Conference minutes.*
- *Deliverable 9 – Final Report.*

To sum, the central interest of this study is to contribute to the understanding of the role of biometrics for the future of security in Europe and to know **by facts, figures and other pertinent information sources,** whether biometric technology is the right step in the right direction for the future of Europe in solving identity, security and data protection challenges.

1.3 Other Biometrics Studies

This report also integrates and presents the results of two accompanying studies carried out on biometrics that were both commissioned by IPTS:

- Security and Privacy in Large Scale Biometric Systems (Author: Max Snijder, EBF).
- Testing and Evaluation (Author: Max Snijder, EBF, also the project coordinator of the BioTesting Europe project).

The present document includes excerpts form the latest report on "Security and Privacy in Large Scale Biometrics Systems" in Chapter 3 and a summary of the current status of "BioTesting Europe"[10] in Chapter 4, respectively.

[10] http://www.biotestingeurope.eu

1.3.1 Security and privacy in large-scale biometrics systems

This report provides input for the European Commission policy in order to achieve a coherent approach and adopt harmonised solutions for the introduction of large scale biometrics systems as required by The Hague declaration of November 2004.
The specific objectives of this report are to:

- Contribute to a better understanding of the challenges concerning privacy and security in large-scale implementation of biometric systems;
- Help to solve or alleviate problems that may rise from using biometric technologies without sufficient consideration of potential threats;
- Provide input for discussion to the participants to a European conference on security and privacy.

1.3.2 BioTesting Europe

The BioTesting Europe project, funded by the European Commission under PASR2006, aims to set out the prerequisites for the establishment of testing and certification capabilities on biometric components and systems in Europe. This is driven by the fact that large scale national and international biometrics based identity systems (passports, visa, eID cards) are being developed and procured, mainly by governments and the European Commission (EU VIS / BMS). Also the increasing use of biometrics in access control and surveillance applications drives the increasing need for developing more trust and predictability of biometrics based applications.

Although much work has been done in the area of independent testing of biometric systems, there are still many open issues to be resolved due to a fragmentation of efforts and a lack of input by end users. The results of many tests in the last few years have shown that test results are still not comparable and that interoperability of biometric technology is not yet achieved. To improve this situation, this project aims at setting up a framework for a European network of testing laboratories for performance and interoperability testing and security evaluation of biometric systems. In order to join forces a business case for such a network is needed, that involves all stakeholders. Because the lack of clear end user requirements it is too early to start directly with in depth technical discussions and setting up the certification schemes.

The objective of the project is to create the basis for the further development of a European Network for the testing and certification of biometric technologies and systems. The network will address the issues that need to be solved in order to create testing and certification capabilities at a European level.

BioTesting Europe provides a platform where the main stakeholders can contribute. These include end users (currently mainly governments), testing laboratories and certification authorities. Industry will also provide input about their products and experiences (technical and commercial).

For details on BioTesting Europe project, see Chapter 4.

1.4 Biometric Fundamentals

This section gives a brief introduction to biometrics technology definitions, methods, differing technologies, measuring units, etc.

Biometric methods are based on an individual's unique characteristics which may be physical (fingerprints) or on behaviour (manual signature). Biometric systems actually deployed are all physical and function by comparison (a match) between a biometric sample given and stored at an earlier time (the reference) and a capture obtained at a certain situation, e.g. a facial image stored in a passport's chip is matched with another image of the same person taken at a border control point (the sample). The advantage is that people always carry their biometric characteristics with them as neither tokens nor knowledge are needed and these given characteristics can neither be lost nor forgotten.

Biometric characteristics are transferred into computer-readable data, called templates. This is not completely precise as two or more biometric samples acquired at different times never yield exactly the same templates. Therefore, matches are based on statistical functions, giving a probability that a match has been found. **This is the reason why biometric systems cannot be not 100% accurate** but rather always have to deal with error rates[11] and require some human interference when the results are in doubt.

The two fundamental types of error rates which influence each other are FAR (false acceptance rate) which means that the system reports a match which is untrue; and FRR (false rejection rate) which means that a true match has not been encountered by the system. These rates are influenced by the system's calibration that is shifting a threshold.

Setting the threshold to zero means that there will be no difference allowed between sample and reference, which would yield 100% acceptances, if there were any positive matches. On the other hand, the rejections would be at a maximum. As a result the threshold is individually shifted to allow more differences until reasonable results for the intended purpose are completed. The point where the FAR and the FRR are equal is called the EER (equal error rate), but practical results are achieved by experience depending on the intended purpose.

This dependency from calibration makes it quite difficult to compare biometric systems.

Another characteristic of physical biometric samples is that they **are neither renewable nor revocable** such as tokens or passwords. If anyone manages to "steal" another person's biometric identifier and make use of it, the person affected has "lost" his/her identity. This issue puts the issue of data security and privacy on the table.

Psychologically, biometrics are felt to be invasive, where computer technology directly interacts with the human body. Fingerprints are often correlated with criminal investigation and taking them is felt as a sign of deep mistrust.

1.4.1 Biometric authentication methods

Verification means that a biometric sample is checked against a known reference of the same person to find out whether it is presented by the right individual. This is called a 1:1 match and it is the same procedure that is currently processed at border control points or when money is withdrawn from automatic teller machines.

Identification means that a biometric sample is checked against a set of references of any persons in order to find out whether there is a record (e.g. a criminal record) or not. This is called a 1:N match and commonly referred in comparisons with watch lists. This function is

[11] DNA analysis, for which it is controversial whether it is biometrics, can be done very accurately.

applied to law enforcement but tends to turn into a political issue as with the example of selecting terrorists out of a crowd using facial images.

Verification usually compares samples and references both captured in controlled environments and with the individual's cooperation. Therefore it is more accurate than identification and less problematic in terms of privacy issues.

Identification purposes often have to use samples captured by chance or from traces and being of low quality, and the 1:N matches require statistical database searches which add complexity and yield lower accuracy.

1.4.2 Types of biometrics samples

Fingerprints

Identification by fingerprints exists for more than 100 years in law enforcement and is well-known. It is based on the fact that every individual has unique fingerprints, i.e. ridges and furrows on the finger's surface. Areas where ridges are separating or ending are called **minutiae**, and they show individual characteristics which can be measured to decide whether a fingerprint matches to a previously enrolled sample. Matching accuracy depends on the fingerprint image's quality in respect to enrolment technique. Therefore, rolled fingerprints of all ten fingers are very accurate whereas flat fingerprints of only one or two fingers are often not. Consequently, law enforcement either uses live-scanners for enrolment or specially trained personnel must identify images from ink-based enrolment using dactyloscopes.

Fingerprint captures require the individual to be physically present, is often felt to be invasive and still carries the negative image that one feels being treated as a suspect.

To prevent counterfeit fingerprints, fingerprint scanners should measure signs of life, e.g. temperature of the finger enrolled or the capturing process is to be supervised.

Facial Images and face recognition

Identification by face recognition analyzes an individual's facial structure captured by a camera by measuring various points, e.g. eye distance and length relations, yielding a template which is unique for every given face. Such templates are stored in chips (e.g. in biometric passports to be matched with the actual person attempting to enter at a border control point - a verification process) or in one or more databases to match against. Face recognition requires facial images with particular qualities, which have been standardised by ICAO for passports.

Facial images can be taken over great distances and theoretically do not need the individual's cooperation.

Today, facial recognition is not accurate enough to solely serve as a means to identify suspects out of a crowd, as desired for counter-fighting terrorism. Therefore, it is used together with other biometric characteristics, e.g. fingerprints.

Preventing fakes can be achieved by measuring slight face movements during the capture phase.

Iris Scan

With iris scan, a video camera captures human eyes from a distance approximately 50 cm, far enough not to be felt as invasive and the device analyzes points in the tissue around the pupil, yielding a unique pattern which is stored as a template.

Preventing fake results can be achieved by varying the light, which forces pupil reactions.

Iris scan yields very few false positive errors, but requires more storage and time than other means, and forces the person to hold his face straight and up until now cannot be performed over greater distances.

DNA

Every individual has a unique DNA pattern which appears in every cell, such as a given saliva sample compared to cells from hair found on a crime scene. DNA matching must be performed by special labs and therefore is time-consuming and expensive. Currently, it is commonly used only for investigations on serious crimes. The analysis provides a series of characteristics appearing as numbers. The more analysed, the better the accuracy is up to almost undoubtable matches.

As well as with fingerprints, a suspected person must be present for taking a DNA reference sample which can also be perceived as invasive. However, trace samples are taken without cooperation from objects the person is in close contact with, like drinking glasses.

Other

Biometric systems based on vein temperature, hand geometry, etc. are not reported to be deployed on a larger scale and therefore are not discussed in this report.

1.4.3 Biometric devices

By functional means, biometric systems consist of:

- The **sensor**, which is the device capturing the biometric characteristic and translating it into a template.

  Sensors are suited to the type of biometric data and in most applications should provide a live-test to ensure that the sample originates from a living organism and not from fake entities (like rubber fingers).

- The **storage media** for templates, whose options are databases or tokens.

  This also depends on the purpose, e.g. passports are carried and presented by their owners; therefore for verifying their identity the biometric template can be stored in the document's chip. Concerning checking a suspect against arbitrary traces, these templates must reside in databases.

- The **matching logic** which performs the statistical analysis between a fresh sample and one or more references.

  This is the crucial component deciding 'yes' or 'no'. Therefore it is often subject to manufacturer's business confidentiality and can be considered as expensive.

- Some other non-biometrics components are needed such as **elaborate software implementation** to integrate all those functions, link the biometric data such as the individual's name etc. and allow data inquiries and exchange between systems.

1.4.4 Error rates

The original intention of this study was to gather error rate data regarding major European biometrics deployment systems. This was attempted with the questionnaire that was carried out, but as a result, it remained too difficult to make comparisons with the results received, when they were given. In fact, gaining this kind of information turned out to be a challenging task as many project managers responsible for the biometrics deployment were often not willing to provide this information.

Comparisons based on the questionnaire wouldn't be significant, because different systems for different purposes in different environments have been reported. Further, this would require to reveal the testing environment, the number of tests being performed and still would differ by the system's purpose and cooperation of the person in question.

Error rates are not absolute measures like weights but rather statistical results of many measurements. **They are only meaningful with given test parameters like thresholds.**

FAR (False acceptance rate = decision by the system) / **FMR** is security relevant with access and border control, because they would allow unauthorised people to pass. With law enforcement, it means that probably innocent people are verified as suspects and the real criminal could still be at large.

FRR / FNMR (false rejection rate / false non match rate) by literature is seen as relevant for convenience. FNMR is a matter of the application and template quality. This is true for access control where every authorised user should match, but practically may have impacts on persons getting into trouble at borders and regarding AFIS database searches it is difficult or nearly impossible to recognise whether an inquiry did not find a matching sample or if there has been a mismatch by error.

Failures to enrol can be recognised in controlled environments, but could have impacts for people not enrol able in passport systems, e.g. fingers from some manual workers, injuries on the fingers – who decides if they were real injuries or by intention?

Passport face images should always be enrolable with the person's cooperation, as exemplified with Iris based system for fast-lane border control showing good results.

AFIS (Automated fingerprint information systems) as a whole have no failure-to-enrol rates, a suspect's enrolling procedure will be repeated as often as necessary with different processes (flat bed scan of paper print or manually by human expert).

Transaction times for single verification have been reported in relatively wide ranges, also depending on type of biometric data. This is a matter of purpose, low transaction times are very important for border and access control. It should be faster than being carried out by an officer. Some seconds, even minutes do not matter for AFIS, where maximum quality is the most important issue.

Yet most crucial is the time needed for the entire verification /identification process.

A reported 1,5 seconds for Iris-based automated access control are very convenient, although an FRR of 1,5% would mean that 15 out of 1000 persons cannot use the fast lane.

Accurate biometric systems usually produce a number of potential matches rated by scores showing the match's similarity. The drawback is that this adds complexity and storage requirements, and today there still is a lack of experience with statistical searches into multi-million record databases.

1.4.5 Large biometric databases with many users

The technical challenges of large biometric databases concern the size (designed for up to more than 100 million individual records), long retention periods (e.g.: US VISIT: 75 years) and the problem of statistical searches (resulting in probable inquiry hits and error rates

exponentially increasing) due to the nature of biometrics. As matches depend on the data quality, this issue must be considered as high priority and standardised.

In terms of organisation, a central database like VIS (Visa Information System) requires many users to have authorised access, which imposes supervision to provide efficient use and to prevent inquiries which are not allowed.

The multi-application, multi-user scenario under different national legislations makes it problematic to provide easy but strictly governed procedures to modify or delete incorrect or poor quality data.

Such large and concise collections of personal data will raise strong interests from entities not originally intended or not allowed to use them. Linking biometric information to personal data should be avoided whenever possible and data security is an utmost issue.

2 Overview of EU Large-scale Deployments

This chapter provides an in-depth look at the current biometrics large scale deployments in Europe. It is the result of data gathered, input received, experiences learned from the survey, expert meeting and final conference on the most relevant deployments that are either ongoing or planned for launch in the near future in Europe.

First, we will describe the actual state of biometrics according to the main applications: law enforcement, border control and access control. This will address the latest developments and best practices in each of the considered applications. This section will also serve as the opportunity to report on the projects that are considered on a European level (e.g. VIS, BioDev I and II)

The **following section** reveals information concerning the specific relevant large scale biometric deployments taking place in each of the EU Member States with details on the institutions, typology of biometrics technology, status of deployment and contact information. This mapping was created utilising both desk research as well as benefiting from the knowledge of experts at the Expert Meeting and input from the final conference. During the timeframe of this study, many developments and news regarding EU biometrics systems (particularly focused on public sector large scale deployments) were monitored. There are cases in which some systems originally investigated from the beginning of the study produced data that changed over the period of the study. (i.e.: EU Member State ID documents that originally intended to incorporate biometrics technology, but later in 2007 decided for various reasons to withdraw the technology or not select other ID tech options to support the systems.)

In addition, large scale biometrics roll-outs tended to instigate political discussion and often the debate drew strong opinions especially from privacy interest groups who are opposed to national ID cards. The best example of this situation focuses on the ongoing debates in the United Kingdom regarding the roll-out of its biometrics-planned ID card initiative. Currently, the UK Home Office has expressed its continued determination to move ahead with the ID card, claiming that the project is actually ahead of schedule and has remained far under projected costs despite rumours of delays in the system roll-out and complaints about the costs of the development. This study recommends that other EU Member States carefully monitor the latest updates in the UK regarding this issue since the privacy concerns communicated by the English public and also by politicians demonstrates how a roll-out could struggle in reaching its goal if issues of citizens' privacy and security are not carefully considered and if public awareness is not carried out effectively.

France is another case of an EU Member State where biometrics implementation to ID documents has been all but banned by its data protection authority.[12] Nevertheless, this study will report on those developments up until the end of December 2007. There is no doubt that the issue is constantly evolving and news on this topic will change in the coming months.

The **final part** of this chapter will provide a comparison of the status of large scale deployment in other parts of the world. This report specifically cites the United States and Canada following the presentations that were made at the study's final conference in Brussels.

[12] For a statement made by the French research authority CNIL, see the following link (in French language) http://www.cnil.fr/index.php?id=2166&news[uid]=421&cHash=14b66b0d0c

The following tables demonstrate the large scale biometric systems that have been identified and will be discussed in this chapter. References are made to where more detailed information can be found. Data in this table has last been checked in December 2007.

Table 1: Large-scale biometric deployments overview: EU level

EU level				
Biometric System	**Name of Institution**	**Application**	**Biometrics tech.**	**Ref. Info**
EURODAC	EDPS + Data Protection Authorities from participating member states	AFIS	Fingerprint	Pg. 26
SIS II	European Commission DG Justice, Law Freedom	Visa	Fingerprint	Pg. 32
Visa Information System (VIS)	European Commission DG Justice, Law Freedom	Visa	Fingerprint	Pg. 34
Bio Dev I		Visa	Fingerprint	Pg. 34-35
Bio Dev II	Border control institutions from Austria, Belgium, France, Germany, Luxembourg, Portugal, Spain and the UK	Visa	Fingerprint	Pg. 35

Table 2: Large-scale biometric deployments overview: EU Member State level

EU Member States			
Biometric System	**Name of Institution**	**Application**	**Biometrics tech.**
AUSTRIA (pg. 34)			
Austrian biometric passport	Osterreichische Staatsdruckerei (OeSD)	Passport / Border Control	Face
AFIS	Ministry of Interior	AFIS	Fingerprint; Facial Image DNA
BELGIUM (pg. 36)			
Belgian biometric passport	Federal Public Service Foreign Affairs, Foreign Trade and Development Cooperation	Passport / Border Control	Face
AFIS	Belgium Refugee Bureau	AFIS	Fingerprint
BULGARIA (pg. 36)			
Bulgaria eID card	Ministry of Interior	E-identification	Fingerprint Retina
CZECH REPUBLIC (pg. 37)			
Czech Republic biometric passport	Ministry of Interior *Office for Personal Data Protection*	Passport / Border Control	Face
DENMARK (pg. 38)			
Denmark biometrics passport	Danish National Police	Passport / Border Control	Face
Denmark Visa	Ministry of Integration	Visa	Fingerprint
ESTONIA (pg. 39)			
Estonia biometric passport	Ministry of Interior	Passport / Border Control	Face
FINLAND (pg. 40)			
Finland biometric passport	Ministry of Interior	Passport / Border Control	Face
AFIS	Finnish Police	AFIS	Fingerprint
FRANCE (pg. 42)			
VISABIO	Ministry of Interior	Visa	Face Fingerprint
France biometric passport	Ministry of Interior	Passport / Border Control	
"PEGASE"	Aeroports de Paris (ADP) Air France	Airport Access	2 Fingerprints

GERMANY (pg. 43)			
Germany biometric passport	Federal Office for Information Security (BSI)	Passport / Border Control	Face Fingerprint
"Ausländerzentralregister (AZR)"	BSI Federal Office for Migration an d Refugees	Visa, Asylum seeking initiatives	Face
Electronic office ID card for Germany's federal authorities	Federal Criminal Police Office (BKA) and BSI	ID card	n/a
Biometric border control system based on iris scanning at *Frankfurt Airport*	Bundespolizei (Federal Police)	Airport Automated Border Control	Iris
GREECE (pg. 44)			
Greece biometric passport	Ministry of Public Order (Hellenic Police)	Passport / Border Control	Face
HUNGARY (pg. 44)			
Hungary biometric passport	Central Data Processing, Registration and Election Office	Passport / Border Control	Face
IRELAND (pg. 46)			
AFIS for national police force	Irish Naturalisation and Immigration Service and Ireland's National Police Service (An Garda Siochana),	AFIS	Fingerprint
Ireland biometric passport	Irish Department of Foreign Affairs	Passport / Border Control	Face
Automated visa application and tracking system for foreign nationals seeking to enter Ireland	Irish Department of Justice, Equality & Law Reform	Visa	Fingerprint
ITALY (pg. 48)			
Italy biometric passport	Ministry of Interior	Passport / Border Control	Face
Carta di Identità Elettronica (CIE)	Ministry of Interior	ID card	2 Fingerprints
Ministry of Justice "Multi-services" Card	Ministry of Justice	ID card	Fingerprint
Carta di Difesa	Ministry of Defence	ID card	Fingerprint
AFIS	Ministry of Interior and Criminal Police	AFIS	Fingerprint
Permesso Soggiorno Elettronico (PSE) – Italian Work Permit	Ministry of Interior	Visa/Work permit	Face Fingerprint
LATVIA (pg. 49)			
Latvia biometric passport	Office of Citizenship and Migration Affairs	Passport / Border Control	Face Fingerprint
LITHUANIA (pg. 50)			
Identity documents issuance system (ADIS)	Ministry of Interior	Passport / Border Control	Face
LUXEMBOURG (pg. 50)			
Luxembourg biometric passport	Ministry of External Affairs	Passport / Border Control	Face
MALTA (pg. 51)			
Malta biometric passport		Passport / Border Control	Face
NETHERLANDS (pg. 52)			
Privium Automated Border Passage	Immigration and Naturalisation Department (IND) and the Koninklijke Marechaussee Schiphol (Airport Police)	Registered Traveller Programme	Iris
Netherlands biometric passport	Ministry of the Interior and Kingdom Relations	Passport / Border Control	Face
POLAND (pg. 53)			
Poland biometric passport	Ministry of Interior and Administration	Passport / Border Control	Face
PORTUGAL (pg. 54)			
Portugal biometric passport	Serviços de Estrangeiros e Fronteira	Passport / Border Control	Face
Citizen's Card (Cartão de Cidadão)	Unidade de Coordenação para a Modernização Administrativa (UCMA)	ID card	Fingerprint
RAPID (Automatic Identification of Passengers Holding Travelling Documents)	SEF - Serviço de Estrangeiros e Fronteiras	Passport / Border Control	Face

ROMANIA (pg. 55)			
Romania biometric passport	Ministry of Interior	Passport / Border Control	Face
SLOVAKIA (pg. 55)			
Slovakia biometric passport	Ministry of Interior	Passport / Border Control	Face
SLOVENIA (pg. 56)			
Slovenia biometric passport	Ministry of Interior	Passport / Border Control	Face
SPAIN (pg. 57)			
Spain biometric passport	Ministry of Interior	Passport / Border Control	Face
eID card	Ministry of Interior	ID card	Fingerprint
SWEDEN (pg. 58)			
Sweden biometrics passport	Ministry of Interior	Passport / Border Control	Fingerprint
	SAS Airlines	Registered Traveller Scheme	Fingerprint
UNITED KINGDOM (pg. 60)			
UK biometrics passport	Identity and Passport Office	Passport / Border Control	Face
National ID card	Identity and Passport Office	ID card	Fingerprint
Biometrically enabled access control trial at Heathrow Airport 2006/07	BAA	Registered Traveller Scheme	Iris
UKVisas	Identity and Passport Office	Visa	Fingerprint
Other European countries			
NORWAY (pg. 61)			
Norway biometric passport	Norway's Ministry of Foreign Affairs and the National Police Computing and Material Service	Passport / Border Control	Face
SWITZERLAND (pg. 61)			
Switzerland biometric passport	Federal Office of Police	Passport / Border Control	Face

2.1 Biometrics Applications

The most advanced – in terms of deployment – application area are **automated fingerprint identification systems (AFIS**) used for **law enforcement** purposes. Although "fingerprint" is part of the title, they use all kind of information available depending on the objectives. Police are able to exchange data respectively by inquiring in various biometric databases in cross-border locations.

The EU decision to implement biometric features (digital facial image and in the near future also fingerprints) in **EU passports** and the US Visa Waiver programme led to a widespread deployment of large-scale biometric systems for face-recognition and fingerprint technology in Europe. In addition to the obligatory implementation of biometric data in travelling documents, some Member States also provide their national e-ID cards with biometric data. However, at this point **biometric enrolment** is regulated and performed, whereas its usage for border control is so far in pilot status.

A new development area that will focus attention in Europe in the near future revolves around "**registered passenger**" systems. A Registered Passenger scheme is an **access control** application whereby interested passengers would apply to a national authority, be subjected to a risk assessment and, if successful, be registered as someone presenting a low risk to aviation security. When departing from an airport in the European community, registered passengers would be subjected to lighter (or maybe even exempted from) certain security checks after identification or would be allowed access to an expedited process of security checks and eventually even border control. The Privium project at the Schiphol airport in the Netherlands, the ABPC (Automated Biometry-Supported Passport Control) project at the Frankfurt airport in Germany and the IRIS (Iris Recognition Immigration System) project in the U.K. are examples of deployments of which utilised iris recognition technology.

AFIS and border control systems are currently or will be using fingerprint or face-recognition technology. Some access control systems are using iris recognition. As AFIS and border control systems will integrate together in the automated border control scenario, iris scan could be potentially left out because it is not intended for biometric passports or visa, and its usage for law enforcement is not developed yet respectively. Iris is not considered to be a type of biometrics used in crime scene investigation by now.

Other technologies as voice scan, dynamic signature verification, keystroke dynamics, vein pattern recognition etc. could not be identified in large scale deployments and are not included for purposes of this report.

The following applications will be analysed in the next sections:

- Law enforcement,
- Border control,
- Automated access control.

2.1.1 Law enforcement

Law Enforcement (AFIS – Automated Fingerprint Information Systems) are intended to find biometric matches from suspects enrolled with samples from crime scene investigations to understand illegal entries. Therefore this is a security relevant area.

The most relevant **challenges for law enforcement** utilising AFIS systems are:

- to enhance crime-scene investigations by having access on biometric samples in various countries.
- to counteract illegal immigration, e.g. preventing entry of the same person at different border control points.
- to prevent crime, terrorism and damage by unwanted or disorderly individuals by identifying known suspects in advance.

Eurodac is a prime example of AFIS. Eurodac[13] is an information system which was set up with the purpose of identifying the Member State responsible for an asylum application lodged within the European Union, in order to speed up the asylum procedure.[14] The Eurodac system enables Member States to identify asylum seekers and persons who have crossed an external frontier of the Community in an irregular manner. By comparing fingerprints, Member States can determine whether an asylum seeker or a foreign national, found illegally present within a Member State, has previously claimed asylum in another Member State. In addition, by being able to check if an applicant has already lodged a request for asylum in another Member State, "asylum shopping" in other Member States after being rejected in one can be avoided.

Created by a Regulation of the Council of Ministers, in December 2000,[15] Eurodac has been operational since 15 January 2003 in all EU Member States (except Denmark), Norway and

[13] Extracted from: "EURODAC Supervision Coordination Group Report of the first coordinated inspection" - Brussels, 17 July 2007; Secretariat of the Eurodac Supervision Coordination Group, EDPS. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-07-17_Eurodac_report_EN.pdf

[14] The implementation rules for Eurodac are set out in Council Regulation (EC) No 407/2002 of 28 February 2002.

[15] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention (hereinafter, "the Eurodac Regulation").

Iceland. In May 2004, ten new Member States joined the users group, followed by Denmark (on 1 April 2006), and in 2007, Romania and Bulgaria. Moreover, agreements have recently been signed with Switzerland and Liechtenstein in order to allow those countries to use the system, probably by around 2008.

In accordance with the Eurodac Regulation, all asylum applicants over the age of 14 have to have their fingerprints taken when they request asylum either within or outside of the EU. The fingerprints are then sent in digital format to Eurodac's Central Unit, which is hosted within the European Commission. The system compares the prints with others already stored in the database, thus enabling authorities to check if the applicant has already lodged an application in another Member State or if they entered the European Union without the necessary papers.

The Eurodac system is equipped with an Automated Fingerprint Identification System (AFIS) and an electronic data transmission application (provided by TESTA). AFIS receives data and transmits positive and negative replies to the National Access Points (NAPs) in the Member States. The system also allows Member States to exchange information about asylum seekers and illegal immigrants. Only national authorities dealing with asylum have access to the database.

Personal data processed by Eurodac falls into three categories: applicants for asylum of at least 14 years of age ("category 1"), aliens apprehended in connection with the irregular crossing of an external border ("category 2") and aliens found illegally present in a Member State ("category 3").

The following data are recorded:

- the Member State of origin,
- the fingerprint,
- the sex, and
- the reference number used by the Member State of origin.

In case of a hit, an additional exchange of data takes place through the DubliNet system. The Members States concerned can thus exchange personal data different from the Eurodac data: name, date of birth, nationality and photo, particulars of family members and in certain cases addresses.

In accordance with the Eurodac Regulation, the European Commission has to produce an annual report on the activities of the Central Unit responsible for operating the central database. Until now three reports have been submitted to the European Parliament and to the Council. The three annual reports underlined among others some issues related to data protection.

Like Eurodac, the concept for international data inquiry exchange has developed from national systems (paper-based AFIS) composed of a consortium of a few Member States[16] and now maintains valuable experience.

The workflow components have been developed by the local public authorities, whereas specialised components like biometric matching have been produced by industrial stakeholders.

[16] Germany, Austria, Netherlands, Belgium, Spain, France, Luxembourg

The experience is positive in organisational and technical terms as well as in reasonable and acceptable costs.

Process features

One of the case studies used as a prime example of a law enforcement system is that of Austria's Ministry of the Interior (BM.I) whose staff members were contacted by A-SIT and provided much relevant information for this study that is hereby described in the following sections.

This Austrian ministry runs an integrated, workflow-oriented system to assist law-enforcement covering international criminal, suspect, asylum, illegal immigration and vehicle data including biometric information as image, fingerprint and DNA. International cooperation is based on the Prum Treaty, initially signed by 7 EU Member States which is subject to become EC legislation by the Council.

Some **process examples** described here are already performed and can serve as best practices to comply with by fully operational Prum Treaty members.

Biometric data are captured together with registering text data for known persons (suspects, asylum applicants), mostly 10 fingers rolled in dactyloscopic quality, in addition also palm prints (i.e. the whole hand) as well as photographs (front/profile) of biometric quality. Where feasible, life scanners are used. A quality check is always performed immediately and a second capture done when quality is not sufficient. This is acceptable in law enforcement because there is no immediate need for processing speed at enrolment with the suspect or applicant present as long as needed, poor data quality could have much more negative impacts. The quality is so high that fingerprints serve as match keys for inquiries in databases.

DNA samples are only taken if the person in question is a suspect for selected heavy crimes. Analysis is completed by contracted DNA labs while the data transfer to and from the lab is anonymous by barcodes. If the result from the lab matches with a trace, a second analysis is done for confirmation. The confirmed DNA analysis results are stored in a specialised DNA database.

All police officers dealing with a case or the person in question have a standardised user interface showing all data available in respect in correspondence to their personal access rights.

Crime prosecution inquiries (e.g. to prove a suspect's identity) are 2-step operations. The first step is an anonymous search for automatic matches, mainly based on fingerprints. The second step following a positive match from the prior one, is a manual confirmation check (dactyloscopic analysis for fingerprints). Only after both matches are confirmed is when the identity of the person in question is unveiled. If the match is a result of an international inquiry, requests for personal data have to be done conventionally (in writing – e.g. Interpol).

Conceptual features which could serve as generic best practices:

- There is a strong **focus on data correctness** to avoid doing harm to innocent individuals. Data capture including biometrics is always performed twice, even positive DNA matches always require a second analysis for confirmation.

  Other relevant characteristics:

  - Automatic positive fingerprint matches always have to be confirmed by manual check.

- If a sample can not be confirmed in the second run, the issue is either manually clarified or the sample is dropped.
- Even manual confirmation is always double-checked.
- System provides a current identification quality status for a given sample (proven/likely/ undoubtable).

- The system provides a **uniform workstation functionality** and user interface to optimize support and user productivity and minimize user errors.

  Other relevant characteristics:
  - Working data based on XML-sheets.
  - Upon inquiry, first screen shows text data (name, alias, case), image and which biometric information is available.
  - Differences are only in component capabilities (e.g. biometric capture or not) and user rights (read-write access).

- Access, transfer and matching of **biometric information are anonymous**.

  Other relevant characteristics:
  - It is based on a barcode attached to biometric sample.
  - No personal information is exchanged for automated biometric inquiries.
  - DNA labs do not have knowledge on personal data linked with the samples.

- **Databases** are decentralised and **specialised for particular purposes** (data vs. biometric):
  - historically grown.
  - They avoid performance bottlenecks.
  - relaxes storage limitations (e.g. for cold cases).

  However, centralised databases like EURODAC, VIS and SIS II are subject to integration.

- **High flexibility**, also for identification criteria (e.g. multiple alias names).
  - Identification is mainly based on fingerprint match (identifies when only alias names are known).
  - Almost all information can be used for inquiry (name, alias, fingerprint, etc.).

- **International data transfer** is handled via the TESTA network which is compliant to EU policies.

- Definition of **minimum quality criteria** for biometric information in the Prum Treaty:
  - to cover the problem of different qualities in different countries, (e.g. DNA matches depend on number of DNA measures).
  - to limit the daily number of daily cross-country database inquiries (which could overflow in smaller countries).

- Functionality has been developed based on **ongoing consensus with data protection** officials.
  - Austria's Data Protection authority has been involved from the beginning of the process which helped avoid additional problems and debate after implementation. This has led to legal compliance and public acceptance.

Practical experiences:

- The extremely high fingerprint (rolled ten-prints) quality permits the use of matching keys. However samples from crime scenes are of low quality resulting in few false positive matches, but more false negative than there ought to be.
- Flat single fingerprints (e.g. from passports) are usable for verification (1:1), but not for matching with traces (1:n).
- The error risk with good biometric samples is lower than the risk of typing errors with barcodes or names. Therefore data typing is always done twice for identification-relevant data. The biometric information (anonymous) is less dangerous than text and protocol data (personalised).
- Fingerprint capture is not a trivial task and needs user training.
- Full-electronic life-scanners are expensive and require cooperation of the person in question for good results, otherwise flat-bed scanned paper prints are used.
- Biometric components are expensive.
- Face recognition testing has so far: good results for 1:1 verification, but is not reliant enough for 1:n identification.
- Response times within a few minutes for biometric match inquiries are acceptable for law enforcement, but will not be for border control.
- The development has met functional, timeframe and budget expectations.

International cooperation – the Prum Treaty

Law enforcement has a long history of collecting all kinds of data, and therefore **different databases have grown** in EU Member States over the decades. Automated data exchange and cross-country inquiries are relatively new features and face the problem of different locations, formats, **data qualities** and legal obligations to be interoperable.

Therefore, some European law enforcement authorities have agreed on the "**Prum Treaty":**

Fully operational members:
Germany, Austria, Netherlands, Belgium, Spain, France, Luxembourg

Partially operational:
Italy, Finland, Slovenia, Portugal

Members, but not yet operational:
Hungary, Bulgaria, Romania, Greece, Sweden

The treaty is based on the general idea that every MS runs its own system under its own laws, whereas international data transfer is handled on contractual and technical standards basis. In fact, in June 2007 the European Justice and Home Affairs Council reached agreement about a Council Decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, incorporating in the framework of the Union important provisions of the Prüm Treaty dealing with police co-operation and information exchange on DNA-profiles, fingerprints and vehicle number-plates. These elements of the Prüm Treaty have now become part of the legislative framework of the European Union and will be implemented in all Member States.[17]

[17] EC press release on "The Integration of the "Prüm Treaty" into EU-legislation - Council decision on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime" http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803

The treaty sets legal, technical, quality and functional standards to achieve interoperability. Every member state is responsible for the collection of its own data (text and biometric) and assurance of minimum quality standards. Other entities such as Europol and Interpol can inquire to find matches under the treaty's limitations (e.g. number of inquiries per day to avoid that one country is flooded by inquires from others.)

Experience shows that automatic matching based on Prum technical standards and agreements works well with systems from different vendors. Biometric samples stored in the country in which they have been captured can be mutually inquired for matches, but their number per day has to be limited by agreements to avoid overloads.

There is no single encryption standard as the particular members apply (or do not) encryption according to their system. Data transfers are processed over the European **TESTA** (**Trans-European Services for Telematics between Administrations**) VPNetwork, which functions on European standards.

In parallel, large central databases (EURODAC, VIS, SIS II) are being implemented as well and are intended to be used by law enforcement, but they also introduce some challenges to be solved, such as the following:

- General problem with statistical database inquiries: in multilaterally used databases, false matching rates grow exponentially with the number of datasets. This means that searches by many different users will yield higher error rates as expected.
- There is no practical experience with statistical searches in multi-million record databases. Central databases create potential bottlenecks.
- A relevant challenge regards data that are already wrong, primarily mistyped or transliterated names.
- An upcoming challenge with increasing number of databases and functions is the number of different samples for the same individual, with very different qualities. This will especially apply to samples from surveillance devices, for which capture quality is not controllable.

The **perspective** being developed is **a bus-type topology**, comparable with an Ethernet. Such are also being developed in other pan-European areas like e-Government.

In a bus topology, all the applications in different organisations are lined up on one side, and all the resources (national and international databases) on the other. The interface bus handles the requests from the applications, translates them to the resources which could bring results and eventually hands them over. This concept raises many detail challenges, but experiences have been satisfying so far.

Typical features of AFIS systems:

- Multimodal, decentralised and historically grown data storage and access with long experience.
- Relevant number of authorised users, also with write access, managed according to Member States and supervised by very restricted protocol data.
- Clear but wide-range purposes: enhancing conventional law enforcement procedures with automated assistance, also in new areas like tracing stolen cars.
- Designed for public security objectives.
- Automation-assisted credentials for asylum fraud and crime prevention in respect to prosecution.

- Focus on data quality and therefore few wrong decisions, bad data subjected to be disposed.
- Persons in question can always be forced to enrol, backup enrolment procedures in place.
- Standards and procedures defined and agreed upon by multilateral treaty (Prum).
- Open discussion with data protection authorities starting from the design phase which leads to an overall stable consensus.
- Bottom-up approach with many interoperable features under a common user interface.

Challenges / open issues for AFIS systems:

- Integration of large central databases (VIS, SIS II) with possibly lower data quality and more concurrent authorised users.
- Increase of redundant samples/data for the same individual of different or uncontrollable qualities.
- Enhancing technical results of identification tasks like face recognition in public areas.
- Extension of Prum treaty to new members.
- Implementation of bus-type topology access concept.
- Data exchange issues with non-EU countries.
- Solving additional data protection issues coming along with new identification purposes.

Conclusion

Law enforcement currently is the first and only large-scale biometric application area, that is fully deployed and internationally used.

The successful implementation originates from a bottom-up and step-by step growth from independent national law enforcement systems which always had the perspective of further integrating of all necessary data. The Prum Treaty provides a legal and technical standard basis which is flexible enough to work efficiently under specific national laws but also allows automated international cooperation. Focus on data correctness and close cooperation with data protection authorities from the beginning has eased the treatment of conflicting issues in relation to security and data protection needs.

The most relevant challenge is the incorporation of more data concerning very large multi-purpose central databases.

2.1.2 Border control

Passports shall easily and quickly prove the identity and right of persons wanting to cross a border. To achieve this, they must be genuine, issued by trusted authorities and match the person in question. If the country of origin is not trusted or allowance of entry is subject to a decision, the traveller must present a **visa** issued by the destination country's embassy or consulate. It contains information about the applicant collected by the own means of the country – or the EU in general. Usually visas have more details included than the information in the passport. As documents, passports and visa are used for verification purposes.

Border control always had the intention to know whether entry of a person can be allowed without further action or if there is some special action or decision needed such as when

individuals are matched against watch lists of criminal suspects or when it is concluded that their entry has been previously refused. This is considered as an identification task.

Biometric information in passports primarily shall guarantee that the passport is valid and it can be subject to automatic match with biometric information gathered at the border. This could lead to automated border control (a scenario that will be discussed in following chapters of this report) in the future. (e.g. establishing unattended lanes at the entry point) However, a fallback procedure must be implemented to handle mismatches and automated border control stations ought to perform as quickly and efficiently as live officers would.

If the information matches and no further documents are needed, the person can pass. Otherwise intervention will be required. In this task, biometric data should enhance the travel document's quality and robustness against fakes. There is much potential in the identification task, but this does not exclude controversy. The first step was to incorporate machine-readable document data to be checked against electronic blacklists like the **Schengen Information System (SIS),** which is much more efficient than comparing the passport with separate paper blacklists. Using biometric data would make such checks resistant against fake passports because the individual is subject to comparison rather than the document. The primary intention is to prevent the same unwanted person trying to enter with different documents.

Another intention that requires effort resorting to conventional means is exit tracking for travellers with visas that have expiration dates. Biometric checks on visa holders at exit locations could improve the process of identifying those who have overstayed more than their allowed duration.

Fighting against terrorism and organised crime extend the ideas to use biometric data once they are stored for purposes such as creating travel profiles, which conflict with data protection and privacy issues.

Adding more databases for inquiry purposes and augmenting their corresponding functions will result in increasing processing times. If these potential adjustments cause lines at border control to get out of hand, citizens most likely will have even more complaints than they do today. Mass-tourism, which is a major portion of many European countries' economies, and convenience call for fast processing times.

Biometric passport issuance:

The EU directive requires that all EU Member States incorporate biometric photographs in all newly issued passports. By 2009, they also must contain two flat fingerprints. The biometrics are stored in an RFID chip on the passport and comply to EU and ICAO standards. Those standards define some technical qualities to allow facial recognition. It is noteworthy that the required age for the photograph is not specified.

Although EU passports must comply to the EU directive, there are many unregulated areas which have the potential for interoperability problems.

Some Member States are storing the biometrics in a central database while others do not or are not allowed to do so due to their national legislation. Italy is a prime example of this as *Il Garante*[18] (Italy's public data protection authority) forbids the storage of biometrics in a database.

[18] http://www.garanteprivacy.it

Some countries require the applicant to bring ICAO-compliant photographs; others have them taken by the authorities. Both options have their disadvantages. Having photos taken by an external professional can result in them being non-compliant and the applicant must show up again and repeat the process. Otherwise, the authorities must act as professional photographers (which, of course, they are not) and they must provide a suitable facility in the office with correct light conditions (as is done in Switzerland).

Some countries perform an immediate check after enrolment to understand whether the facial recognition works. Others tend to leave the applicants with their new passport without knowing whether all data is correct.

Overall, positive feedback regarding biometrics passports has been reported from the survey conducted for this study. The conclusion is that the systems function stably. However, this can be said only for the enrolment phase today because there are no EU border control systems deployed up to date.

Experiences with biometric passport issuance:

- In general our survey showed satisfactory results.
- Unregulated areas result in different procedures and technical characteristics in the particular Member States: some digital photos are taken by the authorities, elsewhere they must be provided by the applicants. Some countries offer immediate check of data correctness in the chip, others do not.
- An unresolved problem is capturing biometric data from photographs from small children – this can take up to 30 minutes per case.
- In some countries, biometric passports are mostly produced centrally for technology reasons, whereas conventional passports have been produced at the passport office and handed over immediately. Therefore, applicants have to wait longer and pay more than in the past.

ePassports updates – shift from Basic Access Control (BAC) to Extended Access Control (EAC)

The next 12 months should provide major developments in the ePassport systems. As the last Member States are complying with the ICAO standards and the Visa Waiver Programme decreed by the United States, the next required implementation processes have become the focus to meet the next mandatory VWP deadline. Fingerprints must be introduced into the passports by 2009.

Germany is the first EU Member State to have issued passports with both fingerprint and facial recognition. As of November 2007, all German citizens can request the fingerprint-integrated passports (See Section 2.2).

Specifically, 2008 will see the emergence of new and more sophisticated electronic passports across the globe, particularly in European Union (EU) countries. New information technology is emerging to better protect and verify the personal information contained in these documents.

The second generation of ePassports with fingerprint biometrics is one more tool that agencies can use in order to ensure that the person presenting a passport to a border guard is, in fact, the person represented on the travel document. Extended Access Control is the next set of certification scheme that will be used more than the previous Basic Access Control. through the use of strong encryption and PKI-based public/private key pairs to ensure impenetrable data transmission.

Visa Information System (VIS)

VIS is a future scenario to prevent illegal migration into the EU. At the time of publication of this report, news on the VIS has become an issue at the forefront both on political and social terms due to the increasing concerns of immigration and the millions of foreigners arriving from Asia, Africa and elsewhere. This document provides information on the status of this large-scale system as of November 2007.

The main purpose of the VIS is to improve the common (Schengen) visa policy by facilitating the exchange of information between EU Member States on short-stay visas. It will be based on a centralised architecture, with a central database where all information is stored and national interfaces located in the Member States allowing their competent authorities to access the central system. The system will lead to a huge collection and processing of personal and biometric data. Information on approximately 20 million visa applicants will be stored annually in the system and with a five year retention period; this could lead to no less than 70 million fingerprints data stored at any one time. **Therefore, the VIS will be the largest biometric database in the world when it is officially launched.**

Access to the system will be given to visa, immigration, asylum and border control authorities but also to member states' police and intelligence services as well as Europol for the specific purpose of fighting terrorism and serious crimes. **This means that VIS eventually will be a multi-purpose and multi-user scenario with dimensions and complexity unprecedented in Europe**.

Presently, two pilot systems serve to gather experience with biometric visa enrolment and check, with the overall objective to result as part of the EU-wide VIS:

- **BioDev I** (with 70.000 biometric visas) trialled the basic functions in French and Belgian consulates in different countries. (e.g. Congo but also in the U.S.).
- **BioDev II** includes seven EU countries and consulates that has also led to more challenges. For example, consulates will issue biometric visas on behalf of other EU destinations. It has become a general problem with EU visas that the traveller has the right to enter the EU at any EU border and can then travel anywhere within the EU.

With this concept, visa applicants must enrol with a digital facial image and 10 fingerprints at the consulates. The data is subject to storage in the VIS database which eventually will be online at every border control point in the EU.

A common Biometric Matching System (BMS) is being developed to arrive at the same result for a given visa at every border control point. The fingerprints can not be older than 48 months. Although there are problems experienced with juvenile fingerprints, currently there is no age limit defined and there is no relevant study available on this age-related issue

Experiences with BioDev I and II:

The recent mentality, that a particular Member State's consulate needs to take responsibility for the entire EU (Schengen) area has been reported to be working well. Few technical problems with enrolment devices are detected, but environmental problems were experienced such as the difficulty in taking digital photos of sufficient qualities over the counter. In addition, some consulate or embassy building designs are not feasible for biometric enrolment and need to be adapted accordingly.

The process also takes longer than in the past and produces long waiting lines. Children under the age of six, ill people and some VIPs had to be excluded as well. There were more people

with missing or damaged fingers than expected. Many VIPs do not accept the procedure and tried to interfere with help of local authorities.

There are several **benefits and drawbacks** expected from using **biometrics in the VIS**:

Benefits:
- facilitates a more thorough examination of visa applications,
- facilitates reliable identification and verification of travelers,
- can reduce visa fraud and illegal immigration,
- can contribute to internal security in general.

Drawbacks:
- significant financial costs,
- potential increases in the visa fees for applicants,
- significant impact in terms of convenience (e.g. no longer possible to obtain by travel agencies) for applicants, privacy and discussion about human rights.

Proposed border control scenario:

As announced by Frank Paul - Head of Unit of Large Scale IT Systems from the European Commission's Directorate-General for Justice, Freedom and Security[19] - in his keynote at the final conference in October 2007, there will be three forms of procedures of travellers at EU borders:

1) **EU citizens** will enter into check-in lanes presenting their biometric passports, and having their fingerprints taken. When those match with the passport, they may proceed.
2) **Third-country travellers carrying biometric visas** will enter into separate lanes and have their fingerprints taken. A check is made against the visa sticker in the passport and the VIS, where the data has been previously stored when they applied for their visa as well as blacklist-type data from SIS and others. When the official authorisation is granted, they may enter.
3) **Third country travellers who do not need visas** (for example US, Canadian, Australian citizens): For these candidates, a registered traveller program (as pilots are described in 2.1.3) has been announced but no details presented. However, generic conclusions can be made from the pilots and experiences in other countries like Canada.

Since very few information has been provided about the proposed Registered Traveller programme, some questions linger as to its functionality. Whereas the border control process aspects can be imagined as quite straightforward, there are still concerns for the enrolment process because this could potentially impose additional inconvenience and most likely extra costs for travellers:

- Who is responsible for enrolment?
- Where can travellers enrol?
- What checks (for example against VIS etc) are performed at enrolment?
- What type of biometric is to be used? (Some RTPs at Schiphol (Amsterdam), Frankfurt and Heathrow Airports and non-EU countries like Canada are using iris scan, but this is not used in this RTP related to the VIS.)
- What will enrolment costs be?

[19] http://ec.europa.eu/justice_home/index_en.htm

- How long will the registration be valid? Will there be a possibility to extend it quickly? (It is to be expected that some travellers will forget to renew it in time).

Many **organisational issues** should be kept in consideration:

- What will happen to families when one of their small children has a problem at the automatic border control point and the parents have already passed?
- How should mothers with babies enter lanes intended to isolate the individuals during the checking process?
- Problems affecting innocent families and children will not only be generally inhuman, but also produce very negative headlines in the media.

The scenarios are imaginable at large border control points such as at airports with well-trained personnel and sufficient infrastructure including technical assistance. The question remains: how will they work at **remote land borders** with many travellers arriving by bus or train and no technical service nearby?

Typical features of the proposed scenario:

- Once rolled out, VIS will be world's largest biometric database.
- Large number of authorised users, also with write access.
- Centralised top-down approach with many additional interoperable features.
- Concurrent purposes not defined in detail: verification of passport holders for entry/no entry decision identification of possible suspects assistance for law enforcement.
- Possibility for function-creeping such as itinerary tracing.
- Unpredictable data quality and therefore error rates.
- Unpredictable ability to correct or revoke wrong data because of multilateral implementation.
- Users are forced to enrol, low motivation to be assumed.
- Designed for generic security goals (preventing visa fraud, finding terrorists) but not effective in explaining the big picture to EU-citizens.

Challenges / open issues for automated border control:

- Many key features do not exist yet. For example, the Biometric Matching System, VIS and biometric SIS II are in pilot or development stages and automated border control stations are not implemented.
- Lack of experience with such large and complex databases with data from different sources in different qualities.
- A large proportion of users will have to be authorised to have access under different legal and technical environments for different purposes.
- Technical problems may arise when passports originating from unique issuers using different devices will be automatically checked at borders where it also can not be assumed that the same devices will be used for every control point.
- Lack of standardised testing and certification will even increase probability of such problems.
- Lack of legal and organisational solutions for small children, elderly people and individuals who are not able to enrol.
- Exit procedure for non-EU citizens is announced but no concept presented.

- Functionality for EU citizens (verification or identification, blacklist checks) hasn't yet been reported.
- Functionality for travellers from third countries without visa obligation (verification or identification, blacklist checks) not yet reported.
- Reported scenarios are designed for airports but not for remote land border control points.
- No decision or measures on outsourcing of processing tasks into third countries.
- Potential for function creeping.
- Potential for misuse and problems when biometric features would be checked by third countries.
- Investment risk when the Schengen border will be shifted further.

Conclusions

Biometric Passports and the Visa Information System will be crucial elements for the proposed Automated Border Control scenario. Biometric passports, which are already being issued but are still in ongoing development phases, can be described as a "large scale enrolment".

1) **We would like to highlight the challenges faced with the different procedures to obtain photos which could raise problems of inconsistent results due to a variety of issuing and checking devices.**
2) **Legal requirements are not coherent in EU Member States. Not all countries allow central storage for passport data.**
3) **The VIS will include the greatest biometric database in the world and part of a multi-purpose and multi-user information system, but almost no experience is available for such dimensions. In any case such a system will depend on trust in data quality and in the users.**
4) **The Automated Border Control Scenario discussed still leaves many open issues to be clarified such as the practical border control procedures and treatment of third-country citizens who do not require visas.**

2.1.3 Automated access control

Access control to premises and/or IT applications assisted by biometric information is an important and relatively straightforward field. Its generic purpose is to decide whether or not a particular person is authorised to gain access to a specific area. In these situations, it is not relevant to identify the individual. Therefore, biometrics need not to be stored, exchanged or matched with references in huge databases but very often are carried on the user's chipcard to be matched with the actual data captured at entry point.

Face recognition, fingerprint and iris scan are successfully used and due to relatively high quality of data enrolled, they are working with low error rates. An important driver for this is the fact that individuals are interested to be successfully enrolled and matched. Since mostly the number of enrolled users is relatively limited and data ownership is clear, procedures to correct faulty data can be implemented relatively easily. Usually, failure to enroll errors can

be recognized and handled in such controlled environments, however there are impacts on those not able to enrol, like people with injuries or manual workers with worn finger surfaces. For those that are unable to enrol, this would lead to inability to have access to do their job. However, problems with automated access control in general usually do not originate from the biometric system but rather from the organisation or the unattended and/or the surrounding uncontrolled environment. An example refers to access to bank-safe rooms with iris scan and a weight check to prevent two persons from simultaneous entry. This can make it impossible for mothers with little children to enter. However, from the few reported systems following this study's survey, satisfactory results are apparent. It even has been reported from an EU airport fast lane program that more than 90% of the users have renewed their membership although the cost is about €100.

Many systems have been developed bottom-up from existing technology; usually the biometric portion can be integrated easily in existing access-systems because the result is the same as in password/PIN or RFID-based solutions. ("access granted" or "access not granted"). As the security lies in the "Yes/No" decision, many systems are designed to offer convenience as well.

As long as personal data is not stored in databases or exchanged, since this is not necessary when the reference is carried on a card, the legal basis usually is an agreement between the party allowing access and the person wanting to receive it. In most cases a person is not forced to have access. This is a simple point, but opens many more subtle problems, because access to premises often is a prerequisite to do one's job; someone may feel forced to surrender personal data beyond privacy protection.

Most local access control systems are not designed to be multimodal and they are using the type of biometrics felt to be the most appropriate for the particular implementation. Often, overall cost is an important decision base and for the original purpose there is no or little need for interoperability.

For local access systems, managing large scale amounts of users is often not the prime challenge, the number of users normally can be handled (up to some 10.000). **Therefore experiences with these systems cannot be transferred to other systems with enormous databases designed for millions of users**.

Typical features (do not apply to systems integrated into others):

- Limited number of users per system,
- Often stand-alone system,
- Clear purpose: yes-or-no decision,
- High data quality, therefore low error rates,
- Personal data as a whole correctable and revocable because of local implementation,
- Users interested to enrol,
- Bottom-up concepts designed for convenience (replacing password or PIN based systems).

Challenges / open issues (for integration into a registered traveller program):

- Some characteristics shown above will not apply anymore,
- Proposed scenario has not been explained yet: verification or identification at entry point (identification could be checked perpetually since the pre-captured data always is available),

- Central storage or decentralised interoperable systems?
- Expiration period of data enrolled,
- Cost for the traveller,
- Enrolment facilities in third countries (could be airlines or travel agencies),
- Iris scan is used in some existing systems but not planned for border control, VIS and SIS II.

Conclusion

Existing Access Control Systems on biometric matches are limited to a clear purpose and require a minimum of data and therefore are reported to work satisfactorily and to be well-accepted. The intended purpose to use their concept for a registered traveller program implies interoperability at all possible entry points for which there is no experience from the pilot projects. Further, this implies the need to establish reliable and convenient enrolment facilities in many overseas countries.

2.2 Brief Overview per EU Member State

This section provides information concerning the specific relevant large scale biometric deployments in each of the EU Member States with details on the institutions, typology of biometrics technology, status of deployment (if available) and contact info.

These are results based on all relevant developments and updates up until the end of December 2007.

2.2.1 Methodology

As mentioned in Chapter 1, this study was supported by several tools to monitor large-scale biometrics deployment in Europe. Initially, a task of identification of stakeholders was carried out with the aim of uncovering all relevant systems either ongoing or in the planning stages.

This work was performed based on Internet research supported by a special content retrieving process involving intelligent agent technology. The online sources that were gathered range from biometrics portals, governmental institutions' websites, presentations, reports, databases, etc.

The ultimate goal was to identify the large scale biometrics systems in the EU Member States and to provide corresponding details of the systems and projects.

These results were enriched with information obtained thanks to the participation of experts at the Expert meeting in Brussels and the final conference in October 2007 that brought together speakers from various disciplines.

In addition some interviews were conducted that aimed to learn more about the target national biometric systems identified.

The task of receiving full information has been a challenging issue as sometimes it has been difficult to clearly understand the status of some of the ongoing or planned large scale biometrics systems. In fact, in some cases complete details as to the foreseen roll-out launch

dates, latest developments or improvements and system integrator information are not made available. In response to this, some further investigations were attempted by personal or phone contact, but collecting relevant information in this way turned out to be quite difficult.
For purposes of this study, there were several well-known websites in the biometrics field that were monitored frequently. The following table highlights the key sources that have been used often during the study in performing the online research task.

Name of biometrics website	Link	Brief description
Security Document World	http://www.securitydocumentworld.com	Constantly updated secure ID portal that frequently provides recent updates of the latest developments, opinions, publications, statistics, surveys on biometrics projects and systems.
Find Biometrics	http://www.findbiometrics.com	Biometrics-specific portal that categorises the information into application, technology, industry, etc. and disseminates fresh news relevant to biometrics, including press releases from industrial stakeholders and system issuing institution.
European Biometrics Portal	http://www.europeanbiometrics.info	European Commission supported biometrics online portal with sections on biometrics news, resources, events, market studies, EU Member States status in biometrics.
European Biometrics Forum	http://www.eubiometricsforum.com	Online resource for biometrics-related topics, led by CEO Max Snijder – contributor of said report and participant of this study's expert panel. Much emphasis is placed on the societal impact that biometrics has on EU citizens (privacy, security).
Secure ID News	http://www.secureidnews.com	Secure ID technology news site with frequently updated articles concerning all secure ID developments, including biometrics.

There are other online sources which have sprouted in the last few years with the intention of informing the public on happenings in the biometrics fields, but overall, the websites mentioned above are those most relevant where the most significant news on a European and international level are accessible.

Concerning another relevant source, this study kept in consideration the trend reports published by UNISYS for the European Biometrics Portal, especially the most recent edition, *Biometrics in Europe – Trend Report 2007* - released in June 2007.

2.2.2 EU country profiles

The following section provides an update to the most relevant large-scale biometrics deployments in the EU Member States. Information is primarily collected from Internet sources. The purpose of this list is to review which systems are in operation and those significant ones that are being planned. Therefore, this report does not go into full detail on the political implications regarding debates on the roll-outs. The original sources are provided where more information is given on political issues.

This study would also like to point out the analysis performed on national ID cards. Although it wasn't considered as one the major applications in the previous sections, the application has been included in the following country profiles since it has evolved as a significant issue. While this use of biometrics is often discussed, beyond use of biometrics at the border, there are very limited activities to use biometric verification elsewhere.

As of the end of 2007, recent studies show that out of 32 countries, 28 issue identity cards and only 7 are actually deploying their eID cards (Austria, Belgium, Estonia, Finland, Italy, Portugal and Spain). From this group, Italy, Spain and Portugal are the only countries that have announced that their roll-outs of their ID cards incorporate biometrics technology. Other Member States are proceeding with their eID card initiatives such as Germany and the United Kingdom which has been in the news recently with the debates and rumours of the potential implementation of its identity card initiative. Almost 50% of the Member States are in the process of designing eID cards for future roll-out.[20]

Lastly, since data protection is a major issue in practically all EU deployments, for full reference to the specific EU Member States DP commissioners, it is suggested to visit the following link which is part of the European Commission DG JLS website: http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm.

AUSTRIA

Having ranked at the top among all European countries in eGovernment,[21] Austria has demonstrated developments in large scale biometrics systems. However, data protection is always considered in roll-out plans as the importance of privacy is often kept in the debate during biometrics implementations.[22]

Austria met the October 2006 deadline conforming to ICAO and EU guidelines regarding the introduction of biometrics when its ePassport was rolled out in June 2006. The passports, which are produced by the Austrian state printers – Osterreichische Staatsdruckerei (OeSD contain an electronic chip with a facial scan and information about the holder.

Austria is also part of the Prum Treaty and has an AFIS implemented. For a full explanation about this system, see section 2.1.1.

---

[20] *Review and Analysis of Current and FutureEuropean e-ID Card Schemes* by Siddhartha Arora, M.Sc Thesis, Royal Holloway, University of London: http://www.porvoo12.net/MSc_Information_Security.pdf

[21] According to the results of Cap Gemini's 7th Annual EU Online Services Study released in Sept. 2007, Austria is considered the most advanced European country in online public service delivery achieving 100% against the criteria for the 20 services measured. The full report can be downloaded at here: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3634

[22] Austria Data Protection Commission (*Datenschutzkommission)* website: http://www.dsk.gv.at/

No biometrics is currently implemented into the Austrian Citizen Card, the country's national ID initiative.

Other developments/news
It has also been learned that Austria is participating to the EU Bio Dev II project (see 2.1.2) where Motorola has won the contract in April 2007 to provide the technology for the biometrics visa system.[23]

In November 2006, 3M ePassport Verification Systems have been chosen and installed at passport issuance locations throughout Austria. The 3M ePassport Verification System gives Austrian passport holders a means to personally check the electronic data stored on the new high-security passports the country began issuing in June.[24]

Austria overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Austria biometric passport	Osterreichische Staatsdruckerei (OeSD).	Fingerprint	OeSD (State's printing institution) 3M: Verification system	Passport	Operational	http://www.staatsdruckerei.at/oesd.html?lang=en Austrian Ministry of Interior (BMI): Dr. Heinrich Pawlicek: Head of Department III//16/b (Passports) heinrich.pawlicek@bmi.gv.at
AFIS	Ministry of Interior	Fingerprint; Facial Image DNA		AFIS	Operational	

BELGIUM

As of the end of 2007, Belgium results in two large scale biometrics systems in operation: the ePassport and the AFIS.

Belgium was one of the first EU Member States to have its biometrics passport available in accordance to the ICAO requests for the introduction of biometrics to passports. Despite some claims of cracking the passport in 2004, Belgium has been issuing biometric passports since June 2004 incorporating an electronic chip. During this first phase, in accordance with international agreements, the chip contains information such as the passport holder's identity,

[23] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1037
[24] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=826

signature and photograph, i.e. information which is visible to the naked eye on page 2 of the passport. During this initial phase, fingerprints are not yet included on the chip.[25]

Belgium is one of the fully operational members of the Prum Treaty (see 2.1.2) as Motorola Biometrics led the implementation of the AFIS for the Belgium Refugee Bureau. The system designed by Motorola using biometrics technology was installed at the Bureau's Brussels-based headquarters, and the results were immediate.

Some characteristics of the system, cited by Motorola:[26]

- Fingerprints are searched against the Asylum Agency's database to ensure the application is not being made under a false identity;
- The claimant is then photographed and issued with the necessary documents;
- Their information is stored in the agency's main database;
- The refugee is then free to leave the Bureau until their case has been reviewed;
- Once refugee status or Belgian nationality is approved, personal records are deleted from the Asylum Agency's database, which cannot be cross-referenced during criminal investigations under Belgian law;
- Failed applicants are held at the Centres for Illegals until deportation is arranged;
- Fingerprints can be captured, either in the field, or at the bureau and searched against the Asylum Agency's database in 60 seconds;
- Fingerprints are automatically forwarded in NIST file format to EURODAC under a fully-automated process that results in a 'Hit/No;
- Hit' message from EURODAC being returned rapidly to the Bureau's ADS.

Other developments/news:
Belgium is also participating to the BioDev II pilot project in coordination with the European Commission for biometrics visa implementation. Zetes was selected in June 2007 to design the system for the Belgium pilot. As of September 2007, Zetes has announced that they had already installs first operational installation at Belgian embassy in Kinshasa.[27]

The Belgium National ID card is currently operational. In November 2006, a press release stated that already 4 millions of citizens had an electronic ID.[28] By 2009, 8.2 millions electronic ID cards should replace the former ones. Non-Europeans living in Belgium could also receive one. *The current e-ID card however does not include biometrics*. According to the release, this could be the case with a new roll-out, for which Belgium could look for collaboration and standardisation with a pool of other Member States.

[25] http://www.diplomatie.be/en/travel/passportsdetail.asp?TEXTID=53991
[26] http://www.motorola.com/governmentandenterprise/contentdir/en_US/Files/ISD/Biometrics/Belgium_CS3.pdf
[27] http://www.zetes.com/en/fiches/corporate/media-centre/news/2007/070827-pilot-biodevii-kinshasa-pdf.cfm
[28] http://www.zdnet.fr/actualites/informatique/0,39040745,39364280,00.htm

Belgium overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Belgium biometric passport	Federal Public Service Foreign Affairs, Foreign Trade and Development Cooperation	Face Fingerprint (in later stage)	Oberthur Card Systems	Passport	Operational	http://www.diplomatie.be/en/travel/passportsdetail.asp?TEXTID=53991
AFIS	Belgium Refugee Bureau	Fingerprint	Motorola	AFIS	Operational	Case study document: http://www.motorola.com/governmentandenterprise/contentdir/en_US/Files/ISD/Biometrics/Belgium_CS3.pdf

BULGARIA

On 1 January 2007, the accession of Bulgaria to the European Union took place. The Bulgarian government had announced that a new generation of personal IDs will be issued from 31 October 2007. However, it was noted at the time that this expected launch date is quite optimistic as comments showed that the production of the cards will likely be time-consuming and expensive. The Swedish company, WISeKey, was in bidding for the tender at the time of the article.

The modernised eDocuments will look similar to the current Bulgarian identity card, but inside will carry biometric information in the shape of either a thumbprint or retina scan. They will also contain a unique digital certificate to be issued by the government. If an ID card is lost, its holder can ring a special number and cancel the certificate, using a personalised pin code.

The new card should improve security and should also speed up procedures at customs controls. Its use could be extended further, in future, to make it a general access document enabling on-line voting, payment of insurance and taxes, updating of health records and registration of property and cars.

Bulgaria overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Bulgaria eID card	Ministry of Interior Office for Personal Data Protection	Fingerprint Retina	Wisekey (in bidding for project)	ID card	Planned	

CZECH REPUBLIC

The Czech Republic doesn't appear to be very active in large scale biometrics system deployment. Besides the ePassport, there are no other relevant systems to report.

In September 2006, the Interior Minister declared the launching of Biometric passports. In October, Mrs. Radka Kovarova, the spokesperson of the Minister, stated that the delivery of the Biometric passports was a success in the whole country.[29]

A major landmark is about to happen concerning a significant border control procedures change. As of 31 December 2007 the Czech Republic will become one of several EU Member States to enter the Schengen system concerning land borders and it is required to be Schengen-ready by the end of March 2008.[30] Therefore, the intention is to eventually be ready for the VIS and SIS II system in the near future.

Czech Republic overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Czech Republic biometric passport	Ministry of Interior Office for Personal Data Protection	Face Fingerprint (in later stage)	Gemalto (former company Axalto originally led the implementation but was acquired by Gemalto) provides the Czech national printing agency Státní tiskárna cenin (STC) with the technology.	Passport	Operational	STC http://www.stc.cz/eng/kontakt/sidlo.htm

CYPRUS

There is no noteworthy available data concerning biometrics in Cyprus. On the government's official web site, there is no information on the English language pages which states anything about the implementation of biometrics passports. However, there was an online article published in December 2006 that referred to a roll-out of the Cyprus ePassports in June 2007 quoting an Interior Ministry spokeswoman.[31]

29 http://www.menara.ma/Infos/includes/detail.asp?article_id=11766&lmodule=Technologie
30 http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=998
31 http://www.cyprus-mail.com/news/main.php?id=29442&cat_id=1

DENMARK

The Danish National Police started issuing electronic Passports in October 2006. These new, secure ePassports, provided by digital security firm Gemalto, feature a polycarbonate data page containing a contactless microprocessor chip running the highly secure operating system. The chip not only features the information identity already laser-engraved on the first page, but also contains the passport holder's digitised photograph.[32]

Other relevant news/developments:
In September 2006, Danish Biometrics entered into an agreement with Copenhagen Hospital Corporation about testing, research and development on biometric recognition. The objective of the agreement is to result in solutions for secure log-on procedures when doctors and nurses for instance are entering the Electronic Patient Records (EPR) as part of their daily routines. An important part of the solution is intended to be the integration of biometrics into existing IT Architecture with Single Sign On (SSO) and demand for convergence.[33]

At the end of 2006, the Integration Ministry of Denmark and Sagem Defence Security signed a contract for providing a system capable to register biometric data of Visa applicants. This project is intended to take 4 years to be implemented and the information could be used in the VIS. The applicant's portrait may also come from scanned and digitized photos. The acquisition stations will be deployed in all Danish embassies.

Denmark overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Denmark biometric passport	Danish National Police	Face	Gemalto	Passport	Operational	http://www.politi.dk/en/servicemenu/home/
Denmark Visa	Integration Ministry of Denmark	Fingerprint	Sagem Defence Security	Visa	Pilot	http://www.sagem-ds.com/eng/site.php?spage=03010630

[32] http://www.secureidnews.com/news/2006/10/09/denmark-rolls-out-electronic-passports-based-on-gemalto-technology/
[33] http://www.danishbiometrics.org/news.php?id=48&rel=1&PHPSESSID=2ef42ac60ced480ccb8354ccfa0de5ca

ESTONIA

In a very short timeframe, Estonia has had to react quickly to implement its biometrics passport in compliance with the VISA Waiver Program. Estonia is one of many EU Member States that has chosen Gemalto to implement its e-passport system, which was announced by Estonia's Citizenship and Migration Board.

While in January 2007, Cognitec Systems announced another deal with IBM Estonia to provide facial recognition technology for the Estonian Ministry of Internal Affairs, Citizenship and Migration Board. According to the supplier, the technology will be used as part of a large ID management system, the country's ePassport project, which will see documents rolling out from March this year.[34]

In addition, it appears that the Estonian eID card, which is one of the 8 active eID initiatives, is planning to contain biometrics data as mentioned in a Porvoo conference in November 2006, although there is no further information that refers to these developments.

Estonia overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Estonia biometric passport	Ministry of Interior	Face Fingerprint (at later stage, approx. 2009)	Gemalto IBM Estonia, Cognitec: Face recognition	Passport	Operational	http://www.siseministeerium.ee/?id=17464&highlight=biometrics

FINLAND

It appears that Finland has only the biometrics passport and AFIS systems as their relevant large-scale biometrics projects in operation.

Regarding the ePassports, in July 2006, Finland's Ministry of the Interior assured in a statement that there were no security problems with the new passports to be introduced in August following come concerns related to security and privacy. "Finland's new passports meet all the requirements set for biometric passports.[35]

Concerning the developments in AFIS, Sagem Défense Sécurité signed a contract with the Finish Police to supply a new-generation AFIS. Apart from the standard AFIS police services (i.e. identifying criminals with latents, palmprints and fingerprints), it is said that the new system can also be used when issuing visas, passports and asylum ID.

The new system will acquire and process high-resolution images (1000 dpi) to ensure more reliable and accurate information. As part of the new contract, Sagem Défense Sécurité will supply Finnish police forces with and deploy high-resolution fingerprint and palmprint capture stations and latest-generation laboratory stations.

[34] http://www.cognitec-systems.de/press-releases/PR-Estonia.pdf

[35] http://www.bioxs.nl/go_web.php?id=622&link=1982

For quick and effective ID checks on the ground, and anywhere in the country, Sagem Défense Sécurité will also equip the Finnish police with its latest mobile biometric terminal – MorphoRapIDTM. Sagem Défense Sécurité will also deliver Digiscan Web stations, used to carry out biometric checks of the central database from regular workstations.

As concerns Finland's operation ID card, currently biometrics is part of the initiative.

Finland overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Finland biometric passport	Ministry of Interior	Face	SDU Segenmark Oy	Passport	Operational	http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/indexeng Email: biometria@poliisi.fi
AFIS	Finnish Police	Fingerprint	Sagem	AFIS	Planned	http://www.morpho.com/newsroom/NewsItem.asp?NewsID=49

FRANCE

France is one of the EU Member States that has demonstrated strong opposition to the entry of biometrics technology in large-scale projects. There have been many protests by pro-privacy groups, forums, political parties against the use of any kind of biometrics identifiers in these kinds of deployments. Data protection has been always been given high priority in ID documents.

As an example, the French Government launched an electronic ID card project called INES ('Identité Nationale Electronique Sécurisée', or 'Secure Electronic National Identity'), which was endorsed by the Prime Minister on 11 April 2005.

According to the government's initial plans, the future French eID card would have been fitted with a chip containing all identity information of the holder person, two biometric identifiers (facial image and probably fingerprints), and an electronic signature allowing secure access to both eGovernment and eBusiness services and transactions. Personal information contained in the cards would have also been stored in a new, common database, while biometric data would be anonymously stored in separate files. French citizens would have had to pay a fee for obtaining the new electronic document, which was planned to be mandatory.[36]

However, this bill which was supposed to have been presented in late 2006 received large opposition and a fierce debate ensued which led to the delay of the implementation.

Moreover, the French Data Protection Authority (Commission Nationale Informatique et libertés - CNIL) refused to give its approval, blocking completely every project involving

[36] http://www.epractice.eu/document/3350

biometrics which has been still the case leading into 2008. The current rule describes that the authorisation of CNIL is mandatory concerning any biometric technology integration in ID systems.[37]

Those relevant large-scale biometrics deployments that have been implemented correspond to the required biometrics passport and the "VISABIO" system both coordinated by the French Ministry of Interior.

The "PEGASE" (Experimental Programme for Secure Automated Access Control) pilot project tested for a 12-month period a biometric identity control system in the restricted personnel areas of Paris airports Charles de Gaulle and Orly, in cooperation with the French border police and the Ministry of the Interior.

Voluntary passengers registered with the border police, who collect their fingerprints and a set of personal information: name, surname, date and place of birth, address, nationality, and travel document details (number, expiry date, and type of document). These details are then stored both in a secure database and in a Pegase smart card, delivered to the enrolled passenger free of charge by Air France. The system is based on card and fingerprint readers, which check the passenger's identity before letting him or her cross the border through automatic doors.

The automated biometrics system was set up as a booth where users would apply 2 fingerprints to be authorised for entry. 10.000 users participated in the pilot project and the location of the biometrics data was stored in a database. (This is one of the 4 automated biometric border crossing systems for registered travellers that were assessed at four European airports as part of the BIOPASS study led by Frontex., the EU agency based in Warsaw, which was created as a specialised and independent body tasked to coordinate the operational cooperation between Member States in the field of border security.)

The French Ministry of Interior has decided to require all visa applicants to be issued an electronic portrait that includes prints of all 10 fingers, and a photograph: the "VISABIO" project. Sagem Sécurité is a coordinator of the Visabio project, a biometric visa issued by France to foreigners entering the Schengen area. This project has been approved by CNIL.

Other developments/news:

Sept 2007
It was announced that Air France is launching two new trials of biometric for the passenger boarding procedures.The airline has announced a "Hubway self-boarding trial" to fast-track selected passengers on its Paris-Amsterdam route. This trial, which was set to launch before the end of 2007, will make it able for passengers to load a record of their fingerprint on to a chip card. Using dedicated scanners and check-in lanes, the volunteers will be able to print out their own boarding pass, clear security and board the plane via electronic gates that will check their fingerprint with the one stored on the card. The scheme is planned to be trialed for two months among 1,000 Air France staff and will later be extended to some 2,000 frequent flyers on the same route.[38]

[37] In January 2007, CNIL made an official ruling on biometrics-related issues. For more information, visit this link http://www.cnil.fr/index.php?id=2166&news[uid]=421&cHash=2bd711454d (French language)

[38] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1130

France overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
VISABIO	Ministry of Interior	Face Fingerprint	SAGEM DS	Visa	Pilot	www.interieur.gouv.fr
France biometric passport	Ministry of Interior	Face Fingerprint (later)	Gemalto	Passport	Operational	www.interieur.gouv.fr
"PEGASE"	Aeroports de Paris (ADP) Air France	2 Fingerprints	SAGEM	Airport access	Pilot (tested for 12 months from May 2005 – June 2006)	www.interieur.gouv.fr

GERMANY

Germany is the first EU Member State to fulfil all the requirements of EC regulation regarding passports as it has completed fingerprint implementation into the documents. As of 1 November 2007, German citizens are able to receive the second-generation electronic passports. Each passport chip will now include two fingerprints as biometric identifiers.

Federal Minister of the Interior Wolfgang Schäuble said of the new passports: "Each individual's fingerprints are unique. This technology will help us keep one step ahead of criminals. We want to make it impossible to enter the Schengen area using a counterfeit passport. With the new passport, it is possible to conduct biometric checks, which will also prevent authentic passports from being misused by unauthorized persons who happen to look like the person in the passport photo. And German citizens will benefit from the new application process: All applications will be submitted and sent to the passport producer in electronic form, which will reduce processing times. Following nation-wide testing, the federal, state and local governments are ready to start using the new procedures."[39]

Starting on 1 November, persons applying for a passport will need to place two fingers (usually the index fingers) briefly on an electronic recording device, a scanner. The fingerprints will then be sent with the passport application data to the passport producer, the Bundesdruckerei GmbH, where they will be stored on the passport chip. It has been expressed by the German Federal Government. For this reason, the Federal Office for Information Security (BSI) supervised the development of standards for capturing and transmitting the fingerprints. The data are also securely stored on the chip. Only selected authorities will have access to these data. The fingerprints in particular are protected against 'skimming', or unauthorized access; Germany worked hard to ensure such protection at European level. The only countries that will have access to the fingerprints stored in the electronic passports of German citizens are those with special authorization certificates from the Federal Republic for their scanners.

[39] http://www.bmi.bund.de/cln_012/nn_769658/Internet/Content/Nachrichten/Pressemitteilungen/2007/10/Ankuendigung__E-Pass__en.html

The national legal foundation for all of the new features is provided by the amended Passport Act, passed by the Bundesrat in July 2007, and the related regulations. Apart from the introduction of fingerprints, the amended legislation covers further changes concerning passports and registration effective 1 November 2007, such as changes in the validity period for children's passports. However, there is no need to make an extra trip to the passport office: All passports already issued will remain valid until their original date of expiry. And the passport fees have not changed.

Aside from the second-generation passports, and besides the iris-scanning trial at Frankfurt Airport that took place in 2004, other examples of large-scale biometrics projects are a pilot at a train station in Mainz utilising face recognition as a tool for search in law enforcement. In this case, the system was used for identification and not verification purposes.

Germany overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Germany biometric passport	Federal Office for Information Security (BSI)	Face Fingerprint	Bundesdruckerei GmbH	Passport	Operational (Note: "second generation" available from Nov. 2007	http://www.bmi.bund.de/cln_012/nn_1176866/Internet/Navigation/EN/Topics/Travel__ID__Documents/Electronic__Passport/Electronic__Passport__node.html__nnn=true
"Ausländerzentralregister (AZR)" The system (originating from 1953) includes biometric data (face picture of visa applicants) since Oct. 2003. The system shall contain face pictures of resident aliens in the near future.	BSI Federal Office for Migration and Refugees	Face	EDS Dortmund	VISA, asylum seeking initiatives	Operational	www.bamf.de
Electronic office ID card for Germany's federal authorities	Federal Criminal Police Office (BKA) and (BSI).	Unclear as to which biometrics are implemented	Bundesdruckerei GmbH	ID card	Pilot	http://www.bmi.bund.de/cln_012/nn_1176934/Internet/Content/Themen/Travel__ID__Documents/el__Dienstausweis__en.html
Biometric border control system based on iris scanning at **Frankfurt airport.**	Bundespolizei (Federal Police)	Iris	OKI	Airport Automated Border Control	Pilot (initiated in Feb 2004, completed in Aug. 2007)	http://www.bundespolizei.de/nn_719704/EN/__Home/AutomatedBorderControls/abc__node.html?__nnn=true

GREECE

There is currently no central e-identification infrastructure for eGovernment in Greece. In particular, no plans for e-ID cards have been issued. In the Public Administration context though, there is currently a large-scale project under implementation, namely the National Authentication System. Concerning biometrics, the only known large scale biometrics deployment is with the Greek biometrics passport which is coordinated by the Ministry of Public Order (Hellenic Police).

Greece overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Greece biometric passport	Ministry of Public Order (Hellenic Police)	Face Fingerprint (later)	Toppan (using ASK technology)	Passport	Operational	Hellenic National Passport Centre http://www.passport.gov.gr/index.php?mylang=english

HUNGARY

Hungary started issuing its biometric passports in August 2006. By the time of publication of this report, Hungary is preparing as one of the 8 EU Member States that acceded to the EU in 2004 to join the Schengen area states. This will mean that as of 21 December 2007, Hungary will have border controls lifted along stretches of the Hungarian-Slovenian, Hungarian-Austrian and Hungarian-Slovak border, whilst border, customs and finance guards will continue to operate along the Ukrainian, Romanian, Serbian and Croatian border.[40]

All members of the Schengen area must provide data to the Schengen Information System (SIS), which was set up to enable police and customs officers to track suspicious people, vehicles and goods. No other information is available on relevant large-scale biometrics projects in Hungary.

Hungary overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Hungary biometric passport	Central Data Processing, Registration and Election Office	Face Fingerprint (later)		Passport	Operational	http://www.nyilvantarto.hu/kekkh/kozos/index.php?k=csca_hu

[40] See: http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1222

IRELAND

Recently announced in November 2007, Ireland has launched the first phase of its new Automated Fingerprint Identification System (AFIS) for its national police force, the An Garda Síochána, and the Irish Naturalisation and Immigration Service (INIS).[41]

During this phase, LiveScan electronic fingerprint capture equipment will be installed at the Office of the Refugee Applications Commissioner. This will allow fingerprint data from those seeking asylum to be captured and exchanged with EURODAC, the central EU fingerprint database.

In subsequent phases, which will be rolled out during 2008, individual's fingerprints will be captured and stored when they register with the Garda National Immigration Bureau (GNIB). This will also allow immigration authorities to capture and store fingerprints at points of entry including sea and air ports. The new system will be fully integrated with the Garda PULSE system and the GNIB information system in 2008.

An international consortium, including Accenture, Motorola and Daon Biometric Systems, was commissioned to design and implement this new integrated electronic fingerprint system, or automated fingerprint identification system (AFIS), for use by police and immigration services.

Regarding Ireland's electronic passport, in October 2006, the Irish government started issuing RFID passports with biometric data that can be read at a distance to comply with US regulations for its visa waiver programme. At the time there were some concerns about the security features for skimming purposes. Unlike the RFID passports the USA is now issuing, the Irish ones lack a security feature preventing them from being skimmed, or read surreptitiously.[42]

Also, the Department of Justice, Equality & Law Reform has awarded Siemens Business Services a contract to roll out an automated Visa application and tracking system for foreign nationals seeking to enter Ireland. With a huge increase in visa applications in recent years, according to the Department of Justice, Siemens has developed a streamlined electronic visa application system for the first time in Ireland. According to the Department of Justice, Equality and Law Reform, the critical balance in the visa system is between providing a fast and friendly service for legitimate travellers while at the same time, ensuring that fraudulent applications are recognised and handled appropriately. This system will be able to provide a full audit trail of the visa application process demonstrating accountability. Before now all visa applications were non-automated.[43]

Another major development related to Irish biometrics deployment occurred in December 2007 when the EU court declared that UK and Ireland cannot adopt certain Schengen measures relating to biometrics in passports.

The EU's highest court ruled that the European Council was correct not to allow the UK and Ireland to adopt new Schengen agreement regulations establishing standards for security features and biometrics in passports. The Court of Justice said the UK and Ireland can only

41 http://www.securitydocumentworld.com/public/index.cfm?&m1=c_10&m2=c_4&m3=e_0&m4=e_0&subItemID=1199
42 http://www.theregister.co.uk/2006/10/23/smart_chips_for_smart_crooks/
43 http://www.daon.com/news/2006/14_03_2006_daon_DOJ.html

adopt new measures related to the agreement in areas where the two countries are already authorised to do so. The UK and Ireland are not bound by the Schengen agreement, by which member states agreed to gradually remove controls at their common borders and introduce freedom of movement.[44]

Ireland overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
AFIS for its national police force, the An Garda Síochána, and the Irish Naturalisation and Immigration Service (INIS).	Irish Naturalisation and Immigration Service and Ireland's National Police Service (An Garda Siochana),	Fingerprint	An international consortium, including Accenture, Motorola and Daon Biometric Systems	AFIS/VISA	Operational (launched 1st phase as of 28 Nov 2007)	
Ireland biometric passport	Irish Department of Foreign Affairs	Face Fingerprint (later)	De La Rue Smurfit	Passport	Operational	
Automated visa application and tracking system for foreign nationals seeking to enter Ireland	Irish Department of Justice, Equality & Law Reform	Fingerprint	Siemens Business Services (SBS)	VISA	Planned	

ITALY

Italy is of the more active EU Members in large scale biometrics deployment arising from the public sector. Despite the intentions to roll out several projects, however, there have been some instances of concerns from the national Data Protection Authority (il Garante) which have led to decrees made to provide strict guidelines on procedures for developing the biometric systems.

The large-scale biometrics projects in Italy are generally categorised into two application areas:

- Civil identification
- Physical and logical access control

Regarding *civil identification,* the following relevant large scale systems are hereby listed with the date of initiation in parenthesis:

[44] http://www.secureidnews.com/news/2007/12/18/eu-court-agrees-that-uk-and-ireland-cannot-adopt-certain-schengen-measures-relating-to-biometrics-in-passports/

- AFIS (1994)
- Electronic ID card (2000)
- Electronic residence permit card (2004)
- Biometrics ePassport (2006)

For the purposes of this report, we will focus on the ID card, residence permit card and the Italian ePassport as the AFIS has been in operation for over a decade and the Visas are in relation to the developments that are ongoing with the EU VIS, which has been discussed in previous sections in this report.

Electronic ID card (Carta di Identità Elettronica)
The CIE is the only EU eID card that actually integrates biometrics in the system. Two fingerprint templates are stored in an IC-Chip with microprocessor. The embedded chip will be used to allow remote network authentication and telematic service usage. Even though it is reported by Italian public authorities that 2 million cards have been issued by the municipalities, the full roll-out of the cards appear to have stalled due to lack of funding to support the initiative. In fact, a January 2008 call for tenders has been released which sets a bid for equipment to produce the cards.

In addition, the deployment has been faced with several decisions by the Data Protection Authority that has potentially thwarted its development. For example, in August 2007, the authority decided that a contactless chip is optional and the holder's consent is required for data reading. The more significant decisions declared that biometrics data must be protected and can only be used for identification purposes and the data can not be stored in a central database.
2008 will be a crucial year for the continued roll-out of the CIE as also the unstable political status could have a large effect on the timing and the political support given to the initiative.

Electronic residence permit card (Permesso Soggiorno Elettronico)
The PSE, which is issued by the Ministry of the Interior, is available to Italy regular foreign residents that are non-EU citizens. It follows the same hybrid optical/IC chip card technology specification as the CIE. Again the Data Protection Authority has made several decrees including that the European Regulation EC 1030/2002 doesn't provide for the use of biometric data in the residence permit. In addition, biometric data can be used only during the card issuing process.

In 2006 the European Data Protection supervisor recognised the advantages of the use of biometrics and Ministry of the Interior started to store fingerprint data in the residence permit. However, due to the enormous project that the Italian public authorities had to manage based on the large increase in requests from residence permit applicants, the issuing of these cards has had some delays.

Biometrics ePassport
Since October 26 2006, the Italian e-passport is the only typology of passport issued in Italy, which also received full approval from the Data Protection Authority. The DPA also made the following points: biometric data must be protected and can be used only to verify the identity of passport holder and the "passport database" is hosted by Ministry of Interior without biometric data. CNIPA is currently testing the acquisition devices and the tools for quality control. Some security and privacy concerns have been expressed as being the potential for unauthorized reading, interception of transmitted data and counterfeiting by "cloning."

Regarding *physical and logical access control,* which has been regarded as a prioritised application for Italian large-scale biometrics deployment, the following relevant large scale systems are hereby listed with the date of initiation in parenthesis:

- Ministry of Defence "Multi-services" Card (2003)
- Ministry of Justice "Multi-services" Card (2006)

The development of the above multi-service cards has followed the consensus that the combination of a smart card, certificate (i.e. a standardised electronic identity issued and signed by a neutral party to link an electronic signature with a person) and biometrics is the best solution regarding identification and authentication. It has also been considered as the most expensive solution, but should lose

Ministry of Defence "Multi-services" Card and Ministry of Justice "Multi-services" Card
Both of these ID cards have the same characteristics. A smart card is either used for justice or military personnel for access into an authorised area. There are digital certificates for online authentication and digital signature, which is PIN or biometric protected. Two fingerprint templates are integrated to the cards. The Italian DPA has approved these projects while making specific regulations. Moreover, fingerprint templates can only control the access to sensitive data. Biometrics can not be used can't be used for employees attendance control and the data is prohibited from being stored in a database.

Italy overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Italy biometric passport	Ministry of Interior	Face Fingerprint (later)	Cogent	Passport	Operational	www.interno.it
Carta di Identità Elettronica (CIE)		2 fingerprints		ID card	Operational	
"System of Secure access to the Information Technologies of the Ministry of Justice"	Ministry of Justice	Fingerprint	IPZS - State Printing Office /SIEMENS Informatica S.p.A.	ID card	Planned	www.giustizia.it
Carta di Difesa	Ministry of Defence	Fingerprint	Siemens	ID card	Planned	
AFIS	Ministry of Interior and Criminal Police	Fingerprint	Cogent Systems	AFIS	Operational	
Permesso Soggiorno Elettronico (PSE) – Italian Work Permit	Ministry of Interior	Facial image Fingerprint	Hewitt Packard Finsiel Siemens Informatica	Visa/Work Permit	Operational	

LATVIA

As far as Latvia goes, the only relevant known large-scale biometrics deployment is the ePassport. The roll-out of the ePassports initiated in November 2007 with Giesecke & Devrient (G&D) as main integrator for the Latvian government as part of a five-year deal involving 1.1 million documents.

G&D is responsible for systems integration from data capture to document personalisation. Initially, the ePassport chip which runs on G&D's StarCos smart card operating system will store the digital passport photo as a biometric feature for facial recognition. In 2008, two fingerprints of each document holder will also be stored in the chip.[45]

Latvia overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Latvia biometric passport	Office of Citizenship and Migration Affairs	Face Fingerprint (index fingers of the right and left hand) (beginning in the middle of 2008)	Giesecke & Devrient (G&D) Gemalto	Passport	Operational (as of 28 Nov. 2007)	http://www.ocma.gov.lv/?_p=505&menu__id=13

LITHUANIA

In December 2006, the Ministry of the Interior of Lithuania, BIS Bundesdruckerei International Services GmbH developed a sticker for biometric passports. Bundesdruckerei GmbH is the supplier of the corresponding electronic personalisation system which will allow an upgrade of the Lithuanian passport system. The Ministry of Interior has begun to issue the ePassports and the full roll-out of new Lithuanian Passports following the 'EU model' (cherry-coloured cover with the inscription EUROPOS SĄJUNGA - European Union - and digital passport sign) will commence on 2 January 2008.[46]

In other relevant news, UK-based ePassport reader manufacturer Rochford Thompson has won a €1.8m contract to provide passport scanners for use in Lithuania. The supplier says the document readers will be used at border control points and also by police, immigration and Ministry of Foreign Affairs officials.[47]

Lithuanian integrator AIDETA – a subsidiary company of ORDI - was commissioned to provide enhanced security technology for Lithuanian border guards as part of the country's process of integration with the 15 other Schengen members. No other large-scale biometrics deployment is reported for Lithuania.

---

45 http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1200

46 http://www.epractice.eu/document/3413

47 http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1023

Lithuania overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Identity documents issuance system (ADIS)	Ministry of Interior	Face	Bundesdruckerei GmbH	Passport	Operational	www.vrm.lt www.dokumentai.lt

LUXEMBOURG

Luxembourg is one of the participating countries partaking in the BioDev II project. It appears that Motorola will lead the implementation concerning the Luxembourg. As mentioned in previous sections, the aim of BioDev II is to develop customised biometric enrolment solutions for each of the participating EU member states, and to integrate them with their existing national visa processing systems to test interoperability.

Besides the ePassport systems, which were in operation in August 2006, there are no other large-scale biometrics deployments to report.

Luxembourg overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Luxembourg biometric passport	Ministry of External Affairs	Face Finger (later)	Bundesdruckerei	Passport	Operational	http://www.mae.lu/mae.taf?IdNav=334

MALTA

Ministry for Investments, Industry and Information Technology (MIIIT) is in the process of project managing, for the Ministry of Justice and Home Affairs, the procurement of a Strategic Partnership for National Identity Management Systems (NIDMS). The NIDMS will be used for core identity management processes including the issuance of electronic identity cards (e-ID Card), ePassports and biometric visas. It will also form part of the border checkpoint control systems and the systems for the registration of third country nationals. The e-ID Card will mark the fourth level of the e-ID and thus provide each person in Malta with a secure way of conducting e-Government, of signing electronic documents and of authenticating oneself in the digital world. Most importantly, however, it will be developing a national electronic register of persons which will be populated during the registration process for the e-ID Card.[48]

[48] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=961

In November 2006, the British High Commission issued its first biometric visa to a non-EU citizen wishing to travel to the United Kingdom on Wednesday. The British High Commission has been the first foreign representative office in Malta to issue visas using biometric technology. This state-of-the-art system has for purpose to recognize applicants' fingerprints using an electronic scanner, before sending them to a central database for cross-checking against previous applications.

Despite Malta's many ID management initiatives, no other relevant large scale deployments that incorporate biometrics are known.

Malta overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Malta biometric passport		Face		Passport	Planned	http://www.passaporti.gov.mt/mainpage.asp

THE NETHERLANDS

Prior to 2004, there were many biometric trials that were tested regarding large scale deployments. Some examples have involved municipalities, schools and Registered Traveller Programs.

In fact, one of the most relevant large-scale programs in Europe that is still in operation is the PRIVIUM program. Privium was introduced on in October 2001 as a pilot project incorporating iris scan technology. During the first year, the iris scan was run as a pilot project. The following year, the Ministry of Justice and the Koninklijke Marechaussee stated that the pilot period had shown that the iris scan technology satisfied all the security requirements. This was the official go-ahead for Privium.

The technology used in the iris scan is based on the recognition of specific characteristics of the iris.

When a passenger registers to the program, scans are made of both the left and the right eye. According to Privium, the scans do not cause any irritation to the eyes and do not pose any health risks. The iris scan is not hampered by glasses, contact lenses or coloured lenses. The only time it does not work is when you wear sunglasses.

After the scan, the iris details are only stored on the chip of the Privium Card and not in a database. After a passenger crosses the border, the data is removed from the equipment immediately.

The iris recognition process at Schiphol does not make use of existing equipment. The iris scan was designed by Amsterdam Airport Schiphol according to its own specifications. The required software was developed in close co-operation with the Immigration and

Naturalisation Department (IND) and the Koninklijke Marechaussee Schiphol (Airport Police).[49]
Aside from the PRIVUM program, the Netherlands launched its Dutch ePassport with a chip containing biometric data of the holder in accordance to the EU and U.S. regulations.

Dutch authorities have made the entire application process more transparent towards their citizens. Following a decision by the government to install ePassport scanners in municipal offices throughout the Netherlands, Dutch citizens can get easy access to the data stored on their new ePassports.

Citizens can apply for an ePassport at any one of around 600 municipal offices across the country. The data contained in the application is then sent to SDU – the former Dutch state printer, which is now a developer and manager of ID documents – for the ePassport to be produced.

After printing, the document is sent back to the municipal office, where the applicant can collect it. On collection, applicants will be able to use an on-site ePassport scanner to check the data stored on the ePassport's chip.

The core technology which allows this to happen was developed by Rochford Thompson, and has now been installed in around 25 municipal offices in the country.[50]

The Netherlands overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Privium Automated Border Passage	Immigration and Naturalisation Department (IND) and the Koninklijke Marechaussee Schiphol (Airport Police)	Iris	Dartagnan (system integrator) Iris: LG, Card: Gemalto, Gates: Boon Edam, etc.	Registered Traveller Programme	Operational	www.privium.com
Netherlands biometric passport	Dutch Ministry of the Interior and Kingdom Relations	Face Fingerprint (later)	SDU Datecard Group Collis Rochford Thompson (scanners)	Passport	Operational	http://www.paspoortinformatie.nl/content.jsp?objectid=4804

[49] http://www.schiphol.nl/privium/privium.jsp
[50] See: http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=888

POLAND

In compliance with the European Union recommendations, Poland started issuing electronic passports for its citizens by the end of August 2006 and officially launched the introduction of its biometrics passports in October of that year. Previously, a successful pilot phase including over 3 000 diplomatic e-passports took place, confirming Gemalto as the main supplier for the global roll out handled by the Polish Ministry of Interior and Administration.

In related news, Poland became one of several Member States to join the EU's border-free area by joining the Schengen zone at the end of December 2007.

Poland overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Poland biometric passport	Ministry of Interior and Administration	Face	Gemalto	Passport	Operational	

PORTUGAL

Portugal is one of the few EU Member States that have an eID card that claims to have biometrics implemented.

The Citizen's Card, is the Portuguese electronic identity card (eID). The card was officially unveiled on February 2007 and the authorities plan to make it available throughout Portugal by 2008. The Citizen's Card is a smart card that provides visual identity authentication with increased security and electronic identity authentication with biometrics (photo and finger print) and electronic signatures. The development of the Citizen's Card is part of the Government's plan to simplify the administration and modernize the public services. It will replace five presently existing cards - Identification Document, Tax Payer's Card, Social Security Card, Voter's Card, Health System Card - and will allow for multi-channel identity authentication, namely in presence, through the Internet, or by telephone (with one-time passwords generated with the card), thus allowing the citizen to identify himself electronically and dispose of a legally valid electronic signature from a distance contributing to the deployment of customer-oriented advanced public services. The project is now in its fourth phase (development and implementation of solutions) and the authorities plan to make it available throughout Portugal by 2008.[51]

Regarding Portugal's ePassport, it was issued in August 2006 and is fully compliant with both EU and U.S. standards. For complete information, the in-depth official website is available at http://www.pep.pt.

Portugal has also demonstrated some biometrics-integrated innovative large-scale systems with the project RAPID (Automatic Identification of Passengers Holding Travelling Documents).

[51] http://www.cartaodocidadao.pt

According to its official website, RAPID is a worldwide innovating system that allows an automatic control of passengers in possession of electronic passports, thus eliminating the need for human action. This system combines the operations of reading and checking electronic passports with an innovating feature for assessing biometric data which operates an automatic gate opening device. This device checks on a first phase the genuineness of electronic passports and validates all data stored in the chip and, on a second phase, appraises the passenger's identification by establishing a comparison between the photo stored in the chip and the information of the passenger in loco, automatically opening the border gate when the features of both images are coincident. RAPID was made secure by an intelligent system that allows the entry of one single passenger each time and automatically adjusts the reading camera to his / her height. This innovating system will permit a highly rationalized management and a significant boost to the efficiency of means at border control. By reducing the process of border crossing to an average of less than 20 seconds it will speed up the movement of passengers at border control significantly. After May 25, Faro Airport will be equipped with ten of these units, which will be evaluated by a group of experts / researchers of Algarve University up to the end of June.[52]

Portugal overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Portugal biometric passport	Serviços de Estrangeiros e Fronteira	Face Fingerprint (later)	Vision Box Gemalto Muhlbauer: personalisation	Passport	Operational	www.pep.pt
Citizen's Card (Cartão de Cidadão)		Fingerprint	Gemalto	ID card	Pilot ("development and implementation phase")	http://www.cartaodocidadao.pt
RAPID (Automatic Identification of Passengers Holding Travelling Documents)	SEF - Serviço de Estrangeiros e Fronteiras	Facial recognition	Vision Box	Passport	Pilot	http://www.rapid.sef.pt/

ROMANIA

Romania officially became an EU Member State in 2007. In June 2007, the Romanian government issued an open tender for the manufacture and delivery of ePassports, as well as of related equipment and software. The contract is for the supply of a minimum of 2,085,000 blank ePassports, with the possibility of extending this to 10 million. It also includes the supply and installation of hardware and software for reading biometric and chip data, hardware and software for the national computerised ePassports system, personalisation equipment, software and hardware for connecting the ePassport system to the government's communications system, as well as training, maintenance and support. The government

[52] For more information, visit RAPID's official website at: http://www.rapid.sef.pt/.

estimates that, excluding VAT, the contract is worth 65,000,000 – 75,000,000 euro, and says it will run for 48 months.[53]

Prior to this tender, in September 2006, according the Romanian Interior Affairs Ministry, the Biometric passports were intended to be introduced at the beginning of 2007.

Romania overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Romania biometric passport	Ministry of Interior			Passport	In auction	

SLOVAKIA

As of December 2007, there is currently no central eIdentification infrastructure in Slovakia, but the Government has plans to introduce high-tech ID cards and passports, which will most likely feature one or more biometric identifiers. Electronic ID cards will incorporate advanced electronic signatures, which are required by the Act on Electronic Signatures for communication with government bodies. Slovakia has already transposed the European Directive on Electronic Signatures by the law on eSignatures, which entered into force in May 2002. The definition of accreditation schema to guarantee interoperability of electronic signatures, the accreditation of certification authorities (CA), and the confirmation of certified technical devices and software tools for use with government bodies falls under the responsibility of the National Security Authority (NBU). So far, the use of eSignatures by public sector bodies remains limited. Currently, there are two systems for issuing and holding unique personal identifiers in Slovakia.[54]

The rollout of the Slovak ePassports is expected for the beginning of January 2008.

Slovakia overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Slovakian Biometrics Passport	Min. of Interior	Face Fingerprint (later)		Passport	Planned (roll-out set for Jan. 2008)	http://www.spectator.sk/articles/view/29258/ http://www.minv.sk/

[53] http://www.securitydocumentworld.com/public/news.cfm?m1=c_11&m2=e_0&m3=e_0&m4=e_0&subItemID=1027
[54] http://www.epractice.eu/document/3467

SLOVENIA

At the end of August 2006, Slovenia started issuing its new biometric passports, featuring a biometric facial scan, and in accordance with EU Regulations requiring all Member States to include facial scans. Besides this ePassport deployment there are no other large-scale biometrics projects to report.

Slovenia overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Slovenia Biometrics Passport	Min. of Interior	Face	Muehlbauer (personalization equipment) in partnership with Cetis (printing company) Gemalto (polycarbonate devices) & NXP Semiprocessors (chip)	Passport	Operational	http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SOJ/pdf/Biometricni_PL_SSJ_an.pdf

SPAIN

Spain is another EU Member State that claims to plan to include biometrics identifiers in its eID card. In July 2006, Spain's national printing office contracted Sagem Défense Sécurité to provide its biometric software licences for use in its new national electronic ID card, DNI-e. The software matches the DNI-e holder's fingerprints with those securely stored in the chip. According to the company, "this allows the identity of the DNI-e holder to be checked while ensuring the confidentiality of the biometric data"

Rollout of Spain's eID cards is continuing apace following the country's successful deployment of the first million cards. Reports have communicated that during the second half of 2007, cards are to be issued to citizens of Madrid, Catalonia and Murcia. The government aims to have issued 2 million cards by the end of 2007 and to have issued 5 million by the end of 2008. The Interior Ministry, which is responsible for deployment of the cards, says the documents are designed to guarantee maximum security and privacy for citizens, while ensuring convenience and ease of use.[55]

The biometric data are, it says, available "only to the citizen" plus, in secure surroundings, to "a few service terminals in the eID card issuing offices". In addition to electronic security measures, the card itself is "a document which, physically, contains numerous security elements". A website and helplines are available for people who have any questions about the cards.

Regarding the Spanish ePassport, Spain Ministry of Interior has looked to Gemalto to implement the system and it is currently operational.

[55] http://www.epractice.eu/document/3905

Recent news in November 2007 surrounds the announcement that Cogent Systems have been awarded an initial $11 million contract from the Spanish Ministry of Interior, General Directorate of the Police and Civil Guard for a national criminal automated fingerprint and palmprint identification system. (APFIS) The new system will be used by law enforcement officials for the Spanish National Police and Spanish Civil Guard and will integrate with the Ministry's criminal history system, with other European AFIS systems via the Prum Treaty and Interpol. Cogent Systems will serve as prime contractor on the project which can support over 500 workstations nationwide and includes Cogent's livescan units and mobile ID units.[56]

Spain overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Spain Biometrics Passport	Min. of Interior	Face	Gemalto	Passport	Operational	http://www.mir.es/SGACAVT/pasaport/Pasaporte_electronico.html (Spanish language)
eID card	Min of Interior	Fingerprint	Sagem Défense Sécurité	ID card	Operational	http://www.dnielectronico.es/Asi_es_el_dni_electronico/ (Spanish language)

SWEDEN

At the end of 2006, SAS Sweden launched a new biometric system throughout Sweden. It entailed the innovative features of using traveller fingerprint to match to passengers' checked baggage. The new technology which is provided by Precise Biometrics was launched in November and December 2006 at almost all airports served by SAS in Sweden.

SAS claims that this system is one of a kind in the world and offers many benefits. A passenger registers his fingerprint when handing in your baggage and again at the gate. In this way the passenger is automatically matched to his checked baggage. The new system eliminates the need to show photographic ID, rather relying on fingerprints for identification. This system guarantees security, according to SAS, as at the end of the passenger's trip; the fingerprint is automatically erased by the system. The use of fingerprint ID is also optional those who prefer may still travel with an identity card or passport.

Its introduction means SAS is the first airline to meet the security requirements agreed by the EU in the spring. In the long term, fingerprint reading will take place in connection with all flights within Scandinavia. The technology is expected to affect some 10 million travellers per year.[57]

In November 2006, the result of tests of the biometric technology implemented by SAS showed an improvement in passenger flow beyond expectations, and a warm welcome to the introduction of biometrics by passengers.[58]

[56] http://www.thirdfactor.com/articles/search?q=livescans
[57] http://feed.ne.cision.com/wpyfs/00/00/00/00/00/08/C8/F9/wkr0001.pdf
[58] http://www.travelbite.co.uk/newsbrief/flights/scandinavian-airline-first-use-fingerprint-scans-$452572.htm

Sweden overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Sweden Biometrics Passport		Face Fingerprint (later)	Gemalto	Passport	Operational	http://www.secureidnews.com/weblog/2005/01/31/swedish-epassport-solution-selection-ensures-compliance-with-international-interoperability-standards/
	SAS Airlines	Fingerprint	Precise Biometrics	Registered Traveller Scheme		SAS press release: http://feed.ne.cision.com/wpyfs/00/00/00/00/00/08/C8/F9/wkr0001.pdf http://se.yhp.waymaker.net/sasgroup/release.asp?id=140426

UNITED KINGDOM

UK is the country where many reactions have emerged, both positive and negative, about biometrics and identity management. In particular, the Home Office's national ID card and biometric visas have been cause for debate.

In 2006, the British Parliament passed legislation to introduce biometric-based national identity (or ID) cards.[59] Under a timetable set out when the legislation was passed, from 2008 onwards, everyone renewing a passport would be issued an ID card and have his or her personal information (including biometric data) placed in an associated database – the National Identity Register. The biometric portion of the system would likely use face recognition, fingerprints and iris scans. Until 2010, people can choose not to be issued a card, though they will still have to pay for one, and will still be placed in the database. Possessing an identity card will eventually become compulsory.[60]

Towards the end of 2007, there were some rumours that the ID card campaign is very far behind schedule in its planned roll-out, but few weeks later the Home Office denied this idea and on the contrary claimed that they are ahead of schedule and way below costs. Subsequently, there were more developments that involved denial by the UK Government of the current status of the ID card and UK Visa campaigns. It is believed that even more news on this heated topic will most likely occur in the next months as the issue of the ID card implementation has emerged in the policy agenda.

There are strong concerns about the accuracy and the vulnerability of the biometric systems and worries about privacy infringement as a specific report released suggested that the

[59] http://www.identitycards.gov.uk/downloads/ukpga_20060015_en.pdf
[60] Trend Report 2007 - UNISYS

technology is mainly untested and that the database with all details of every ID card holder is likely to become a major target for security attacks.[61]

Another report,[62] by a House of Commons committee, noted that there was a lack of transparency surrounding the incorporation of scientific advice, and that "choices regarding biometric technology have preceded trials". Although there are privacy concerns related to the identity cards proposal, much of the criticism of the scheme has centred on its cost.

The developments of the UK Visa have also been discussed on a regular basis almost just as much as the ID card initiatives.[63] At the end of 2007, there were reports from the government that the visa programme was advancing according to the original plans.

Also, there was a major trial that took place at Heathrow Airport, called miSense, involving iris scan technology. miSense was designed to test the principles contained within the Ideal Process Flow developed through IATA's Simplifying Passenger Travel Programme.[64] One of the underpinning principles of the Ideal Process Flow is to collect and verify traveller identity information as early as possible and by using the same information throughout the remainder of the airport journey, facilitate easier air travel while maintaining high standards of security and identity management. Several journey stages were linked together to create a single travel experience including check-in, entry to security screening, aircraft boarding and automated self-service border clearance.

During the sixteen week trial held at London Heathrow Airport, more than 3,000 travellers participated in what is widely regarded as one of the most comprehensive trials of biometrically enabled access control to be conducted in an operational transport environment. miSense was developed and delivered by a consortium of nine private and Government sector organisations and was conceived, developed and delivered within twelve months. The final report of the trial was released in June 2007.[65]

---

61 A report was released by researchers at the London School of Economics and Political Science (LSE). LSE Identity Project 2005, The Identity Project: an assessment of the UK Identity Cards Bill and its implications (PDF), London School of Economics and Political Science, June 2005.

62 House of Commons Science and Technology Committee, *Identity Card Technologies: Scientific Advice, Risk and Evidence* (PDF), Sixth Report of Session 2005-2006, August 2006

63 See: http://www.ukvisas.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1165344659165

64 http://www.spt.aero/

65 http://www.misense.org/documents/miSense_summary_report_v.1___June_2007.pdf

United Kingdom overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
UK biometrics passport	Identity and Passport Office	Face Fingerprint (later)		Passport	Operational	http://www.ips.gov.uk/passport/about-biometric.asp
National ID card	Identity and Passport Office	Fingerprint	In Procurement	ID card	Planned	Home page: http://www.ips.gov.uk/identity/index.asp Strategic Action Plan: http://www.identitycards.gov.uk/working-suppliers-framework.asp
Biometrically enabled access control trial at Heathrow Airport 2006/07	BAA	Iris	Sagem Défense Sécurité is supplying the various biometric sensors for the trial: fingerprint MorphoSmart sensors, handheld MorphoRapID terminals, digital photo cameras, modified iris cameras, ICAO standardised smartcards and all relevant software tools.		Completed pilot	http://www.misense.org/home.html
UKVisas	Identity and Passport Office	Fingerprint		Visas	Operational	http://www.ukvisas.gov.uk

Other European countries

NORWAY

In December 2006, Motorola announced a contract with Norway's Ministry of Foreign Affairs and the National Police Computing and Material Service to provide for the collection and verification of biometric data for Norwegian passports, visas and other travel documents.[66]

Norway overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Norway biometrics passport	Norway's Ministry of Foreign Affairs and the National Police Computing and Material Service	Face	Gemalto Motorola (enrolment procedures)	Passport	Operational	http://www.politi.no/

SWITZERLAND

Since 4 September 2006, the Swiss can apply for biometric passports. This type of passport not only involves "engraving" data into the document, but also storing it on microchip.

Within the framework of a six-year contract, Siemens has developed the solution for capturing and verifying the biometric data of Swiss citizens and checking Swiss biometric ID documents. This system is based on ID document readers and fingerprint scanners from CrossMatch Technologies, a photo capture station and camera from Digital Card Systems (DCS), and the Homeland Security Suite from Siemens, developed by the Biometrics Centre of Siemens PSE (Program and System Engineering) in Austria. In the same time, some biometric applications have started to be used by Private Banks.[67]

Switzerland overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Switzerland Biometrics Passport	Federal Office of Police	Face Fingerprint (in 2009)	Siemens CrossMatch: ID scanners	Passport	Operational	www.schweizerpass.ch

[66] See: http://www.kauppalehti.fi/.../releases/press_release.jsp?selected=other&oid=20061201/116531121646 90&lang=EN

[67] http://www.ws-huethig.de/news/5/d7424e4fb87.html

EU LEVEL

An introduction to the VIS (VIS-II), Bio Dev I - II and the SIS II is available in Section 2.1.2.

On 14 May 2007, the EU Parliament approved the VIS-II project. European Institutions reached agreement on the new information system on the issuance of European visas after 18 months of negotiations.

The objective of the new EU VIS is to improve the process and security of procedures of the issuance of European visa. The system should also contribute to the improvement of the internal security of the EU and to the fight against terrorism and other serious crimes. The central issues for negotiation revolved around: the fundamental rights of millions, legitimacy of purposes of the system, proportionality and necessity, and the access to the database by authorities is not a routine handling.

EU-level overview table

System	Institution	Biometrics technology	Integrator info	Application	Status	Contact info / link
Eurodac	EDPS + Data Protection Authorities of participating member states	Fingerprint		AFIS	Operational	http://www.edps.europa.eu/EDPSWEB/edps/lang/it/pid/39
VIS	European Commission DG Justice, Law Freedom	Fingerprint	Accenture + SAGEM Consortium (also includes Daon, Bull, Steria, UniqKey, WCC)	Visas	Planned	
BioDev II	Border control institutions from Austria, Belgium, France, Germany, Luxembourg, Portugal, Spain and the UK Project leader: FR Tech matters: DE Consular cooperation : UK Border cooperation : AU Communication : BE	Fingerprint	Motorola, Zetes Sagem	Visas	Pilot	PPT presentation that provides information on both the previous BioDev I and current BioDev II projects http://www.idfraudconference-pt2007.org/cms/files/programa/PFL4734784d4bb1b.pdf
SIS II	European Commission DG Justice, Law Freedom	Fingerprint		Visas	Planned	http://europa.eu/scadplus/leg/en/lvb/l33183.htm

2.3 Non EU Major Developments

This study outlines some of the major relevant developments that are occurring in the United States and Canada. We have chosen to focus on these two countries as they were well represented at the final conference in Brussels. Input was gathered from their presentations and has been consolidated for this report.

U.S. VISIT program

The following provides some background information and an overview of the programme.

Driven by the traumatic experience of 9/11, U.S. government rapidly introduced a strict surveillance policy confronting incoming travellers. As a structural change, the Department of Homeland Security (DHS) has been established to improve coordination and information sharing of authorities as for example FBI, Department of Defense (DOD), US Customs and Border Protection (CBP), US Coast Guard. After legal changes, the US-VISIT program was introduced with the objective to know as much as possible about every non-U.S. citizen before allowing them to enter the U.S. Measures include:

- Travellers must yield many personal data before boarding flights to the U.S.
- Photographs and fingerprints are taken from every incoming traveller at the U.S. borders,
- U.S. authorities have access to airline booking databases all over the world (which conflicts with European data protection regulations).

Countries within the Visa Waiver program (citizens of which do not need a U.S. Visa to enter the USA) had to introduce biometric data in their passports, although the data thus stored are not trusted by the U.S. authorities.

It should also be noted that the whole program does not apply to U.S. citizens.

Regarding biometric deployment, the world's largest-scale database system as of today[68] containing personal data has been established, with currently 80 million individuals being stored and a storage duration of 75 years.

US-VISIT program's biometrics-based identity management services are intended to help the U.S. government identify, mitigate and eliminate human security risks. The program provides its services to authorised officials within agencies throughout the immigration and border management system, law enforcement and intelligence communities and supports DHS's efforts to meet a congressional mandate for an integrated, automated biometric entry-exit system.

The most recent updates in the program will convert from a two-fingerprint standard to a 10-fingerprint collection requirement for first-time enrolees at all air, sea and land ports with the intention to improve accuracy and enhance security and reduce the problem with those people who have poor quality prints (about 4% of the population). Further development should yield interoperability between the US-VISIT's Automated Biometric Identification System (IDENT) and FBI's Integrated Automated Fingerprint Identification System (IAFIS) so that biometric and biographic data can be exchanged. This should be achieved by assigning a

[68] In the next few years, the European VIS will become larger in terms of data, but eventually the U.S. system surpass the VIS due to its because of its long retention period.

unique identifier to each individual for information linkage across data systems to establish and manage a single unique identity for each individual.

Another development is an exit procedure with the objective of finding visa overstayers. On completion of a biometric exit pilot at selected air and sea and other potential options, US-VISIT airport exit procedures will be incorporated into the airline check-in process in order to minimize the impact on legitimate travellers by end of 2008.

It is claimed that the U.S. DHS' Chief Privacy Officer and US-VISIT Privacy Officer ensure that privacy protection is integrated into the programme's processes and procedures to ensure that "any foreign national" has the same protection as a U.S. citizen within the US-VISIT programme. It remains unproven whether this practically works in any case.

At the EBF seminar, Mr. Troy Potter from DHS stated that the deployment of a large scale system was considered a risky task (concerning the technology risks and the scalability); because the system was deployed aggressively before understanding if it could effectively work. He also claimed that currently there are over 80 million individuals in the database, and therefore the conclusion is that it does work.

This is a different sight than the ones discussed in Europe. Although the general concept is known, there are many important issues which still have not been undisclosed and therefore raise fundamental questions:

There is not much knowledge about data quality and its assurance. There are several reports in the media about travellers experiencing refusal of entry and even more trouble because of incorrectly linked personal data. Some reports tell that data processing is outsourced to countries like Bolivia for cost reduction leaving unknown how it is protected against modification or unauthorised access.

Many issues discussed in this report (see Chapter 5) for Europe would also apply to the U.S.:

- Experience with such large databases in terms of performance, error rates, multiple and different entries for the same individual, supervising authorised access for so many users, etc.
- Policies and measures to prevent function creep when so many authorities have access, if such are implemented at all.

It is not disclosed in detail how these (and more) are covered.

It could have an impact on European planning that the U.S. is switching from 2-finger to 10-fingerprints. This could imply that matching of two flat fingers does not yield satisfactory results, as many experts have already surmised.

The whole issue regarding correction of wrong data or data security breaches is not described satisfactorily for the understanding of European Data Protection and the people affected. It is stated that such problems are addressed to responsible officers but some travelers experience that they do not have any rights when something is wrong with data that is claimed to be theirs. There is a chance that one who is affected by incorrect data or linkage will never be allowed to enter the U.S. (or worse, being subject to special law enforcement procedures outside the U.S. justice).

CANADA

Although being exempt from the U.S. VISIT regime, Canada is planning to introduce new passports by late 2007 using biometrics (digital images), beginning with diplomatic passports as a pilot. The image and personal information will be stored in a chip to be read at border control points with the only objective to verify the information contained in the passport. It is not intended to establish a database to be compared with the information in the passports. However, at enrolment passport applicant's photos will be compared against a database of against 21 million images of Canadians to find duplicates under different names or suspects on security watch lists.

Officials said to the press that this will be Canada's largest biometric deployment so far.

Canada also develops frequent traveller systems like CANPASS (Canadian Passenger Accelerated Service System) to enhance and increase efficiency at borders, especially those with the U.S. CANPASS is a program by Canada Customs affecting both goods and people travelling between the U.S. and Canada. The objective is to streamline customs and immigration clearance for pre-screened, low-risk, frequent travelers. (E.g. truck drivers' fingerprints) Furthermore, at major airports, frequent travellers can enrol to the CANPASS AIR program using iris scan. Other specialised CANPASS programs will cover airline staff, private air or watercraft operators, as well as people frequently crossing remote land borders.

No exact scale figures have been found except that the biometric passport program will be funded with $10.3 million, which is a small amount compared to what is expected in Europe.

Different from the U.S., Canada has demonstrated a strong concern on data protection and privacy. There are many public discussions about biometrics and the impact of the increasing interest in personal data in general; claiming inaccurate technology and how to prevent function creeping.

Some concerns in Canada fear a "misguided faith that among many that technology will solve security problems in the aftermath of the Sept. 11 attacks." "There's been a real move in governments to create a whole infrastructure of technological surveillance."[69]

At the final conference, Mr. Fred Carter from the Information and Privacy Commission of Ontario, Canada, explained the strong belief in "built-in" data protection and privacy from the very beginning of a sensitive project, referring it to "Privacy by Design":

- Built-in privacy implies early into the architecture, design specs, and technologies; design must start from maximum privacy
- Assessment of all privacy risks: conduct privacy impact assessments; annual privacy audits
- Minimization of the collection, use, data: minimization of routine collection, use, and retention of all personally identifiable data
- Be comprehensive and systematic: effective privacy requires an integrated approach; privacy must be applied to entire data systems and throughout the data life cycle
- Privacy rules must be enforced; enforcement must be trustworthy for system to earn trust and use.
- Use privacy enhancing technologies (PETs)

[69] Valerie Steeves, a law professor at Carleton University in Ottawa

Therefore he addressed concerns also discussed in Europe as:

- Large centralised databases, especially the false negatives and false positives which could lead to serious consequences,
- Far-reaching consequences of errors in large-scale networked systems;
- Interoperability that invites unintended additional “secondary” uses (function creep)

3 Security and Privacy in Large-scale Biometric Systems

The following text in chapter 3 contains extracts from a report developed by EBF for IPTS on privacy and security in large scale biometrics deployment. The extracted parts are cited in original and discuss some of the issues that have been covered in the previous chapters but analysing them from a different perspective.

3.1 Background

Under increasing pressure to secure the safety and liberty of European citizens, EU Member States have embarked on the introduction of large-scale biometric projects such as passports, visa, ID cards, driving licences and so forth. Biometric technology involves the collection of digital representations of physiological features unique to an individual with a sensoring device. This digital representation of biometric data on a document can then be used in many different ways for biometric identification of a person or for verification. Biometrics is seen as the important new tool in the effort to increase the efficiency of systems designed to check European citizens and/or visa or residence permit holders at border crossings or other points of control. However, at the same time, the implementation of these projects introduces new challenges that, if not addressed, may limit the benefits of this technology for Europe. In fact, it can be argued that if these challenges are not dealt with properly, these schemes might even introduce more significant security risks than they aim to diminish and make serious inroads to traditional principles of data protection. The following questions help to identify some of the **challenges to security and privacy**, which may arise as a result of implementation of biometric projects:

- What will the exact function (identification, authentication, verification / security, convenience, efficiency) of the biometrics be in each application that is currently introduced in Europe?
- How will the biometric data in these applications be managed (e.g. central vs. local storage, on chip vs. remote processing)?
- What are the privacy aspects related to the use of biometrics in the context of these applications?
- What measures can be taken (technical and procedural) to prevent misuse of the biometric data?
- What common legal agreements should be put in place in order to facilitate interoperability of biometric technologies within the EU?
- What are the best practices and how can we make sure that weaknesses, once identified, are repaired instead of repeated all over Europe?

Without alignment on credible ways to address privacy concerns in biometric information systems, and without legal and technical conformity of such systems with privacy laws within Europe and around the world, the benefits of such systems could be minor. Even more seriously, it can be assumed that under those circumstances market acceptance and trust of large-scale biometric systems will be hindered.

Therefore, one of the main immediate concerns of the **European information society is to find a widely acceptable, cost-efficient, user friendly and effective solution to the task of identification and verification of individuals which strikes the right balance between privacy and security**. Biometric technologies play an important, if not key role in this process. It is therefore of utmost importance that in the design phase potential negative side effects of individual measures based on biometrics are identified and addressed and informed decisions made.

The following sections detail the findings made from EBF on security and privacy in large scale biometric systems, based on a workshop with relevant experts (see 4.2 'List of Attendees').

3.1.1 Methodology

The method for producing this report is:

- Identifying the main threats for security and privacy in implementing large-scale biometric systems, in the private and the public domain in EU25 countries.[70]
- Assessing the risk potential of the identified threats considering the specific application domain.
- Proposing solutions which will increase security and privacy protection in biometric systems.

3.1.2 Structure of the workshop

The one day workshop was structured according to specific agenda topics. Knowing that the discussion would be multi dimensional due to the complexity of the issue, the chosen approach was followed to make sure that within this complexity no specific subjects would be missed.

The different topics have been introduced through a five minutes presentations of one of the invited experts (see also Chapter 3.3). The experts that have been invited to the workshop come from a variety of backgrounds: end users (government related, banking), industry (technical, program management e.g. EU Visa Information System and Schengen Information System) Data Protection Authorities (national and EU DPAs), research (TILT, University of Tilburg) and counter terrorism agencies. The composition of the group was organized to make sure that a balanced discussion would take place.

3.1.3 International Biometrics Advisory Council (IBAC)

The subject of this workshop has been put on the agenda of the meeting of the IBAC, which took place on September 13th 2006. The preliminary agenda of this workshop was discussed and several remarks and suggestions were made. This resulted in some changes to the proposed agenda and to a better insight in how the workshop should be structured. Attendees to this IBAC meeting where:

- Christer Bergman (International Biometrics Industry Association, Sweden/US),
- Christoph Busch (Cast Forum, Germany),
- Bernard Didier (Sagem, France),
- Norbert Kouwenhoven (IBM, The Netherlands),
- Helmut Reimer (Teletrust, Germany),
- Max Snijder (European Biometrics Forum, Chair, Ireland/The Netherlands),
- Ann Cavoukian (Canadian Data Protection Officer),
- Ted Dunstone (Biometrics Institute, Australia).

Current government liaisons of the IBAC are Robert Mocny (acting director of US Visit / US Department of Homeland Security) and Marek Rejman-Greene (UK Home Office).

[70] Note: at the time of the publication of this report, the European Union consisted of 25 Member States. Since then, the European community has expanded to 27 MS. However, this analysis covers only those of the EU 25 – as the work carried out spanned 2006 into the beginning of 2007.

Synergies of experts have been created between the Biometrics Deployment Study and the Security and Privacy in Large Scale Systems project as both Mr. Snijder and Mr. Busch also participated at the Expert Meeting of the BDS in Brussels during March 2007. The exchange from the same experts helps guarantee a common voice throughout the two studies since the objectives of the studies are quite inter-related.

3.2 Challenges and Issues to be addressed

3.2.1 Introduction

In the initiatives which have evolved after the adoption of The Hague Programme EU governments have made use of the new technology applications that not only make European documents machine readable, but also involve the physical characteristics of European citizens. In the measures proposed or adopted, biometric technology is used to prove the linkage between an individual person and an identity document by using one or two biometric identifiers. The use of this link intended to reduce identity related crime and illegal border crossing and therefore also to detect or prevent terrorists moving into or throughout the European Union. For example, the use of a biometric identifier will make it difficult for a look-a-like to use a passport of another person or for an asylum seeker to apply for asylum in a second EU country when a request has been turned down in the first.

Although other uses of biometric technology are feasible in the future, the current EU schemes only concern the limited use of the biometric as a means to prove a linkage between document and holder. Nevertheless, the use of biometric identifiers in travel and identity documents creates a whole new set of challenges and issues for policy makers. These issues can only to a limited extent be compared to those relating to government handling of traditional documents. The coupling of biometrics with IT in the context of a European Union with over 25 Member States suddenly creates multiple problems of scale. As has already been briefly discussed in the previous background section, these problems relate especially to the storage, retrieval and use of biometric data, the protection against un-authorised use, and privacy protection.

One of the few issues that also apply to traditional documents and databases is the principle of **proportionality**. Measures taken and costs involved must be proportionate to the goal they are destined to achieve. The introduction of biometrics indeed requires big investments, in terms of infrastructure on government side, and costs of obtaining a valid document for the citizen. In fact there are forecasts that projected costs may spiral for the citizen as technology is still lacking maturity and experience with the implementation of large scale biometric systems is scarce. Probably, costs will continue to remain high for a long time to come. In addition, a large scale system will involve many authorised users. The UK Health database has shown that an ingenious system of hierarchical layers of authorisation is very costly. In the case of the Visa Information System, which was introduced in the previous chapter, (EU VIS which is primarily designed to prevent VISA shopping on the basis of using false names) the use of biometrics and a central database is regarded as the only credible option in achieving this goal. In the case of the e-passport, the proportionality test is subject to debate. If for example, central storage of biometric passport data and its possible privacy and security implications have to be weighted against the advantages for border control authorities of being able to link persons to passports, any outcome will not go undisputed.

For some biometrics as it stands now have intrinsic flaws. Therefore a golden guideline may be that in relation to privacy issues, but foremost for security reasons, biometrics should never be used alone. And at the very least, the use of biometrics should be subject to constant reflection. During the process of introducing biometric systems the question whether the

means serves the end should be asked at every step. It was also voiced in the 2006 workshop that the purposes of the various systems should be carefully articulated and the use **restricted by design** according to the 'purpose binding principle'. This principle means that it should be clearly determined who is in control of the data, **purposes of the system** should be restricted carefully and finally, the number of applications should be explicitly restricted too. If this does not happen it may have severe privacy implications for citizens who have trustfully given their biometric data for one purpose and then find it has been used for another without their permission. What generally is required is a thorough security check (a mandatory check) before introducing a particular system. Whether current arrangements meet this requirement is uncertain. Another concern is that border authorities of countries outside the European Union can also read biometric data in a passport, whilst some European citizens would not choose to hand these authorities their biometric data if they had a choice.

A key question which we would like to bring up once again deals with the **place of storage of data**. Are biometric data stored centrally (on a database) or on a token (on card) only? One concern about central storage is irreversibility, the likelihood that the owner of biometric data will not be able to revoke data. Another perceived danger of central storage is that this encourages **link ability**. This is the possibility that biometric data are linked to personal data from another database and used for unrelated purposes. This link ability is at the same time seen as a distinct advantage when it comes to criminal and/or national security investigations. It is also a disadvantage as it is facilitating function creep. There should therefore be **transparency** about the purpose for which the data may be used. To prevent use outside the original purpose, proper safeguards have to be implemented and risk assessments need to make clear whether the risk is acceptable. Some of the current EU schemes like the EU-passport do include on token storage. This type of storage is regarded to be the safest in terms of privacy protection and data holder control (see also section 3.1). However, the security aspects of the stored data and the token itself remain challenging, also because the exact use of the biometrics is not fully agreed and understood by all parties involved.

The **types of biometrics** with which the EU member states will be basically concerned with are face image and fingerprint. The emergence of international standards (available from the ICAO website) has made the government task of deciding on technical specifications easier. As regards the EU biometric passport and the choice of picture the EU will deal with raw biometric data and this causes concern as this first generation face image irrevocably introduces a weak link between identity and biometry due to limitations of the current face recognition technology and implementations. Especially when own brought pictures are being used for enrolment instead of life made pictures at the place and time of registration, a potential risk in terms of quality and security is introduced. A biometric modality that requires less adaptive measures to the environment (like fingerprint) reduces that risk, as it won't be necessary the bring your self made finger print images to the passport registration counter.

Another concern is the lack of experience by the operators of biometric devices at public places such as consulates and city halls, where now the capturing of biometric information is (or will become) a new part of the registration process. Also the subjected individuals might be confronted with a biometric sensor for the first time in their life. The interaction between an individual and a biometric sensor is in most cases of crucial importance for the **quality of the captured data**. A skilled and well trained front desk operator can have a significant impact on the quality, as well as a well informed and educated end user. Also the **environmental conditions** (lighting, humidity…) can have a significant impact on the quality of the capturing process. This has to be assessed at *every single location* where biometric equipment is being installed. Biodev, a European Commission funded pilot project driven by

the Ministries of Internal Affaires of France and Belgium, is assessing these aspects in the actual environment of EU embassies and consulates. (see 2.1.2)

In terms of **control of the data** and the system in general, template protection is an important management issue, which needs addressing in the design stage of a measure. The key question is who does the template protection and who controls the authorised users. There is also concern about grey areas of use, such as the legal question of how you can prevent police forces from conducting **cross data searches**, which are not allowed in one country but are in the other. To prevent interconnection of databases there is a technical solution; it consists of placing the individual in control of the data through the requirement of an electronic signature in combination with for example a fingerprint.

It was noted in the workshop that the **handling of personal data** would eventually make or break the convergence of technology, security, privacy and identity. This includes the exchange of personal data between organisations and nations. In that process of convergence **testing and certification** can play an important role. The establishment of European capabilities on testing and certification of biometric components and systems will help in building up trust. **Trust** in a European biometric system is essential to facilitate its operation. In section 3.7 this will be further elaborated upon.

To summarize we singled out at least nine key issues, which need addressing:

1. Proportionality of the measures.
2. Purpose of the measures, and restrictions on the use of the data collected.
3. Place of storage of biometric data.
4. Type of biometrics used in documents.
5. Effects of interoperability of databases.
6. International data exchange.
7. Control: rights of those providing their biometric data and transparency of purpose and authorised use.
8. Testing and certification of biometric techniques.
9. Quality control of the biometric capturing process (especially at enrolment) on both technical and non-technical aspects (e.g. human factor, environment, processes).

The main challenge facing the EU is to achieve the Pan European roll-out of the EU biometric passport concept (and other biometric travel and identity documents) without introducing problems related to its large scale. These new problems would very likely fall into the category of technical problems of implementation or opposition in the context of a privacy debate. In general it can be argued that privacy enhancing technologies enhance the trust of the citizens. Therefore, although privacy concerns and associate technical and regulatory solutions are delaying the process, they deserve full attention because the solutions thus found are instrumental in achieving successful implementation.

A second challenge can be found in improving the legal framework. There are several issues deriving from the current legal framework which need addressing (see below 3.5). The Article 29 working party document (see Annex) has raised a few points in this respect. The prerogative here is to find a common understanding of legal issues and make this work. It has been suggested in the workshop that the issuing of EU guidelines or recommendations on privacy enhancing measures in the field of biometrics would increase rates of acceptance of the introduction of biometrics by the EU population.

The final challenge to be mentioned here is safeguarding a realistic European approach towards the use of biometrics. Instrumental in this is that the EU precisely determines the role biometrics is to fulfill as well as the results to be expected. This means finding an answer to the question over what an adequate purpose in using biometrics in a constant process would be. An even more fundamental question is whether the EU needs biometrics or whether goals can be achieved through other means.

3.2.2 'Large-scale' biometric systems and their impact on society

Large scale biometric systems have been chosen as a subject of discussion because of the (potential) impact of those systems on national communities and on European society as a whole. In the workshop it was agreed that "large scale" not only applies to the potential size of the database or, more specifically, to the number of people whose biometric details are enrolled in the system, but equally to the number of searches that are carried out. Although governments have experience with databases in the area of police and judicial cooperation, these databases normally only cover 5 % to 10 % of the population. An application such as the biometric passport will eventually include most of the population. More difficult to predict is the intensity of the searches which will be carried out. The number and nature of searches to be carried out will depend very much on a large set of variables including the design of the system, the purposes laid down in national and European law, legal context, user culture and authorised user control.

It was thus agreed that scale related factors are:

- the number of people enrolled,
- the number of applications to be used within one system,
- limitation or selection on people to be enrolled / to be able to be enrolled (e.g. due to religion, race, disabilities, diseases etc.),
- number of access points,
- the number of searches per day/week/month/year,
- the degree of control.

However, the scale of an application is not the only factor that will have an impact on society. There are a number of important non-scale related factors in the use of biometrics, which lead to increased potential benefits but also to increased potential risks.

3.2.3 Non scale-related factors

In this respect, the growing number of purposes for using biometrics and other personal information and the increased quality of biometric reference data should be mentioned. An example of this is identification without consent, which has been created by the quality of video surveillance images combined with automated identification of people (e.g. through the use of face recognition). Here the thin line between voluntary or non-voluntary participation of citizens in biometric applications becomes evident, and this development has an important impact on the life of ordinary citizens. With an increased inclination on the part of at least some EU member states to share databases containing information on criminals and on people who should be traced for other reasons, there is a serious need to examine the use of face recognition data in the various contexts. It is not so far fetched to argue that in the current situation face recognition data collected in one member state could be used in private or public places in video surveillance operations in another member state without the citizen involved becoming aware of this. The societal impact of this development needs further examining.

Other non-scale related factors are interconnectivity and database ownership. Increased data storing by a wide range of data owners as a result of the growing use of computer and Internet facilities in all sectors of society has made linking up databases interesting from an economical and a government enforcement point of view. Linking databases that have different owners and/or purposes and/or data, also across the private and public divide, has intrinsic privacy and security dangers and should be addressed. The question is whether current legislation, and the enforcement of this legislation, is sufficient to regulate the exchange of data in the interest of the public (see section 3.5 and 3.6).

Finally, in the workshop the societal impact of the number of access points in any European public database and the level and kind of organisation that is in control of the application and data were discussed. It was agreed that unnecessary inroads into the privacy of citizens should be avoided. Therefore the impact on privacy had to be minimised at every stage of the process of introducing and designing a system involving biometrics. The workshop subsequently discussed a non-exhaustive list of requirements needed each time you introduce a biometric system; this included a targeted implementation plan, a safe enrolment process, assessment of accuracy and efficiency of the system, continuous risk assessment, and a fall back procedure.

Summarizing we can say that the main **non scale-related factors** are:

- the growing number of purposes for using biometrics,
- the increased quality of biometric reference data,
- interconnectivity with third party databases,
- database ownership,
- kind and level of organisation that is in control of the application and data,
- international data exchange (e.g. between EU Members States and/or between EU – US).

The above indicates that scale alone is not always the decisive factor for a biometric system's potential impact on society. It is the combination of scale related and non-scale related factors that can lead to an increased risk when considering privacy and data protection issues. The relevance of the different factors and the potential threats they might pose to society can only be properly assessed when being put in the context of a specific application scenario.

In section 2.1 and 2.2, we provided a list of those large scale systems at both an EU and Member State level. Considering the difficulty in the issue and the delays in some of the systems, this list provided information that is available as of the end of 2007. During the meeting of experts in 2006, it was expressed that it would be instrumental to compile this list of large scale systems at EU level as well as a list of national ID systems involving biometrics. This list would also have to entail the specific application scenarios used. This list would help in determining the state-of-the-art in this respect and facilitate the exchange of best practices (see below section 3.5)

After this general discussion, the attendees agreed to focus the discussion during the rest of the workshop on e passports, national e-ID cards, the EU Visa Information System (VIS) and the future European Biometric Matching System (BMS), which was intended at the time to be added to the EU VIS in 2007. As regards video surveillance without consent, because these systems rule out the voluntary aspect of the use of biometrics, several attendees expressed a major concern about the use of Non-Voluntary Discrete Validation such as using facial recognition on Video Surveillance systems as put into practise at the USA Super Bowl. At this event, where more than 50.000 people are being gathered in a stadium, every single person's face in the audience was checked against a watch list, with remote cameras and

without anyone being aware or having given their consent. There is a case for convening a meeting to discuss this topic in greater detail, as the agenda of this workshop did not allow for elaboration.

3.2.4 Purpose of using biometrics

All discussions about privacy and data protection centre on the core question: "What is the purpose of the system and what kind of personal data are strictly needed to serve that purpose?"

This question is relevant to all systems that are using/processing personal information, including biometrics. Biometric data as such are generally being considered by Data Protection Authorities (DPA's) as personal information. To some extent, positions of the DPA's in the EU member states do differ regarding the assessment of data processing of biometric data.

In order to assess the risks -e.g. of function creep- in a biometrics enabled ID system it should be first determined what the exact use of the biometrics is in the system at hand. In other words: before the purpose binding principle (explained above section 3.1) can be applied, the purpose of the use of biometric data within a specific administrative system should first be determined and agreed by all stakeholders. Not in all cases of envisaged large scale biometric systems are this purpose well defined or agreed upon by all parties involved (e.g. passports and e-ID cards). This inhibits a common definition of how biometrics should be used and managed at European level. As a result performing a targeted assessment of security and data protection vulnerabilities of the systems in question is not enabled.

The question whether or not to install a central repository of biometric data of citizens in national public administrations is a good example of this issue. If there is no EU decision on this, which means that all member states have to agree on one specific model, we will end up with a variety of models at national level. (This has evolved to be the current situation as of the end of 2007.) This will lead to a fragmented approach and it will become impossible to perform one assessment for Europe as a whole. That situation makes it difficult for European representatives to negotiate as one European entity with non EU countries (like the US) on issues like international data sharing and the privacy/data protection principles.

3.2.5 Risk modelling: the need for targeted scenarios

The concerns that will be listed in section 3.3 should be positioned within the context of the application scenarios chosen. When a targeted threat analysis can be performed, this will result in the development of specific threat models. When conducting a targeted threat analysis the following questions should be addressed:

- What is the value of the transaction that is being enabled by biometrics?
- What is the quality of the biometrics used: is it easy to spoof or to frustrate the system?
- What is the fallback scenario and how secure is it?

Measuring the effectiveness of a biometric system requires knowing the original state prior to application of biometrics, in order to be able to measure whether there has been an improvement or not. False Acceptance Rates (FAR's) are intrinsically difficult to measure, but that is not unique for biometrics.

To be able to assess the quality of biometrics it is important to be aware of the intrinsic flaws that exist in biometrics. Depending on the kind of threats, a choice for one specific biometric modality or a combination of biometric modalities (multi modalities) should be made. Only when an assessment of the whole chain of processes and procedures (including the human factor) has been carried out, a threat assessment can be made.

In principle, we need a thorough security check (a mandatory check) before introducing a system, leading to a security refinement. This pre-check has not been carried out in most large scale biometric systems in operation in Europe today. To repair this and be prepared for future developments an integrated security concept for the European passport is needed, although Extended Access Control already is a step in the right direction. Existing security standards will also support such security checks.

3.2.6. Data Protection Authorities (DPAs)

The legal positions of the national DPA in European member states differ considerably. Whereas in several countries the DPA only has an advisory role, in other countries the DPA has a legal position prescribed by national law (e.g. France). This means that, for example, Data Protection Directive 95/46/EC and Article 8, the Charter of Fundamental Rights of the European Union will be enforced differently within each EU member state. This observation raises the question what could be done to develop tools for a better coordination of practices and initiatives towards adopting best practices. It should be noted that within the context of the Article 29 Working Group much relevant work is done on best practices in privacy and data protection. Part 1 (on privacy and usability of biometrics) is almost agreed on and Part 2 starts Jan 07 (biometrics in workplaces).[71] You can find more information on the web site of the EC DG Freedom, Security and Justice under 'Data Protection' (http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm).

3.2.7 Standards, testing and certification

Standards, testing and certification are not only needed to address issues of interoperability, conformity, performance and security, but are also important to build up trust in general. Especially, because privacy is a concern of each individual, trust in any system is essential for its successful implementation.

Biometric verification and identification methods are spreading to more and more fields of application, including European border control systems and applications (e.g. ePassports, European Visa Information System (EU-VIS), the European Biometric Matching System (BMS, to be coupled to the EU-VIS in 2007), National eID-Cards). In applications where biometric data might be processed by components of different vendors, the interoperability of components and systems is of critical importance. This situation requires standards. Relevant bodies inside ICAO and ISO/IEC have been developing these standards. Regretfully, there are no criteria to determine to which extent a system that claims interoperability and conformity and that is being tested, actually complies with those standards.

Given the inadequate coordination on a European level and with 25 EU member states (before the recent expansion) now implementing the new e-passports with biometric identifiers, new risks are being created in terms of efficiency, security and convenience of the envisaged applications. Still there are no adequate testing criteria, nor are there any commonly agreed

[71] Since the September 2006 meeting, the Art. 29 WG has adopted several new opinions on various issues, including the "concept of personal data". For complete details, please refer to the following link: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm

and certified compliance tests to verify conformity of biometric components and systems to certain standards. There are also no European testing centres to perform these tests and to publish results such as a white list of components that comply with a certain standard. This means that currently no vendor or systems integrator can guarantee interoperability or compliance with existing standards, resulting in ad hoc solutions at national level, often with proprietary products and systems.

This is not an ideal situation for building trust in biometric systems, or for establishing a harmonized approach towards the implementation of biometrics into European border control systems.

The European Commission is justifiably concerned about its ability to adequately determine the necessary requirements (technical and non-technical) for future European biometric programmes and to provide a Europe-based capability to perform its own compliance and other testing. This includes technical and non-technical aspects, such as the quality of processes and the operating personnel. **BioTesting Europe**, a pan-European project managed by the European Biometrics Forum, aims to address these concerns by unifying European interests and by providing a pathway that shall lead to the development of proper European testing capabilities in the area of biometrics.

3.3 Topical Report

We will now focus on the topics discussed in the workshop and based on its agenda. The different topics have been discussed in the context of the applications that have been chosen as the most urgent to assess.

3.3.1 Privacy concerns in different phases of the biometric process

Registration (enrolment)

The enrolment process is the critical phase in a system based on biometrics and improved standards for enrolment are required to ensure data quality and the quality of the overall enrolment process. This includes training and education of the operating personnel.

Breeder documents on which enrolment is based ought to be thoroughly checked and the enroller needs to be fully trained to verify that these documents are genuine. Low quality of biometric data fed into the system will lead to more false rejections (FR) and false matches (FM). In certain circumstances a false rejection can be very distressing for an individual, because follow-up procedures can be intrusive. A high FR-rate leads to inconvenience and to people not wanting to use the system any more. Of course each system is dependent on the preparedness of people to enrol where this is required. It has been proven that guidance by qualified personnel during the enrolment process will result in a significant higher quality of the enrolled biometric data. This will increase the performance of the biometric matching process drastically, both in terms of False Reject Rate, False Non Match rate and False Match Rate. Additional procedures to compensate for this can impact the privacy of the individual.

From the point of view of the enrolee the decision to enrol is crucial too. At the moment of registration the enrolee has to decide whether or not to trust the system. Once enrolled, data can often not be revoked, and thus any subsequent intrusion of privacy or breach of security cannot be prevented.

When it comes the registration of the biometrics several questions can be posed concerning the basic principles of privacy and data protection:

- Is the purpose for registration clear to the user (transparency)?

- Is registration voluntary or not, and: what constitutes voluntary and non-voluntary systems?
- Who are responsible for the system and can it be trusted that they protect the personal data sufficiently?
- Are the registered data correct? Specific concerns are with the quality of the biometric enrolment data: low quality biometric data significantly increases the change on mismatches (False Matches) or non matches (False Non Matches), which makes the process less reliable.

Concerns:

- When no/unreliable breeder documents are available it will be difficult to make sure that the right person is claiming a certain name/identity (identity theft).
- Non-qualified operating personnel and less educated end users will decrease the quality of the enrolment data, resulting in inadequate performance of the biometric matching system.
- Low quality of biometric enrolment data will lead to a significant lower performance of the biometric matching system. Additional procedures to compensate for this can impact the privacy of the subjected individual.
- When there is a central biometrics database it will have to be clear to all what link (if any) exists between the biometric data and other personal data (i.e. home address, etc.).
- It may be difficult to guarantee that well trained photographers are available locally to supply photos in the technical format needed for enrolment for e-passports, especially considering multiple enrolment points.
- Failure to enrol might lead to discrimination of certain parts of population. People with certain professions (like a worker in a building company) might damage their hands/fingers so it might be impossible to read their fingerprint. It is also said that Asian people have difficult fingerprints to read.

Potential solutions:

- Standardisation and certification of the enrolment process.
- Transparent and clear communication to the user about the purpose of the application.
- Quality control of biometric data during the capturing/enrolment process.
- Training of operating personnel and education of the end users.
- Proper and acceptable fallback scenarios in case of failures to enrol and failures to acquire.

Storage

In Central storage can lead to ID theft rather than actual theft of the biometric. Connecting the personal data to another physical identity by only changing the biometric data and leaving the rest unchanged, is a larger risk than stealing the biometric data only. Biometrics may be stronger and privacy concerns neglectable when an individual carries his or her biometric identifiers on token and verification rather than identification is used. This is different in a situation where the personal information is based on unreliable sources, e.g. in cases where no official papers are present and only non verifiable information is available. In those cases a central biometric database could be the right and even only solution. Otherwise it can be said that there is a trade off between privacy, where a token is a better option, and security, where a central biometric database might be preferential.

Concerns (central storage):

- Once registered in a central database the owner of biometric data may not be able to revoke his/her biometrics himself (irreversibility).
- The possibility of a link between biometric data and other personal data.
- The probability that the purpose of the use of the data changes over time.
- Linking up with other databases might create the possibility that the data, combined with other information, are used for other purposes elsewhere.
- Biometric data (especially raw images) stored may possibly reveal diseases to authorised users, which may lead to privacy problems for the individual concerned.
- Larger possibility of 'mistakes' in the matching results due to increased change of more conformances between multiple biometric data sets.

Concerns (local storage, e.g. on token):

- The security of the token is very important so as to avoid possible loss or abuse.
- In the issuing process, mistakes can be made which are irreversible once the holder has left with the token.
- All responsibility is delegated to the holder which may cause problems with under age children, handicapped holders or even people showing irresponsible behaviour.
- The replacement of a token if lost or stolen will be costly, but may also cause administrative problems and the loss of the token potentially poses a security threat to the holder depending on the circumstances.

Potential solutions:

- A procedure could be designed for data owners to revoke their biometrics, including procedures for complaints.
- New methods of matching biometrics data in irreversibly encrypted form might overcome some of the problems mentioned.
- 'Weak link' between biometric data and other data so biometric data do not automatically lead to the connected personal data.
- Central databases, if not strictly needed, can be avoided in principle.
- Dynamic encryption.
- Matching on card.
- Quality control of biometric data during the capturing/enrolment process.

Retrieving (matching)

Important question in any system that contains personal data and biometrics is who has the authority to access those data and what data he/she is allowed to see. Especially with large databases of fingerprints and faces there might be many organisations which would whish to match their own data against those databases. The accessibility of those organisations to such databases can be limited. For example with EURODAC, the European central database containing fingerprints and other personal data of criminals, is based on a hit / no-hit base, meaning that no other information is being released from that database apart from the biometric matching result.

Concerns:

- Number of authorised users (i.e. entitled to access the database and perform a biometric matching) and their access rights: the larger the number, the more difficult it will be to supervise their activities and to prevent abuse of the system

- The organisation of an abuse free system of control over their activities
- Who decides whether the use of the system is proportional to its purpose; does the operator in question have the right to ask for a biometric comparison?

Potential solutions:

- Inform data owners about the purpose of the application so they can decide themselves about the proportionality
- Make clear that the operator is authorised (certified personnel, badges).

Modification (updating) / un-enrolment

When an application ends (e.g. by cancelling a subscription or by law) the personal data should be updated or erased. When governments gather information on people who visit their country it should be clear what information is being gathered and how long it will be stored. People also should have insight in their records in order to check if the gathered information is correct. If not, this information should be corrected or removed. In any case an enrolee should be (made) aware of the conditions upon which he/she will be removed from the database.

Concerns:

- Access rights of the operator: who has the authority to modify/erase information from the records
- How to verify the identity of the person to be modified
- How the owner of the biometric and other personal data can verify objectively that he/she is being removed from the system when an application ends (either by law or by ending a membership) and what information can stay in the system (if any)
- Labelling of people without them being aware of the criteria of how the labels change due to certain behaviour.

Potential solutions:

- To introduce certified processes and procedures (on EU level: across all member states)
- To employ certified personnel (on EU level: in all member states)
- To guarantee transparency for the owner of biometric data
- To provide good supervision by DPA's through the allocation of more resources and concrete training programmes.

3.3.2 Security aspects of biometrics

There is a perception, in some quarters, that information, which could be used for medical diagnosis, could be present in some biometric templates. This requires further investigation as it directly impacts the sensitivity to privacy of biometric data. If stored in template format it is expected that with most biometric modalities a significant amount of information is irreversibly lost, which will make it more difficult – if not impossible – to retrieve physical characteristics that might reveal medical information. From this perspective templates are preferable above raw images for passports.

Although spoofing is a potential weak point in most biometric modalities, this does not mean that biometrics can never be used in security applications. Some biometrics are more difficult to spoof than others. Using two biometric identifiers reduces the chance of spoofing

significantly. Supervising the interaction between the individual and the sensor makes spoofing a high risk effort and will prevent from spoofing in most cases.

Spoofing of biometrics is comparable with stealing keys and losing passwords. However, the irrevocability of biometrics put this into a more complex perspective. Also the fact that biometrics are more or less public features (pictures of faces can be made on any occasion, fingerprints are all over the place etc.) makes biometrics intrinsically different from a PIN or password.

It may be possible to define a process, which secures the biometric data within a token that can be replicated without compromising the biometric data. The principle of 'matching on card' (MOC) constitutes a local secure environment, without the biometric data leaving the card or other token. MOC leaves the owner in control of his/her data, as it will be the decision of the owner whether or not to present the data to a person or a device. Again it is required that the owner of the data understands the purpose of the system and trusts the person and/or device to which he/she presents his/her personal data. In case of MOC the exposure of personal data can be limited to a minimum, meaning that only the live captured biometric data are entering the card and a match/no-match decisions leaves the card. Therefore MOC might be suitable for authentication purposes.

Another concern is that not all people can physically become enrolled in a biometric database (Failure to Enrol, also FTE), because for some reason their physical characteristics cannot be captured. If the fallback procedure does not meet the same security requirements as the primary process, the FTE can cause security weaknesses in the enrolment process. People could deliberately frustrate the biometric enrolment in order to end up in a less secure fall back procedure.

Concerns:

- Biometric information is strictly bound to an individual, yet is not a secret. Stolen biometric characteristics (e.g. by spoofing a biometrics sensor with a fake fingerprint) cause an immediate threat of identity theft
- Biometric information (especially raw images) can expose health information concerning the individual and this information can then be used against her or his wishes
- Biometric data can be 'stolen' or modified when being transferred from sensor to central matching system
- In cases of Failure to Enrol (FTE) there is no clear fall back unless special measures are taken in advance

Potential solutions:

- To create awareness of what biometrics can do and what it can not do (demystification)
- 'Live and wellness' detection by automated means
- To place a heavy emphasis on supervised procedures when required
- Developing and storing advanced templates rather than images
- To do matching in a local, secure environment only (e.g. MOC)
- To develop proper fall back scenarios

3.3.3 Protection of data in nationally-managed ID systems

Information should be used only when and where authorised; it is necessary to create trust. Biometrics used through a decentralised system offers advantages: the highest point of security can be achieved by matching on card as all matching is done on the object (card, SIM, token …). The personal information as well as the biometric matching process itself are under a higher degree of control of the owner, which leaves room for the owner to decide whether or not to release his personal data and to allow a biometric matching process. Of course the token has to be secured against reading it without consent with the use of technical means like remote antennas.

There exists proof that current passport information can potentially be hacked by use of a laptop with an antenna when a machine readable code is used as a key to generate encryption, This encryption method, called Basic Access Control (BAC: the printed numbers on the machine readable zone of the passport are being used as code to encrypt and decrypt the information on the chip), seems not to be sufficient to protect the personal data on the passport chip. Thus a more robust method is needed.

There is general understanding, that the BAC is not sufficient to protect the personal data stored on the chip of the e-passport, especially when we consider the long life cycle of the passport (ref. 'The Budapest Declaration' by FIDIS: http://www.fidis.net/press-events/press-releases/budapest-declaration/). These chips contain all personal data, including biometrics. Additionally, biometrics are currently stored in their most vulnerable form: as raw images. This can lead to direct identification or to copying of the original features. When the raw images are converted into templates, this will be impossible in most cases.

A potential solution to this security risk could be the Extended Access Control (EAC), a PKI based encryption method. EAC reduces the access points to the chip to authorised readers only, i.e. readers that are using Public Key certificates for getting authorised by the chip to access its data. Furthermore EAC also forces a strong encryption of the transmitted data. You can read more on the official website of the German Bundesamt für Sicherheit in der Informationstechnik (BSI): http://www.bsi.bund.de/fachthem/epass/eac.htm).

If implemented, it should be applied to all data on the passport. However, for the EAC key management is still an unresolved challenge.

Storing all personal data on a chip creates a risk as the lock and key are held on the same object. On the other hand, if also the matching process is done on the card then potential connectivity problems can be overcome as no data leave the card.

Concerns:

- The cryptographic weakness of BAC is regarded as a weak point in the chain
- Effective key management is missing for EAC
- The root of trust is not clear and clear communication with the public is needed to foster trust
- Biometric raw images if not properly secured may allow diagnosis of certain diseases to the detriment of the data owner
- Some biometric raw images might allow direct identification
- Raw images can lead to copying the original physical characteristics from the reference data

Potential solutions:

- All personal data on the e-passport chip should be at least protected by Extended Access Control (EAC)
- Citizens should be well informed about the use of the e-passport
- Biometric templates should be stored in stead of raw images
- Revocability could be considered through the using of biometrics one way hashed with a PIN
- A detailed definition of security requirements at international level

3.3.4 Proportionality

One of the main drivers for biometric travel documents can be found outside Europe (USA). Although in Europe the discussions on applying biometrics in passports had started earlier, it were the 9-11 events that have put a strong political pressure on implementation of biometrics into the passports within a shorter period than originally planned. Due to this pressure and haste the principle of proportionality has not been properly assessed before embarking on implementation of biometrics in travel documents. ICAO recommendations and existing European directives leave too much freedom on the implementation, which makes a proper EU wide assessment on proportionality very difficult.

Based on a clear usage scenario and a thorough proportionality assessment a legal framework should be put in place to ensure compliance with data protection legislation. Generally privacy seems to come last in system design although Privacy Enhancing Technology (PET) can enhance purpose binding and inhibit function creep (i.e. dis-proportionality), provided that these technologies are being embedded in the overall design from the very beginning.

Due to a lack of experience at application level there is little common understanding about the design of large ID systems including biometrics and its underlying processes. People do not understand what is behind a system and cannot therefore make a judgment as to its proportionality; this can easily lead to a general distrust towards those systems.

Concerns:

- Having no clear purpose for the use of biometrics impedes the assessment of proportionality.
- BAC as a means to secure the personal data in the passport chip is being considered as insufficient – and therefore not proportional – to the value of the data being held.
- Lack of experience with biometric enabled ID-systems lead easily to distrust towards those systems.

Potential solutions:

- All personal data contained by the e-passport chip should be secured by EAC
- Unnoticed reading of the chip should be avoided by securing the chip with a ‘Faraday cage’.
- Data protection issues should be brought to the agenda and the DPA’s empowered and enabled to exercise control.
- The actual use of biometric identifiers and other personal data should be clearly specified and restricted.
- Existing PET’s to be applied in large scale ID-systems should be assessed as to enforce purpose binding.

- General guidelines (as detailed as possible) for systems design should be developed.
- The purpose of the system, its main underlying principles and the benefits that it can bring should be communicated to European citizens and brought on the public agenda.

3.3.5 Best practices in privacy and data protection guidelines/legislation

At European level there is a requirement for more guidelines on how to align the privacy and data protection principles through all member states and on how to implement this legislation in a harmonised way. Much existing work is being done, but there is not enough coherence in the implementation of the various guidelines and recommendations. EU projects like **FIDIS** (Future of Identity in the Information Society), **BITE** (Biometric Identification Technology Ethics), **PRIME** (Privacy and Identity Management for Europe, the **Article 29 Working Party** but also the work of **CEPS** (the Centre for European Policy Studies), the **COE** (Council of Europe, Treaty 108), the **OECD** (Organisation for Economic Co-operation and Development) and the relevant communications of the **European Commission** are important examples of existing work in the field of privacy, data protection and biometrics.

For self regulation there needs to be trust in order for this to be effective so that you do not have to rely on Vendors claims. Independent bodies (like testing and certification organisations) need to certify the systems and procedures in order to establish this trust, which will also encourage trust for the citizens.

Existing privacy principles do cover most issues when applied to biometrics. However, by the nature of biometrics itself, not all aspects are being covered. Especially the irrevocability of biometrics brings additional challenges that need to be addressed.

Concerns:

- The supervision of the implementation of National Passport Schemes is unclear and insufficient supervision can lead to a range of problems.
- ICAO standards do not describe yet in detail the use of more complex encryption when used in travel documents whilst at the same time there is a call by DPA's and other civil rights organisations for more sophisticated encryption to make the procedure safer.
- There is no generally agreed interpretation of existing Privacy and Data Protection regulations.
- Biometric data are partly different from 'normal' personal data (e.g. irrevocability). For that part no regulation yet exists.
- Existing work in the field of privacy and security in biometric enabled systems shows only a low level of overall integration and adaptation.

Potential solutions:

- To make better use of existing regulations and directives through stronger cooperation and a more effective communication and use of best practices.
- To create additional data protection guidelines for specific aspects of biometrics that are not covered yet.
- To issue European and EU mandated guidelines to be recommended for implementation in national laws.
- To establish DPAs with regulatory powers in all EU member states.
- To achieve certification of systems.

- To develop and implement protection profiles (e.g. Common Criteria) although their effect may be limited.
- To issue best practice guidelines which cover all aspects including training of operators.

3.3.6 Current status in harmonisation of privacy and data protection policies/regulations in Europe

There are three main stakeholders in the area of data protection supervision:
- National DPA's
- Article 29 Working Party
- European Data Protection Supervisor

Currently available European legislation is:

- **Directive 95/46/EC**

  The protection of individuals with regard to the processing of personal data and on the free movement of such data
- **Directive 2002/58/EC**

  The processing of personal data and the protection of privacy in the electronic communication sector
- **Regulation 45/2001**

  On the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

You can find al these documents and many more information on ongoing projects and legislative actions on http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

There is not necessarily a need for more regulations, although certain aspects of biometrics are not being covered by current legislation. However, more thorough implementation of the existing directives and regulations is long overdue. Because of the different national laws of the EU member states, efforts need to be undertaken to issue guidelines. In addition to the Article 29 itself, the Article 29 Working Party may be the best forum for producing guidelines. In the end, the European Commission is the guardian of the treaty and has therefore the obligation to supervise national implementation. By delivering opinions on new proposals for EU large scale biometric systems, the European Data Protection Supervisor (EDPS) also contributes to the development of these required guidelines.

Concerns:
- Biometric data are not fully covered by existing guidelines and legislation and therefore might compromise privacy and data protection legislation.
- Cultural differences between member states lead to different interpretations of current legislation, which will lead to a different approach to the handling of biometric and other personal data in each EU member state.

Potential solutions:
- Assessment of the position of biometrics within existing legislation.
- If needed, and this is expected to be the case, additional guidelines for dealing with biometric information need to be developed on a Pan European level.

3.3.7 The role of standards and testing/certification in the protection of privacy and the increase of trust in biometric systems

As already described the establishment of European capabilities on testing and certification of biometric components and systems is relevant and urgent. Preparatory work needs to done in order to establish such capabilities:

1. Outlining the need for testing and certification at end user level and defining the 'business case'.
2. Making an up-to-date inventory of:
    a. What needs to be tested based on end user requirements.
    b. Most relevant existing testing schemes.
    c. Existing competencies at European independent testing laboratories in the area of biometric performance, interoperability, and security testing.
    d. Existing work on standardisation and testing (within and outside EU).
3. Based on the outcome of the inventory:
    a. Mapping of the user requirements on the existing competencies.
    b. Performing a gap analysis to determine what existing competencies can be used and what needs to be developed.
4. The final outcome of the project will be:
    a. A European Biometric Testing and Certification Roadmap, including research targets.
    b. Work plans and coordinated actions for the further development of the European biometrics testing and certification network.

Concerns:

- There is no harmonisation of the use of biometrics (i.e. targeted application scenarios) on a European level.
- There is a dependency on vendors' claims instead of independent test results.
- A lack of interoperability between different vendors can lead to vendor lock-ins and/or to significant delays in the procurement processes.
- A lack of conformity of standards can lead to poor interoperability between national systems and can block the way to efficient and effective cooperation between member states.
- Projects can run into excessively high costs due to ad hoc approaches by member states.
- The above mentioned concerns can lead to a decrease of the level of overall trust into these systems.
- Not having European testing and certification capabilities and criteria give way to a stronger influence from non EU industry and governments (like Asia and the US), which as a result will weaken the competitive position of the European industry.

Potential solutions:

- To define European requirements on functional design of biometric enabled applications.
- To establish European guidelines on the system design of biometric enabled public and private applications.

- To set up European capabilities for testing and certification of biometric components and systems, including Europe based test databases.[72]
- To set up an independent group of experts that bring together existing knowledge and that can advice on biometric issues so a uniform approach can be developed.

[72] The BioTesting Europe project aims to address these issues on European testing.

4 Results from BioTesting Europe Project

The following section provides the findings reported at the conclusion of the BioTesting Europe project in June 2008 "Towards European Testing and Certification of Biometric Components and Systems: the Way Forward." The results of the BioTesting Europe project are based on the consultation of a large group of stakeholders within Europe through structured interviews and questionnaires to end users, vendors, testing laboratories, independent experts, government agencies, border control agencies and many others.

4.1 Introduction and Goals of BioTesting Europe

The project BioTesting Europe –funded by the European Commission under PASR2006,[73] aims to set out the prerequisites for the establishment of testing and certification capabilities on biometric components and systems in Europe. This is driven by the fact that large scale national and international biometrics based identity systems (passports, visa, eID cards) are being developed and procured, mainly by governments and the European Commission (EU VIS / BMS). Also the increasing use of biometrics in access control and surveillance applications drives the increasing need for developing more trust and predictability of biometrics based applications.

According to EC policies that have been stated in the Hague program:

> *"A coherent approach and harmonised solutions on biometric identifiers and data are necessary in the fight against illegal migration and security."*

It is a fact that biometric verification and identification methods are spreading in more and more application fields, including pan European border control systems and applications (e.g. ePassports, VIS/BMS, National eID-Cards). In applications where biometric data may be processed by components of different vendors, the interoperability of the components and systems is of critical importance. While this requires standards and those standards are developed by the relevant bodies inside ICAO and ISO/IEC there are no criteria to qualify to which extent a system under test, that claims interoperability and conformity to said standards, actually complies with those standards.

Given the need for a more coordinated European approach and given the fact that 25 EU member states are now implementing the new electronic passports which include biometric identifiers, enormous risks are being created in terms of efficiency, security and convenience of the overall systems. Still there are no adequate testing criteria, nor compliancy tests to verify conformity of the biometric components and systems to certain standards, nor European testing centres to perform these tests and publish the results; for instance a white list of components that is compliant to a certain standard. This means that currently no vendor or systems integrator can guarantee interoperability or compliance to existing standards, resulting in ad hoc solutions at national level, often with proprietary products and systems. The overall result is more market fragmentation that impedes Biometrics evolving into a European motor for growth and jobs while safeguarding and benefiting society as a whole.

On-going work within the international community to define standards for the implementation and testing of biometric devices and systems is mainly performed under the influence of strong political forces, such as the Homeland Security border control requirements for the US VISIT programme. There is a danger within Europe that European requirements will be neglected and that the US-centric focus will extend into the implementation and test regimes,

[73] BioTesting Europe - "Towards European Testing and Certification – The Way Forward", June 2008 - PASR 2006, Preparatory Action on the Enhancement of the European Industrial Potential in the Field of Security Research of Biometric Components and Systems.

leaving European governments and companies with little choice than to utilise the US formulated standards and probably US compliance testing in US testing laboratories. This paves the way for US biometric products vendors and systems integrators to gain a strong position on the European market, thus leaving a less favourable competitive position for the European biometrics and related industries.

The European Commission is concerned about its ability to be able to adequately characterise the necessary requirements for the future pan-European biometric programmes and to provide a Europe-based capability to perform its own compliance and other testing. BioTesting Europe© aims to address these concerns by unifying the European interests and providing a direction that shall lead to the development of proper European testing capabilities in the area of biometrics.

In order to establish European interoperability within the large scale cross national identity management systems, more specific requirements for designing testing and evaluation schemes are needed. An integrated approach is the absolute success factor in achieving these goals. That means simultaneous actions are needed that facilitate alignment between all levels of involved stakeholders, such as testing laboratories, accreditation organisations, industry and ultimately end users. In parallel input will be provided in order to establish links with related ongoing European research activities.

Although much work has been done in the area of independent testing of biometric systems, there are still many open issues to be resolved due to the fragmentation of efforts and the lack of input by end users. The results of many tests in the last few years have shown that test results are still not comparable and that interoperability of biometric technology is not yet achieved. To improve this situation, this project aims at setting up a framework for a European network of testing laboratories for performance and interoperability testing and security evaluation of biometric systems. In order to join forces a business case for such a network is needed, that involves all stakeholders. However, the lack of clear end user requirements signals that it is too early to start directly with in depth technical discussion and setting up of the relevant certification schemes.

Therefore the project has focused on:

- Outlining the need for testing and certification on the end user level and defining the 'business case.'
- Making an up-to-date inventory of:
    - What needs to be tested based on end user requirements.
    - Most relevant existing testing schemes.
    - Existing competencies at European independent testing laboratories in the area of biometric performance, interoperability, and security testing.
    - Existing work on standardisation and testing (within and outside EU).
- Based on the success of the inventory:
    - Mapping of the user requirements on the existing competencies.
    - Performing a gap analysis to determine what existing competencies can be used and what needs to be developed.
- The final outcome of the project is:
    - A definition of the basic requirements for a European network for testing and certification of biometric components and systems.
    - A European Biometric Testing and Certification Roadmap, including research targets.
    - Work plan and coordinated actions for the further development of the European biometrics testing and certification network.

4.2 Conclusions of BioTesting Project

The starting point of BioTesting Europe© is that Europe needs testing and evaluation capabilities in order to achieve harmonized biometric solutions which are interoperable, efficient and reliable in their use. Because the main application areas in the biometrics market place are passports, visa, electronic ID Cards and registered travel programmes, BioTesting Europe chose European members states' governments, government agencies and the European Commission as the primary client targets.

As the need for unified test and certification processes is becoming more urgent, especially as regards border control application among all EU countries, a pan European approach on testing and certifying biometric components and systems is a challenge for all stakeholders involved and probably more so for those countries and organizations having no or limited expertise in the field of biometrics.

4.2.1 Inventory

A comprehensive inventory of the existing testing capabilities and end user requirements has raised a number of issues that are presented below:

One of the biggest problems is the choice of a reliable biometric system, which is predictable in its performance and costs of ownership. Interoperability is a big concern for all, as well as performance and security, and the impact of biometric procedures at the front end processes such at embassies, consulates and border control check points.

It is of particular importance to make sure that external expertise bought in by those countries is accurate and independent. However, such expertise is not widely available. Currently no vendor or systems integrator can guarantee interoperability or compliance to existing standards based on independent third party opinions (such as test laboratories), often resulting in ad hoc solutions on national levels, risking lock-ins with proprietary products and systems.

It is important to certify that common requirements are met, and that the results of these examinations are comparable to evaluation made by others. Therefore it is necessary to define standardized requirements for biometric products, as well as unified, standardized testing and evaluation procedures.

To avoid needless and expensive repetitions of separate and unrelated evaluations, trusted accredited organizations should perform uniform tests, thereby following standardized processes.

By choosing to buy certified biometric systems, the buyers would be sure that the product fulfils all the needed requirements, that way reducing the need to test on their own. Vendors only than can take responsibility on compliancy to certain specifications if their products can be tested on basis of uniform and commonly agreed test schemes and methods.

The overall conclusions of the inventory are:

- Independent testing and certification will improve the overall trust in biometric systems.
- According to stakeholders most relevant and urgent areas to be tested and certified are:

    - Interoperability (especially image interoperability, but also on the level of processes and procedures).
    - Performance (mainly failure to enrol / false acceptance / rejection).
    - Security (spoofing, data protection).
    - Ergonomics and human aspects (enrolment and verification process, kiosks, etc).
- Lack of knowledge and experience leads to unclear requirements and costs situations, resulting into:
    - Vendor-driven pricing.
    - High prices because vendors include risks and costs for benchmarking and pre-tests.
- Independent testing will significantly lower the short term and long term costs of biometric procurements, because there will be:
    - Less vendor dependency, clearer pricing and costs structure, more competitive pricing.
    - Significantly lower integration costs.

4.2.2 Main needs and gaps

Based on the comprehensive inventory of the existing testing capabilities and end user requirements, a gap analysis has been performed in order to identify the gaps in those capabilities, while mapping the existing capabilities against the end user requirements. The main needs and gaps that are not yet being addressed properly are:

- Knowledge transfer and co-ordination:
    - Test results repository,
    - Co-ordinating standardisation and development of standards,
    - Design-for-test and test development consultancy,
    - Auditing,
    - Application profiles development and assessment.
- Methods and tools:
    - Test strategies,
    - Tools for algorithm evaluation,
    - Testability tool set and design methods,
    - Standard test APIs,
    - Conformance testing tools,
    - Tools for visualisation of results and data mining.
- Test data:
    - Development of (synthetic) test databases,
    - Development of reference data for testing conformance/interoperability/quality.

The products and services that are needed to address the current demands have to be structured along the phases of the procurement and development of biometric systems:

- Specification (functional requirements, performance needs),
- Testing during procurement (benchmarking, selection),

- Acceptance testing,
- Performance monitoring during deployment.

4.2.4 Short-term and mid-term priority actions

The following are priority actions required to address urgent needs and to start European testing activities:

- Establishing a co-ordinated dialogue with customers in order to channel the BioTesting services to the clients.
- Co-ordination of activities regarding (low level) test issues.
- Mobilizing the skills to deliver the first test products and services. For the short term these will mainly be consultancy, certain straight forward testing to performance and conformance issues, repository of test data/results, specification support and training and education

In the mid term BioTesting Europe will seek to address the following issues and challenges:

- development of a certification/accreditation program,
- communication activities,
- study on impact analysis of wide spread use of biometrics,
- acquisition of large scale test database,
- improving interoperability of fingerprint templates from different vendors, (see also www.mtitproject.com),
- development of vendor independent quality test tools for fingerprint and face images,
- expanding the partnership network,
- promoting and developing pan European cooperation.

4.3 Inventory and Gap Analysis

4.3.1 Inventory

In addition, an inventory has been made of standards and existing structures and capabilities for testing of biometric components and systems. The outcome is:

- A lot of testing is needed due to the large scale projects there are being implemented (e.g. biometric passports, European visa). This included test execution, test development and design for test of components and systems.
- The majority of testing is conducted by the suppliers and by the customers (the organisations deploying biometrics). This by far exceeds the amount of testing being conducted by independent test organisations. However, it is acknowledged that supplier testing may oppose interoperability assessment in which multiple vendors are involved and that customer testing is rather ad-hoc.
- Most relevant standards have been developed or are currently under development. However, in several cases those are not ready for use or not fully supported/implemented by suppliers yet. Also the current developed standards only cover a part of the chain.
- There are only a few test organizations in Europe that have (parts of) the appropriate knowledge and experience.
- The white-lists of tested biometric products that are maintained by some organisations are not generally accepted by the stakeholders. The reason for this is

that the results of a biometric product test is directly related to the application of that product and has no general validity.

- The inventory also shows the existing accreditation, testing and certification in Europe and internationally. To be accepted by most governments, a network for testing and certification of biometric products should fit into this structure in order to capitalize upon existing knowledge experience and practices.
- The most mentioned requirements for biometrics systems are operating speed, accuracy and interoperability.
- The most relevant, as well as urgent subjects to addresses are the further development and implementation of standards that support interoperability and performance, such as image quality, biometric matching performance (FMR/FNMR), security (spoofing) and ergonomics. Also training and education of operating personnel and program managers has been highlighted.

4.3.2 Gap analysis

For the priority applications in border control being considered in this project, the testing of biometrics is being carried out by suppliers of biometric products, by the organisations deploying the biometric systems and by test organisations.

It is clear from our consultations that by far the majority of testing is being undertaken by operators and their suppliers. Only in a minority of cases independent test organisations are significantly involved. Cooperation between member states on an EU level is only seen in specific cases, e.g. at the BIG. Furthermore, it is thought unlikely that an increased amount of third party testing would reduce the amount of testing conducted by either suppliers or customers; however, such additional testing will improve the level of assurance of deployed systems and reduce overall costs of individual testing if tests are commonly agreed and distributed to all EU member states.

On the basis of the Inventory, the user requirements are depicted as follows:

- Technology and Product assessments
  In order to make a selection of suitable biometric modality, vendors and their products, operators need independent, repeatable and accessible test results. These results should focus on operating speed, accuracy and interoperability.
- Component testing
  Deals with sub-systems built with biometric products such as kiosks or credential checking in the back-office. Focuses on biometric performance, security, ergonomics and interoperability.
- System testing
  These are the end-to-end systems that implement the buyers' business processes. Directly interferes with confidentiality and sometimes even national security policies.
- Standardisation
  This subject covers products, methods and tools. Is primarily driven by interoperability improvement and cost reduction.
- Certification
  Involves (vendors of) products and services, methods and tools. Aims at increasing confidence and quality.
- Training and Education
  Involves vendors (experience), test labs (independent technical knowledge) and

independent consultants (implementation, project design etc.) and is targeted to the operators.

It may be concluded that the main gaps in European testing capabilities are:

- Open questions in performance,
- Fragmented approach to testing,
- Areas not sufficiently tested (usability, accessibility, conformance, interoperability, quality, security),
- Lack of suitable test data,
- Lack of certification schemes,
- No unified approach to understanding test results,
- Insufficient testing capabilities,
- Lack of commonly shared knowledge and experiences.

4.3.3 Training and education

Training and education has been mentioned several times be the stakeholders in the interviews and questionnaires, especially in the answers of the operators (i.e. the end users). Because the functional requirements for biometric enabled ID-systems are the starting point for further specification and (later on) testing, it is of utmost importance that (future) operators are well aware of the various aspects of biometrics and its impact on processes, procedures and system specifications.

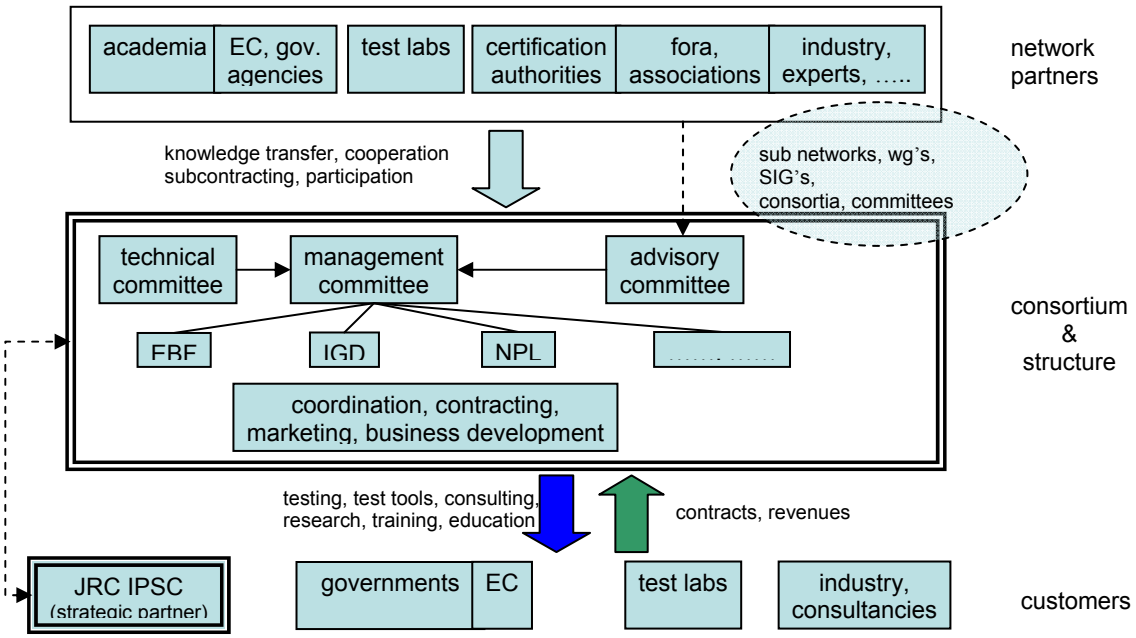
There is a need to ensure lessons learned are shared with other programmes. Training requirements mentioned by operators are:

- Training would give a better understanding to the first line officers and a better acceptance of this tool. Training is needed, but not accomplished.
- Training support concept.
- Communication of reason and goals of the biometric system
- Explaining the general way of function.
- Handling.
- Work flow in normal process.
- Work flow in special situations like false acceptance or false rejection.
- Training how to cooperate with the public.
- Training for border guards must be provided (Frontex).
- More practical experience with the use of visa biometrics control at the border crossing has to be gained.

4.3.4 Organization

It has always been the target of BioTesting Europe not only to deliver the results of a study through a report, but to establish a sustainable infrastructure in Europe to provide independent testing, consultation and training services to the community. Currently the BioTesting Consortium has developed an organizational structure which accommodates the development and delivery of the appropriate products and services.

The organizational structure is as follows:



5 Input from Expert Meeting and Final Conference

This section aims to present the numerous challenges that face large-scale biometric deployments, with a specific focus on systems originated in Europe in the public sector.

First, a brief synopsis of the lessons learned and challenges identified at the end of the study's different actions (in particular, Expert Meeting and Final Conference) are outlined. Secondly, a discussion of a relevant evolving challenge concerning the *automated border control scenario* is analysed in depth.

5.1 Expert Meeting

The expert meeting gathered experts representing several important disciplines: technical issues, research, testing, standardisation and data protection.

An insightful day of discussions provided the opportunity to raise the significant issues facing large scale biometrics deployment. What is evident from the results is all experts agree that in order for systems to be deployed with any amount of success, all the above categories must be considered. Overall, the challenge that was shared by all experts is that biometrics systems must have a purpose and this purpose for deployment must be explained clearly to the users of the systems or else problems such as privacy infringements, faulty or misuse of data or citizens' lack of trust towards their governments could occur.

The most relevant points articulated in the expert meeting were:

- It is not certain to which extent biometrics will increase security in terms of preventing illegal actions. For example, there are still concerns of false fingerprints, multiple names in biometric databases and biometrics skimming.
- It is not sufficiently effective how current biometric systems address multi-disciplinary issues in their deployments. For deployments in large scale projects to be successful, it is essential to consider not only the technology aspect but also take into consideration legal and regulatory terms, economic costs, data protection and privacy, social impact regarding public acceptance and convenience, psychological reactions and in general understanding if the purpose of the system corresponds properly to the implementation.
- Many detailed complications arise from non-biometric technologies such as unauthorized reading from RFID chips. Therefore, it is imperative to effectively combine the various technologies and organisational issues to address the security problems.
- There is a lack of experience with very large-scale and long-term use of biometrics. With the upcoming SIS II system to be launched, this will be a test of major proportions.
- Many standards exist (and maybe too many) but there is a severe lack of compatibility. Conformance testing standards must be implemented to solve the major problem of interoperability. Not all of the numerous ISO standards are interoperable For example, there are 2 different test suites for ISO/IEC 19794-2 (Information technology – Biometric data interchange formats - Part 2: Finger minutiae data), one provided by ILO and one by Fraunhofer that yield different results for the same set of data. Therefore, a common standard framework must be created.
- There are almost no certification procedures in Europe for biometric systems. Testing and certification capabilities in Europe are needed in order to improve interoperability, conformance, security and overall trust, based on European requirements and values. The BioTesting Europe project is a first step in the right direction, but more needs to be done.
- Error rates strongly depend on environmental issues, which strongly would call for testing, certification and training standards. One expert expressed that although

technology may and should be improved, current error rates will not allow relying on biometric systems for high secure areas and today's biometric technology may be improved against attacks. Therefore it is not secure enough for deployment in unattended areas. There is also a lack of specific criteria for quality assurance.

- There seems to be reluctance to establish, fund and animate a high-level expert group to support the pan-European deployment of Biometric systems – the European Biometrics Expert Group (EBEG) was expected to start operations in the beginning of 2007. The EU Joint Research Centre has, nevertheless, expressed its interest in continuing with stated EBEG objectives since working towards them could assist EU policy makers better understand what the possibilities for future biometrics deployment are and which applications should not use biometric technologies.

5.2 Final Conference

Eventually, the Final Conference focused on the "big picture", announcing the ultimate large scale biometric scenarios planned in Europe together with the main issues that are still left open.

The conference approached the topic from different entry points:

- The emerging top-down concepts articulated by the European Commission.
- The actual status of research presented by EC-funded projects.
- The actual status of EU large-scale biometrics, with also some insight to the experience reported in the U.S. and Canada.
- The controversial issues of security versus data protection, prevailing in many presentations and discussions, concisely covered in those about the Visa Information System.

The importance of striking the proper balance between security and privacy is acknowledged by this study as the right approach to take with biometrics. However, this issue is not as straightforward because the above EC motto can be interpreted in many diverse ways as was demonstrated with the event's specific presentations and discussions. Unfortunately, there is still quite a gap between what biometrics technology promises and what has already been achieved – expectations vs. results. In addition, there is still a lack of necessary and urgent political decisions that need to be made on a European level to tackle the issue of privacy.

The **top-down concepts** call for a fully integrated Automated border control scenario covering personal data including multi-modal biometrics from European citizens as well as from visa applicants and third-country citizens exempt from visa. Although the concept has not been presented in detail during the meetings, the scenario will be basically derived from the U.S. approach, i.e. collecting or combining all data and biometric samples that will be available and have it stored in gigantic databases accessible to many interested authorities. Citizens will accept the scenario provided as long as security is increased, illegal immigration is prevented and the (Schengen) border control can be quickened.

The **research–oriented presentations** contribute to the view that there still are a lot of technical and functional issues to be solved before biometric technology and its integration can be considered as mature enough to make European Security depend on and trust biometrics. The research topics range from sensor technologies over multimodality issues, the lack of standards for calibration and testing (i.e., to make devices comparable and interoperable) and the problem that there is no experience with systems that require the management of large amounts of data and possess complex functions.

Presentations about large-scale biometrics deployment status (which is the central topic of this report and the objective of this study) show that biometrics are yielding positive results in law enforcement with high quality assurance efforts, as well as for straight-forward access-control systems, whereas Border Control is primarily focusing on large-scale enrolment (e-passports) or pilots for the Visa Information System. Remarkably, there was no significant focus presented at the final conference on law enforcement experiences, although this is so far the only large-scale interoperable deployment area in Europe.

What can also be concluded is that U.S. and Canada have different attitudes about the use of biometrics in border control: while the U.S. acquire all data possible from travellers to be matched with any reference (but completely exempt their own citizens), Canada regards biometrics solely as a means to improve the travel document's quality and robustness against fakes and gives high priority to data protection. In terms of technology, the fact that the U.S. are extending from 2 fingerprints to 10 could have a large impact on future European approaches, because this may imply that the quality of the data is not sufficient.

Data protection and privacy issues remain at the forefront of discussion amongst all relevant stakeholders. There is also a need for public awareness by the EU and the Member States to directly respond to their citizen's expectations.

Repeatedly stated issues continually raise the concern about data quality in the multi-national, multi-database and multi-user concepts, with the problem of correcting wrong data and preventing function creep and uncontrollable access with outsourcing. Other important items for discussion centred on the lack of practicable solutions for children, being engaged in many areas by biometric systems (technical/enrolment, organisational/access lanes and legal/responsibility for data).

Discussions about further developments brought up the concern about "technology totalitarism" when every function that is technically possible would be implemented leading to a thoroughly monitored, "Big Brother" surveillance society. The European Commission should aim to take countermeasures by preaching the importance of securing European citizens without infringing any of their rights to privacy. One way of proceeding in this direction is to make sure that the EC can obtain decision-relevant information about biometrics deployment taking place at national level when public funding is granted to these kinds of pilot projects. It is necessary that no significant details on the system deployments are kept secret. In turn, the improved information circulation could help better understand the success and best experiences associated with the projects.

5.2.1 Future areas of application

This section briefly offers some ideas as to future areas of application, which was an item of discussion. Considering the numerous factors surrounding biometrics deployment (standards, interoperability, data protection, etc.), the following two suggestions are based on feedback gathered at the final conference

Banking and e-commerce: Biometrics would replace or complement authentication now based on PIN or password. This would be a verification process which could improve secure authentication provided that the link of personal data with biometrics is secure. However, currently reported error rates would be not acceptable at automatic teller machines.

Risk analysis by behaviour: Concepts are being developed to filter individuals to be considered as a risk based on behaviour patterns calculated from travel itineraries, surveillance results and other available information. Many of such application ideas would conflict with existing data protection and privacy legislation in Europe and in terms of society potentially lead to the vision of "standard-compliant citizens" not daring to do anything which is not expected by the "standards". This can not be compliant with the understanding of European democratic values

6 Challenges and Issues to be addressed in Large-scale Biometrics Deployment

This section aims to present the numerous challenges that face large-scale biometric deployments, with a specific focus on systems originated in Europe in the public sector.

First, a discussion of a relevant evolving challenge concerning the *automated border control scenario* is analysed in depth. This application has been chosen over others due to the current relevance of many recent, ongoing and future deployments such as: the second generation of EU biometrics passports, the ambitious VIS project, the enormous database system as part of the transition from SIS to SIS II, test trials from BioDev II and the registered traveller programmes such as the iris trials at Heathrow, Frankfurt and Schiphol Airport.

The idea of "Automated Border Control" is a frequently discussed topic at the moment. Therefore in the following section the challenges surrounding this innovative scenario will be presented.

Second, overall challenges are presented that cover the general state of large scale biometrics deployment.

Third, challenges according to biometrics technology function will be detailed followed directly by recommendations on how to address the challenges and potentially solve them.

Fourth, recommendations are provided that concern the findings from the Security and Privacy report. There are in fact some themes in common that have been presented in this report and some contain similar findings on security and privacy. Therefore, since the two studies agree on several points, we intend to list all of the suggested recommendations together as they are all relevant for the purpose of this report. The convergence in the results of the two studies in itself strengthens the weight of the conclusions and recommendations formulated in the two different contexts

Fifth, overall conclusions are given that sum up the findings gathered in this study.

Lastly, actions to be taken will be outlined as to how it is suggested that European policy makers proceed in approaching the various issues.

6.1 EU-wide Automated Border Control

What is today described as "Automated Border Control" will eventually be in the future the combination of passport/visa control with law enforcement and crime/terror prevention. Functionally, it will consist of existing and future biometric database checks, centralised and decentralised, as well as possible match-on-card (MOC) checks for EU citizens. The political intention of aiming to prevent crime and terror will require additional surveillance functionalities which have not been laid out yet. When completed, **it will be the largest data conglomeration in the world**, with unprecedented dimensions of size, complexity and possible consequences. On the one hand, it is promoted for providing more security to the citizens by preventing illegal immigration and finding suspects or terrorists before they can do harm; on the other hand critics fear a variety of negative results ranging from technical failure to omnipresent surveillance. It will be beyond this project to cover every particular issue of this controversial discussion.

However, the concept must be explained in more detail than it is at the moment.
Measurements must be created that describe if and how automated border control can achieve its promised benefits, how it will meet the challenges and how transformation into "technology-totalitarism" will be prevented.

6.1.1 Particular challenges for passport and visa control

Whereas the process of issuing passports including biometrics is defined by an EU regulation, most parts of the border control process is under national legislation, although any individual entering into a Member State has the freedom to travel anywhere in the Schengen area. Based on this study's analysis, this is an ever-growing problem that needs to be addressed especially when it comes to the challenge of long-term visa overstaying. Some elements in the concept are of particular concern and under intensive discussion, because they have considerable impact on data protection. Several challenges have been identified and will be detailed below:

Challenge 1: Different data qualities that lead to inconsistent results.

The concept is based on personal and biometric data to be captured in locations all over Europe (for passports) and worldwide (for visas) using different devices and implementations and different calibrations with technical standards not being considered as mature. Further, including surveillance information will in fact introduce unpredictable data qualities from various sites. As a result, much data in different qualities will be available which may or may not be assignable to particular individuals. This is already a problem in law enforcement and does not only apply to biometrics. For example, it has been reported that transliterated names from Cyrillic or Greek result in different spellings depending on the country where performed.

An Automated Border Control scenario will be requested to arrive at the same result at any border control point for a given individual's personal data collection regardless where it has been captured. This is not a trivial task and will require tight standardisation of such data and its quality, but also of the matching device's calibration and human decision when a probability arises that (low-quality) surveillance information would be linked.

Challenge 2: Currently no age limits exist for the collection and use of biometric identifiers (fingerprints and photographs to be used for verification and/or identification purposes)

Biometric enrolment from children and elderly people causes many technical and organisational difficulties and it is questionable whether those age groups are imposing a relevant terrorism or immigration risk.

Fingerprinting children has been debated with the fight against child trafficking, but there are no serious assessments so far that demonstrate evidence on necessity, proportionality and feasibility.

Challenge 3: Outsourcing of part of visa handling process to external service providers

One intention to outsource is to facilitate applications and release applicants from travelling long-journeys to a consulate. However, because of the sensitivity of the biometric data linked to personal information, and the potential risks for both data security and protection, it is an important issue whether the processing of visa applications by an external service provider in a third country could be appropriate. If outsourcing is allowed into any country and

processing is performed in a poorly managed way without adequate data protection and data security safeguards, there would be considerable risks for individuals and for the integrity of the whole visa-issuing process.

Challenge 4: Potential of function creep

VIS will contain data from individuals where each will set up a complete identity. This is of high value for arbitrary surveillance and data mining, especially when the data is processed under uncontrolled outsourcing conditions or access would be given to users not robust against corruption.

Commercial interest in such data collections articulated by future lobbies is also expectable. The impact of the use of biometrics in such a large and complex system is going to be significant, in particular on the privacy of a great number of individuals but also organisational and technical challenges.

6.2 Overall Challenge: Political Regulations keeping Outsourcing under Control

For EU-wide large scale deployments, many features of those systems already reported will grow together into a gigantic electronic conglomeration of personal data with the risk of creating a surveillance society.

Upon completion of the central VIS and Schengen II databases, complemented by the already existing EURODAC and access to decentralised but interoperable AFIS data, these large scale biometric systems would not be functionally separated any longer. It has not been decided yet, whether and under which regulations the data processing or some portions will be outsourced to companies which could reside outside the EU for cost-saving reasons.

Therefore a prominent overall challenge focuses on the consequences that could lead to a loss of political control over the data and its practical use, if there are no clear measures with due regard to necessity, privacy and proportionality, strong prevention of data mining, phishing expeditions, profiling and other function creeping.

Existing regulations cannot offer guarantees because currently data collection is performed on EU legislature, whereas data usage is placed under national laws. Existing systems such as law enforcement have strict measures for data quality, both for biometric and non-biometric data. It has not yet been disclosed in detail whether or how such measures will also apply on data to be kept in the large central databases.

6.3 Large-scale Biometrics Deployment Challenges by Function and Recommendations

Based on the findings that have been elaborated in this report specific to challenges of large-scale biometrics deployment, the following **recommendations** for European policy makers are listed according to function:

Function: Enrolment lacks a common sufficient framework.

The enrolment process is critical for data quality and for all further matching processes that depend on quality. Failures in enrolment could decrease performance and lead to wrong decisions causing invasive or discriminate follow-up actions for innocent people. The time is appropriate to address the issue to form a common framework for all enrolment procedures.

Recommendation I

The enrolment process must be standardized and certified on a European level. This must include data quality control (biometric and non-biometric), usability for the enrolment application and user training for operating personnel. A un-enrolment process must also be implemented to account for wrong or expired data

It is strongly suggested that the enrolee must be completely aware of the purpose and range of the application and, except for crime prosecution, should have an opportunity to view and verify if the data is correct.

There must be equivalent and acceptable fallback solutions to prevent discrimination of people not able to enrol in case of failures to enrol and failures to acquire.

EU-wide certified **procedures for "un-enrolment"** or data modification must be created that are only operated by strictly authorized and strongly supervised users while transparency must be guaranteed towards the data owner. This must include mandatory data removal when an application or feature expires.

It is advised to implement a Europe-wide standardisation, certification and accreditation scheme. This is an urgent prerequisite to make an interoperable Automated Border Control function properly. Such a scheme should adopt the experience from existing ones such as Prum.

Function: There is no perfect correct answer for storage of biometrics data, but central databases pose more problems than other options.

Once data is officially stored, it needs to and most likely will be trusted. If it is incorrect, it will be very difficult or impossible for the individual to prove its authenticity.

Not just the biometrics on their own, but their combination with a person's identity is posing risks of ID theft or usage for unintended purposes. Biometric database storage can solve problems (e.g. lost or stolen passport) when conventional identity proof cannot be presented (provided that every citizen is enrolled), whereas token storage leaves the data under control (and responsibility) of its owner. Therefore it cannot be stated that one of these options is absolutely better than the other.

A review of the findings concerning central and decentralised databases, and tokens:

Central databases:

- Difficult (in terms of decision making) to have wrong or poor data corrected.
- Technical issues with very-large scale statistical searches (performance and error rates can increase exponentially).
- Possibility that data already stored would be used for other purposes than originally intended, even against the will of a particular EU Member State.
- Many users are authorised to have access most likely under different legal frameworks.
- Lack of experience, unresolved issues with backup and outsourcing procedures.

Decentralised databases (central databases linked together):

- Increases the risk potentials for wrong decisions by having the same person's data in different qualities giving unpredictable matching results.
- Risk exists of having the same data being kept safely in one country, but undisclosed in another.
- On the other hand, correcting or deleting incorrect data is easier in decentralised environments. However this implies a decision whose data is the correct one and procedures to correct it in the other databases.

Tokens:

- Since tokens can be lost or stolen, they must provide high data security to prevent misuse.
- If data on the token is wrong, it usually can not be corrected on the token.
- User responsibility for the token may cause problems in case of children, handicapped, etc.
- With decisions (like border entry) based only on information in the token, lost or stolen tokens could result in identity loss which will not be resolvable at the entry point.

Recommendation II

Based on the advantages and disadvantages of the storage options, central databases should be avoided where possible. In the case that it is decided to use central databases, high data quality must be guaranteed.

There should be a legal obligation and practical procedures in place for enrolled persons to have their stored data revoked or corrected when there is a possibility that they are not correct or of poor quality. One potential solution in this scenario is to implement a European-wide, standardized complaint process.

Biometric data should also not be stored raw, but rather in encrypted templates which achieves the same matching result but reduces the risk of ID theft and some function creep.

The biometrics identifier should not automatically lead to the connected personal data as this should only happen in correspondence to a clearly explained purpose by as few authorised users as possible.

Function: Accuracy and standardisation of matching processes.

Unlike PIN-based matches biometric matches do not decide whether an inquiry produces a hit but rather portrays the probability for a hit. The interpretation of a hit with all its consequences depends on the calibration, application and the user. Therefore in the multi-database, multi-application and multi-user scenarios proposed such decisions could (and will) be differently dependent on the local situation.

Recommendation III

Biometric matches should – wherever possible – only be based on biometric-only matches without knowledge of related personal data, such as the procedures in place for EURODAC. Legal regulations and best practices agreed upon need to limit the number of biometric inquiries to an amount only necessary for the intended purpose.

As a complement to this suggestion, standardized matching algorithm and implementation, standardized calibration, user interfaces and well-trained, certified and supervised operational personnel is strongly preferred. A European Biometric Matching System has been announced but no detailed concept has been presented yet.

Not to be overlooked, the implementation of biometric testing standards, facilities and certification schemes must be considered as necessary prerequisites.

Function: Insecure biometric data could create highly negative circumstances.

Although biometric samples are not considered secret because they are present almost everywhere, their link to a person's identity is a highly relevant security issue. With enrolment and matching devices, it must be assured that a living individual leaves the sample to be enrolled or matched. (This is a problem not new to traces found at crime scenes.) Another environmental problem is unauthorised or accidental access to RFID tokens which could provide the data from the wrong person. A third dilemma is misuse of biometric features for unintended purposes such as interpreting health information about a biometric sample's owner.

With current e-passports, the currently used Basic Access Control (BAC) encryption method is considered to be weak, but the proposed Extended Access Control (EAC) PKI based encryption method is not available because there is no key management in place.

Recommendation IV

Multi-modal biometrics are recommended as the most secure option to prevent spoofing. Future deployments of large-scale biometrics systems should opt for multi-modality and all stakeholders in secure identification scenarios should give the complete security cycle its proper attention: enrolment, storage, acquisition, matching and the entire back-end system.

Enrolment and matching should be performed using 'Live and wellness' detection especially in unattended environments and/or the process should be supervised wherever possible.

Encrypted templates should be applied rather than original samples for storing and matching. It is concluded that matching against tokens yields the highest security level and therefore is preferable.

Regarding specific applications, the new ePassports should contain personal data that is protected by Extended Access Control (EAC) which implies implementing an effective key management.

Overall, security requirements for large-scale deployment need to be defined in detail at an international level.

Function: Few results are available on test data and common European standards are still lacking and need to be formulated.

Although existing systems or pilots are reported to show satisfactory results in technical and performance terms, those results are only valid within the actual system's or pilot's limits. Except for law enforcement under the Prum standards, experience with interoperability has not yet been reported. The future Europe-wide border control scenario will only work when

the matching function at any border will show the same results regardless of the location of the devices and the data origination point as well as the kind of user. This requires Europe-wide standards and certification processes, based on the result of standardized testing parameters and procedures.

Initial results from the BioTesting Europe project demonstrate the significant lack of technical standardisation which worsens interoperability.

In particular:

- Some testing key areas still lack methodologies.
- Many unknowns about performance of biometrics make it seem like an immature technology.
- There is no Europe-wide view on usability which is a less-discussed, but increasingly becoming an important factor for minimizing errors and maximizing overall performance.

Recommendation V

An accreditation and certification structure must be established on a European level as there is currently an urgent need for a common framework.

Such a framework must assure that certified devices and data qualities will yield the same results at every proposed site. Considering the numerous standardisation bodies in biometrics, it is understood that the task could take much time before an agreement is in place.

Lastly, as the BioTesting Europe project is aiming to improve the current situation of test data, there must be a provision of much more data to appropriately cope with the large system dimensions. Therefore, the results of that project could be the right step in the right direction for improving future large scale deployment.

6.4 Security and Privacy Study Recommendations

Based on the findings that have been elaborated previously in Chapter 3 concerning **security and privacy,** the following general conclusions can also be drawn.

Recommendation VI

More detailed guidelines on system and process design are needed to perform targeted threat analysis and quality assessments. This includes the human factor in the interaction with / operating of biometric devices.

In order to assess the risks involved in implementing large scale biometric systems it is needed to define in more detail what these system are in terms of functionality. Once that has been made clear, *targeted assessments* can be carried out on security, privacy, proportionality and overall quality of the system.

Therefore, it recommended to conduct a concise usage scenario and proportionality assessment covering the balance of possible security benefits with necessary decline of privacy that appropriately balances convenience and the financial effort.

In the case of (video) surveillance applications, where biometric technologies can (and in most cases will) be used without the awareness and/or consent of the observed individuals, there is a need for convening a meeting to discuss this topic in greater detail.

Recommendation VII

A European approach is needed to overcome differences between member states in the handling of privacy and data protection issues.

User requirements for large scale biometric deployments are not yet harmonized on a Pan European level. For the large scale cross national systems it is a prerequisite that user requirements are known. Based on those requirements functional designs can be created. This should answer the basic question: what will be the exact function biometrics should fulfill within these systems?

On top of existing work (e.g. by the European Data Protection Supervisor (EDPS) and the Article 29 Working Party) a more proactive approach should be put in place in order to overcome the differences. Consensus should be reached between the member states on embedding the guidelines and directives into national law, based on clear and common agreed description of the purpose of the use of biometrics in specific systems (public and private).

A common European approach will enable a more effective messaging of the European values to other parts of the world when discussing international data exchange and data handling in connection with privacy and data protection issues, thus providing stronger protection of the EU citizens' interests.

Recommendation VIII

Public awareness should be created amongst all the EU citizens about the purpose and use of biometric technologies in large scheme's such as passports and public administrations.

A European wide campaign should inform EU citizens about biometrics enabled systems. It should be clear what the purpose of those systems are, how the citizens have to deal with those systems and what they can/can not expect from it. All stakeholders (citizens, policy makers, NGOs, industry…) should have a minimum level of common understanding on biometrics in order to manage the expectations properly. This should allow a fair and open debate which should enable a balanced discussion on costs/benefits, purpose of the systems etc.

Recommendation IX

European testing and certification capabilities based on European requirements in the area of biometric enabled id-systems are urgently needed in order to improve interoperability, conformance, security and overall trust.

Independent European laboratories should develop capabilities to *test and certify* performance, conformity and security of biometric systems and their components, including non-technical aspects such as the human factor and procedures. BioTesting Europe and the Minutiae Template Interoperability Testing Project (MTIT: www.mtitproject.com) are some first important steps in that direction, but much work still needs to be done, especially in the coordination and endorsement of these activities.

Recommendation X

Biometrics is not yet wide spread as a technology and is still an area for specialists; it is therefore necessary to bring independent expert opinions together on a European level.

In order to overcome the fragmentation of knowledge and to establish a harmonized approach to biometrics related issues on a European level and to assess vendors claims, an *independent authoritative European team of experts* should be established to assist the European Commission and the member states in those processes.

6.5 Conclusions and Suggested Actions for European Policy Makers

Conclusions for large-scale systems that are already deployed or in pilot stage:
Positive experience is detected with these systems within their defined objectives in terms of reliability, results vs. errors, performance and acceptance. So far, only **AFIS** are international interoperable systems deployed on a large scale, showing experience with matching of biometric and non-biometric personal data originating from different sources. Important prerequisites for their successful use are well-defined and standardized data qualities and procedures. Non-matches at inquires remain a fundamental problem since they leave the issue open if those non-matches originate from an error or if there actually is nothing to be matched.

For other systems or pilots, statements about their success only apply within their current limits. Access Control systems usually run in closed environments with no or strictly purpose-oriented reference databases and good experiences with matching-on-card concepts. Biometric passports are currently enrolled at large scale which includes checking the data only in the system environments where the data is created, therefore opinions on accuracy do not apply to future interoperability.

For **VIS**, experiences so far exist for the BioDev pilots performed in a few facilities already deployed and limited number of individuals and users compared with the eventual scenario planned. Accuracy and performance statements also apply only within these pilots; however they have already showed some challenges to be resolved in various areas, like adaptation of consulate facilities and resistance from VIPs.

Conclusions for a future automated border control scenario:
Today this scenario is a concept that will combine components already deployed with clear purposes and other parts in design or pilot stages to eventually be the largest data collection and access system in the world. Data quality and correctness are the key issues, both for biometric and non-biometric personal data. The entire scenario will depend on this, and therefore it must be achieved by the enrolment processes for passports and visa at every particular site. It will be most likely impossible to improve the data quality at a later stage at such large scales.

As a concept now, the scenario has many undefined areas which need to be clarified by stakeholders, especially for political entities as soon as possible:

- **Border control facilities, devices and procedures (normal and fall-back) for different environments ranging from large airports to remote land border points.**

- **Data security concepts and measures through the data's entire lifecycle**. It is required and expected to guarantee data security, which is especially threatened by unreliable technologies, unauthorized access and outsourcing. There is an urgent need for decisions.

Although the highest priority must concentrate on data correctness, secure and transparent correction and deletion processes need to be defined at all levels. Modification will be a difficult task in such a multi-purpose, multi-country and multi-user scenario, but leaving wrong data unchanged is unacceptable.

Interoperability will depend on quality, testing, calibration and certification standards which are not yet implemented at all although expert groups and projects have offered suggestions. This is very urgent because setting up a certification scheme for technology, procedures and users will take a significant amount of time.

As an important part of the scenario, there is no concrete concept for the announced registered traveller program (for individuals from important third countries not obliged to carry visa). It will be necessary to start soon with detailed suggestions, because this concept imposes many additional questions like enrolment facilities and procedures located / performed overseas.

Most important, the lack of experience with such dimensions of data, authorized users, variety of purposes, devices, vendors and complexity must not be under-estimated.

Conclusions of political dimensions:
Proportionality issues cannot be resolved at an expert level. Experts only can explain the features, potential and expectable consequences of technologies. Mechanisms promising to ensure public security need to carefully be balanced with measures for adequate data protection and privacy. Such balance between the provision of maximum reasonable security possible on the one hand, and maximum individual freedom and democracy on the other including criticism and minimum discomfort and cost for the citizens is a political decision to be made under transparent democratic circumstances with responsibility taken.

The implications of the U.S. approach of collecting all available data and treating every foreign citizen as a potential criminal or terrorist unless his/her innocence is proven does not seem to comply with Europe's understanding of a free and democratic society accepting other cultures. Further, this would lead to gigantic costs for the taxpayer.

Not everything that technology may offer needs to be implemented just because it is possible. Therefore, function creep potentials must carefully be monitored as technology will offer more and more options causing an increasing interest. Especially upcoming technologies that promise to assign risk potentials based on individual's behaviour patterns could lead to "compliant behaviour", which would be in contradiction to European values.

Blind faith in technology, especially biometrics which always yields probabilities rather than the absolute truth is to be avoided. It will always require the assistance of on-site human decisions according to legislation and procedures accepted by the citizens. Further, neither existing nor future biometric systems can provide 100% accuracy. There will always be human intervention required (as conducted in law enforcement based on the Prum treaty).

Objective conclusions are that clear data protection measures are necessary and they must be politically defined with regulation frameworks and best practices. This calls for even more intensive cooperation of stakeholders with data protection authorities and transparency to the citizens who will be affected.

It is well understood that data protection only is concerned with protecting citizens for safe data procedures, and doesn't intend to cover illegal functions like pornography, money laundering, planning of terrorist activities, etc. It is, of course, necessary to efficiently prevent illegal border crossing, to fight and prevent crime and terrorism, but a society where everyone will always be watched everywhere by invisible or unknown authorities, and where decisions will be made on information of undefined correctness, is not what the European citizens expect from their governments. **Furthermore, it should be understood that no implementation can guarantee 100% security.**

The issues discussed previously imply an urgent requirement for Europe-wide legal frameworks, standards and accepted best practices, in the areas of:

- Data quality assurance (implying testing, calibration, certification, usability, user training, supervision)
- Ability for persons enrolled to claim incorrect data and have them modified or deleted under well-defined ad supervised conditions.
- Data security measures from protection against theft, loss, misuse, unauthorized access and controlled data flow at any time even when outsourced.

European policy makers should inform their citizens in a transparent way about:

- What and whom are the security targets and how they should be incorporated with large scale biometric technologies
- What are the proposed scenarios and how they will properly address security targets.
- On which options decisions are made when finding a compromise between values to be secured and values to be surrendered by the citizens.
- Which regulations will be set into place to assure that all the processes will work correctly and under supervision.
- What are the practical impacts on the citizens (and travellers) and what will they be in the near and distant future
- What are the expected costs for the taxpayers in both the short and long term

Annex I: Questionnaire Analysis

The Biometrics Deployment Study as mentioned in this report conducted a survey as its primary tool to gather results on biometrics large scale deployment. The objectives intend to report on the key issues surrounding the deployment of the biometric systems.

The survey has been distributed corresponding to more than 60 systems (providers, manufacturers and users) in which the requirement consisted of a capacity of more than 10.000 persons enrolled to the particular system. The questionnaire has been sent by e-mail and followed-up by phone calls and personal visits (concerning physical visits in Italy and Austria, which are the main methodological tool of the study).

The following text provides a synthesis of those questionnaires answered (12 in total) with some statistical analysis representing each of the sections. For confidentiality reasons, the names of the institutions which participated to the questionnaire have been left anonymous.

Table 3: Questionnaire: basic information

Basic information	
1. Name of the system	12 results, 4 of them from manufacturer
2. Is system public or commercial?	12 results, 4 of them from manufacturer
3. Status of deployment (being in use / planned / pilot)	12 results, 4 of them from manufacturer 9 in use, 1 planned, 2 pilots
4. Date (or expected date) of launching the system [dd.mm.yyyy]	
5. If system is deployed for fixed time, please specify the period	
6. Description of application domain (e.g. ePassports, National Identity, Driving licences/ other kind of permits or licences)	2 passports, 2 ID cards, 2 AFIS, 1 VISA/asylum seeker, 5 access control
7. Manufacturer	12 results, 4 of them from manufacturer
8. Provider of the system (if different from Manufacturer)	3 different from manufacturer
9. Geographical scope (International / European/ National / Regional/ Local)	7 results: 3 international, 4 local/national
10. Number of users enrolled into the system	8 results: 80 migration services, 125.000, 35.000, 400, 1200+, 22.000, 22.000 (15 mio planned), 60.000
11. What type(s) of biometric technology is (are) used? (e.g. fingerprints, face image, etc)	12 results: 2 face, 1 iris, 6 finger, 2 face&finger, 1 finger&other
12. Is biometrics used for identification (1:n) or verification (1:1)?	11 results: 4 identification, 5 verification, 2 both
13. Additional source of information about system (web page, newspaper article, etc)	

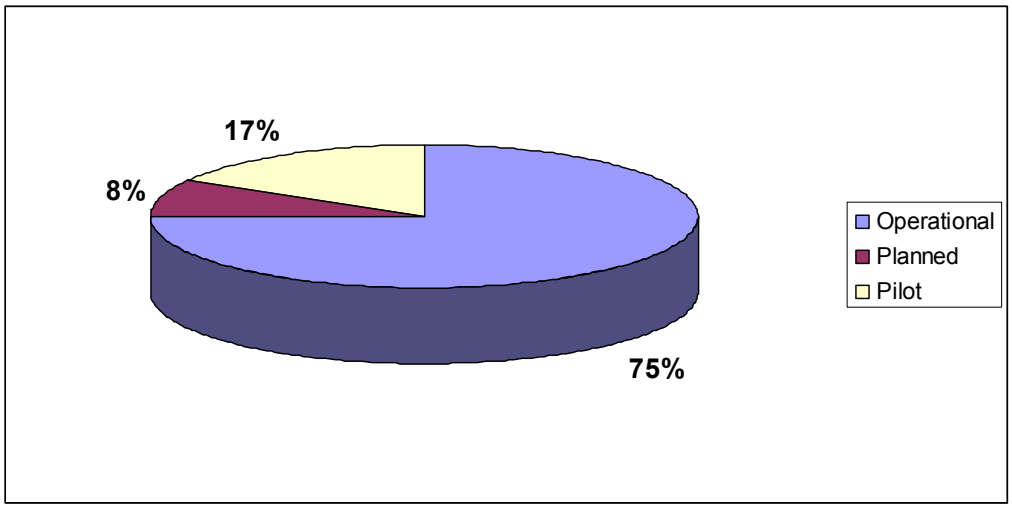


Figure 1: Questionnaire: status of deployment

Main application domains, number of users and type of biometric data reported:

- Law enforcement (AFIS, DNA),
- ID and travelling documents (e-passport, ID-cards,VISA),
- Access Control (includes registered passengers)

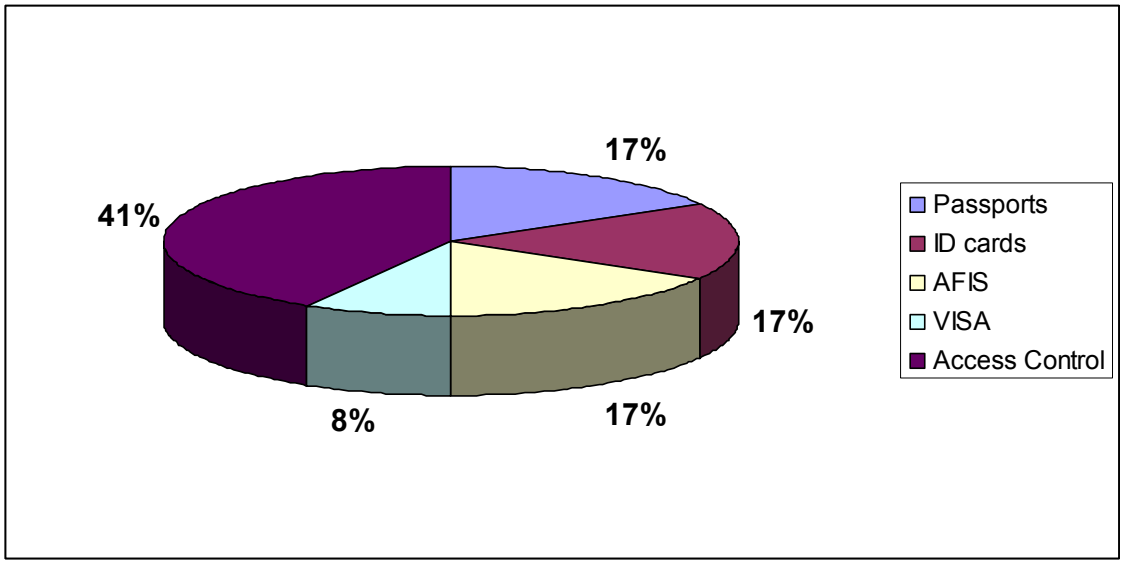


Figure 2: Questionnaire: application domains

Identification vs. verification:

Fingerprints are used in all domains, for identification and verification purposes.

Face (biometric image) is the first choice for ID/travelling, used for verification.

Iris is the choice for registered passengers and used for verification against 'closed-set databases'.

DNA: only used in law enforcement, for verification (proof of evidence) and identification (crime scene marks against DNA from given suspect) purposes. DNA analysis must be performed by special labs and is therefore time-consuming, expensive and also needs effort for enrolment.
Palmprints: are used only in law enforcement for identification.

The **trends** point towards multi-modality in AFIS (every sample could be useful) and Passports (fingerprint added to facial image), access control seems to work well with one type of biometric data so far.

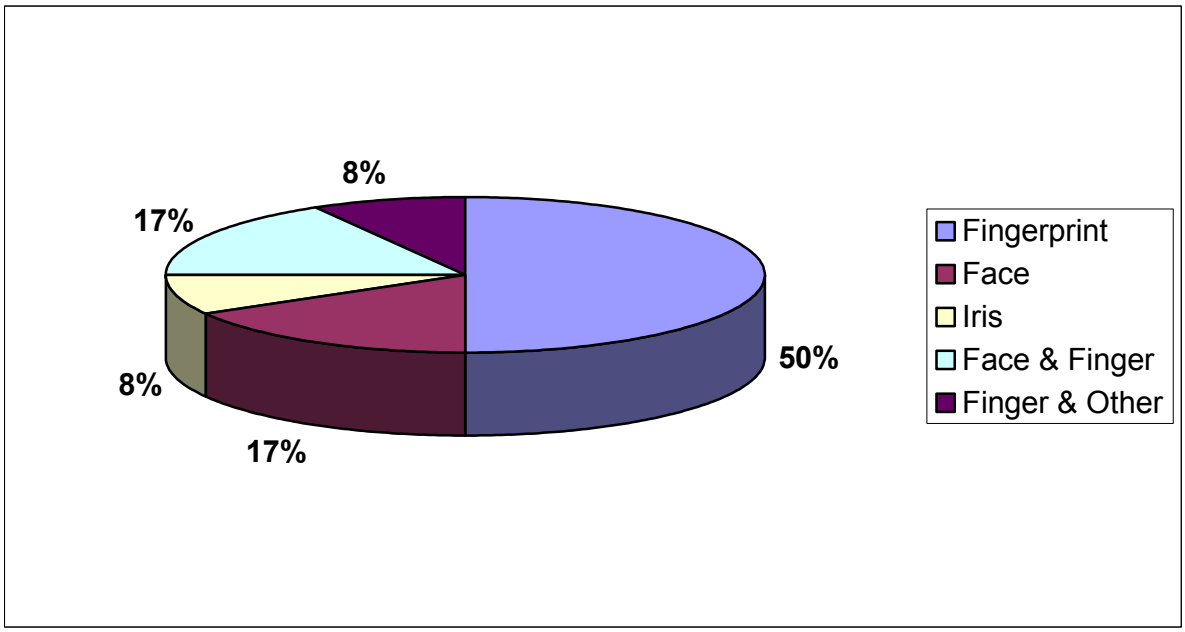


Figure 3: Questionnaire: type of biometric technology

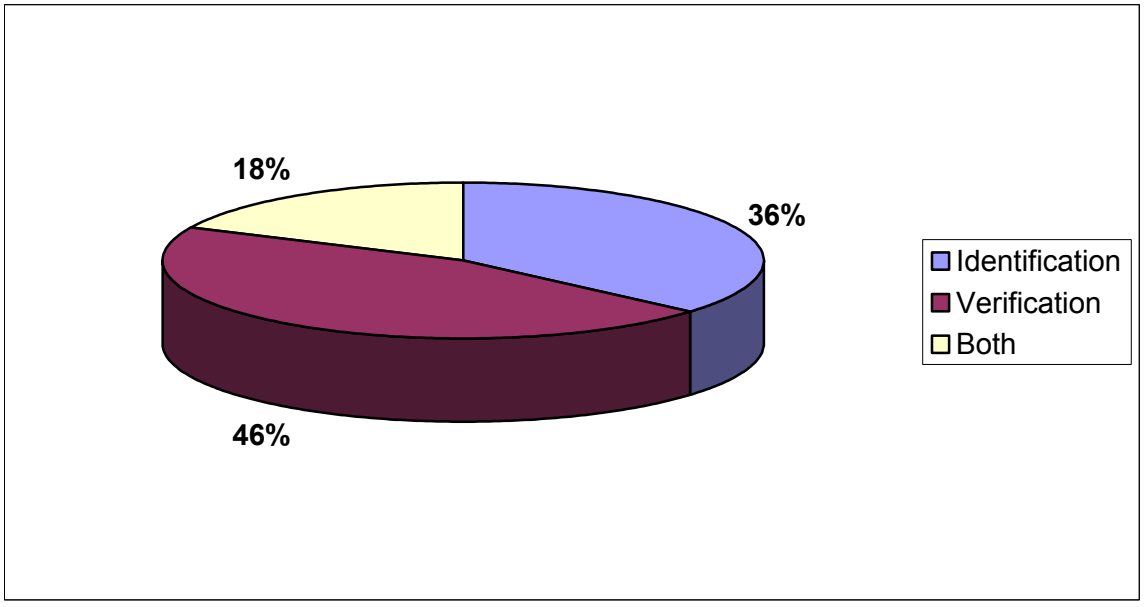


Figure 4: Questionnaire: identification vs. verification

Table 4: Questionnaire: the main drivers

The main drivers – why the system has been developed

rank from 0 (not relevant) to 5 (very relevant)	
14. To increase security	12 results: average: 4,67
15. To increase convenience (e.g. shorter waiting time)	12 results: average: 3,08
16. To save costs	12 results: average: 1,17
17. To fulfil agreements with third parties	12 results: average: 1,42

'To increase security' was considered the most important driver.

'Convenience' is not an issue for suspects in Law enforcement, but important for officers. It is very important for registered passenger access control.

'Save costs': by experience, it is a relatively important driver for AFIS, because the implementation costs are in the many-million-Euro range, traditional manual matching of traces is – besides the importance of quick responses - very expensive. However, no figures have been reported. It can be expected that automated border control will need large investments which would yield reductions in personnel costs over the years.

'Agreement with third parties': This is very important for ID/border control because this concept will not work without interoperability among member states. Up until now, there is an EU directive for issuing biometric passport, but none for border control procedures.

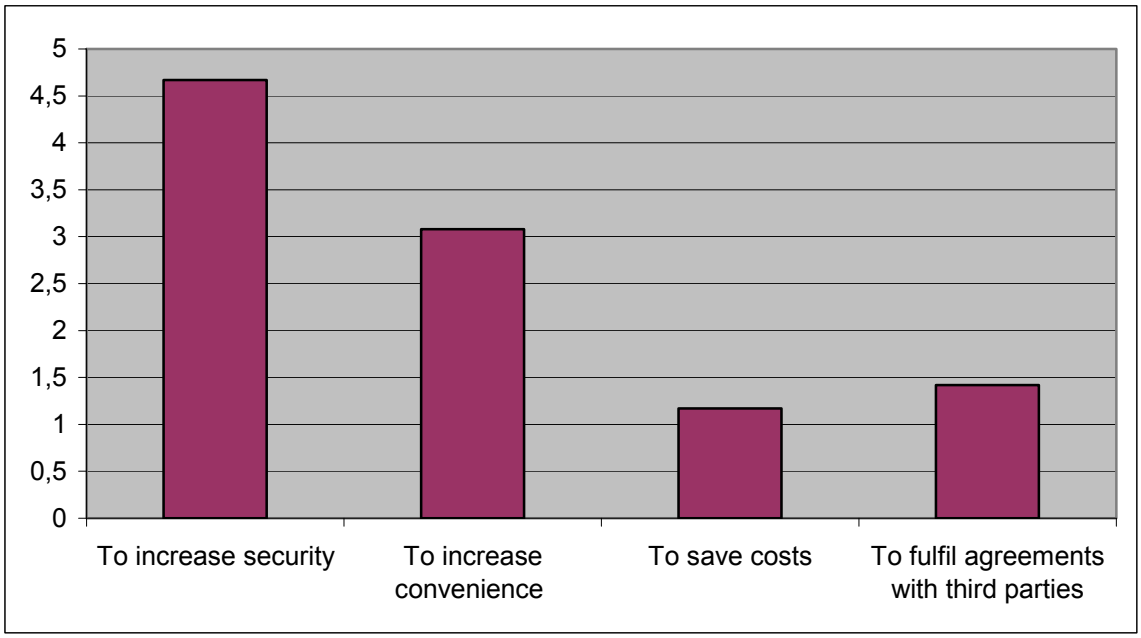


Figure 5: Questionnaire: the main drivers

Table 5: Questionnaire: performance data claimed by manufacturers

Performance data claimed by manufacturer	
18. False Rejection Rate / False Non Match Rate (% of users wrongly rejected by system)	7 results: answers are very divergent, meaningful conclusions and comparisons not possible
19. False Acceptance Rate / False Match Rate (% of users wrongly accepted by system)	3 results: answers are very divergent, meaningful conclusions and comparisons not possible
20. Failure To Enrol Rate / Failure To Acquire Rate (% of users who cannot enrol into system / failure to capture and extract biometric data)	7 results: answers are very divergent, meaningful conclusions and comparisons not possible
21. Transaction time (time required for verification of single user): minimum, average and maximum	8 results: 0 – 15 sec

Comparisons based on the questionnaire are not statistically possible, because different systems for different purposes in different environments have been reported. Further, this would require to reveal the testing environment, the number of tests being performed and still would differ by the system's purpose and cooperation of the person in question. This information has not been given in the survey.

Error rates are not absolute measures like weights but rather statistical results of many measurements and they are only meaningful with given test parameters like thresholds (set to 0 means no difference allowed between sample and reference and would yield 100% acceptances if there were any positive matches, but maximum rejections). Therefore, they are individually set to allow more and more differences until reasonable results for the intended purpose are yielded. Therefore, practical results are growing by experience.

Table 6: Questionnaire: performance data by practical experience

Performance data based on practical observations and comments	
22. Type of biometric performance test that was conducted prior to system installation (e.g. 19795-1 technology test, scenario test, operational test)	4 results: "operational tests"
23. Crew size (test population)	3 results
24. False Rejection Rate / False Non Match Rate	No results
25. False Acceptance Rate / False Match Rate	No results
26. Failure To Enrol Rate / Failure To Acquire Rate	1 result: 0,0005 %
27. Time of identification/verification: minimum, average and maximum	1 useful result from deployer
28. Average time of enrolment	2 results from deployer 75s, 90s; 3 results from manufacturer
29. Is performance of the system close to expected?	3 results from deployers "quite/moderately satisfied", 3 from manufacturer

These are more interesting, but there was very little outcome of the questionnaire.

Testing methods were not reported by anyone, except 4 generic reports of 'operational tests'. We cannot conclude that there was no standardised testing in place at all. Of course this may lead to usable systems as the answers on satisfaction indicate, but it may cause problems when it comes to large-scale interoperability and integration; and it makes technical figures difficult or impossible to compare.

For only one passport system a failure-to-enrol-rate has been reported to be very low and it included facial image and fingerprint: However, we do not know what the figure means – this could be the average of the two types or the rate to enrol to at least one of them.

Similar with the actual time for a verification /identification process there is only one answer from a border control system reporting an average of 5.5s. This could be competitive with visual control by officers, but is not much faster. If this would be achievable even with future searches in large databases is left open.

Time to enrol: reported by 2 different systems in the 1 – 1.5 minute range. It is unclear what has been measured and reported here: an enrolment of ten-print seems to be quite fast; however, for AFIS this is not so important as it its for passports.

The three reported answers on satisfaction remark as "quite satisfied", which could mean that there still is left something to enhance.

Error rates: not enough data and no environment information has been given to allow for meaningful comparisons. The rates themselves are not solely a matter of device quality but the result of calibration, i.e. setting the threshold properly for the purpose ('how much may the template differ from the reference').

There are fundamental differences between FAR/FRR (decision of the system) and FMR/FNMR (depending on the application and quality of references).

There has been no reported execution of standardised tests. If they really are not performed this could yield challenges for integration and interoperability.
Time: Transaction times reported as satisfying. However, as already pointed out, this belongs to the purpose intended. When open-set database inquiries are to be performed this will take much longer, as already experienced in AFIS systems.

Table 7: Questionnaire: standards and interoperability

Standards and interoperability	
30. Claimed Standards (ISO, ANSI, ICAO, others)	4 results: 2 ISO (7816 for smartcards), 2 ANSI NIST - ITL 2000 for AFIS
31. ISO SC37 standards that systems shows compliance	3 results: "no ISO SC37 standards"
32. Scheme that was used in the certification of the system	2 results: "KEMA, CE"; « Compliance IAFIS-IQS, Appendix F & Compliance ISO 7816 1,2,3,4, ed EMV2000"
33. What type of biometric data is stored (image, template, other)?	6 results: 5 template 1 image and template
34. Is all technical information about the system overt?	5 results: "no"
35. Is system *able* to exchange information with other systems?	6 results: 5 Yes, 1 no
36. Is system connected with other systems? If so, with what systems?	6 results (not comparable)
37. Is information with other systems exchanged? If so, with what system? What data are transferred, when and what is the purpose?	6 results (not comparable)

ISO 7816 is the standard concerning smartcards.

ANSI NIST ITL 2000 is a data format for biometric information, from fingerprints to tattoos.

Remarkably, ISO SC 37 has not been referenced, maybe because they are relatively new.

The IAFIS IQS specifies the data acquisition standards for fingerprints, reported as a certification scheme.

Stored usually are templates, with face images the discussion is still there whether they are templates or data.

Yet it is important to point out that detailed technical information has not been unveiled.

Table 8: Questionnaire: token, if applicable

Token, if applicable	
38. Does user carry biometric token (any kind of device storing biometric data)?	5 results: 4 yes, 1 no
39. Kind of token (e.g. contact / contactless smart card, USB key, or other – please specify)	4 results (contact Smartcard)
40. Does the token allow comparison-on-card? Has it been considered as an option?	4 results, 1 yes 3 no

The information available mainly comes from manufacturers; tokens used were reported as contact smartcards.

Biometric Passports use RFID chips which are read by the border control device to compare passport data and image; it is assumable that fingerprints will be matched by the device rather than by some central software. The one reported local access control system matches fingerprints on card, whereas the iris—based fast lane border control does not but rather uses the template stored on card.

Table 9: Questionnaire: biometric database

Biometric database, if applicable	
41. Are biometric data kept in a database?	4 results: 2 yes, 2 no
42. Is the database centralized?	2 yes (answers from manufacturer.)
43. Encryption of *stored* biometric data (yes/no)	2 yes (answers from manufacturer.)
44. If yes, encryption method (DES, AES, other), size of encryption key	1 answer DES (answers from manufacturer.)
45. Encryption of *transmitted* biometric data (yes/no)	4 yes (2 answers from manufacturer.)
46. If yes, encryption method (DES, AES, other), size of encryption key	4 answers 2: DES 2: not known
47. Other means of template protection	No answers
48. Authentication of transmission (yes/no)	1 answer yes
49. If yes, authentication method	1 answer
50. Who has ownership over the database?	2 answers

This set of questions asked for database and encryption information.

Only ‘yes’ and ‘no’ type answers were given (‘Yes’ came only from manufacturers, whereas ‘no’ came from access control systems.

If encryption was specified at all, then DES was reported mostly without details (DES or 3DES which would imply the key lengths), one reported single-DES which is not state of the art because it has already been cracked.

Table 10: Questionnaire: biometric sensor

Biometric sensor	
51. Type of biometric sensor (e.g. b/w camera CCD, sweep thermal fingerprint sensor, etc…)	6 results
52. Manufacturer	6 results
53. Scheme that was used in the certification of the sensor (no medical impact on the subject?)	No results
54. Any other information about device	3 results
Biometric sensor 2, if applicable (in multimodal systems)	
55. Type of second biometric sensor	1 result
56. Manufacturer	No results
57. Scheme that was used in the certification of the sensor (no medical impact on the subject?)	No results
58. Any other information about device	No results

Of course this depends on the type of biometrics used, for fingerprints in AFIS live scanners are the first choice, backed up by Ink-on-paper scanned by flat-bed for enrolment (crime scene marks are taken by conventional means).

Table 11: Questionnaire: costs

Costs (all fields are optional)	
59. Cost of setting up the system	1 result
60. Cost of enrolment of new user	No results
61. Maintenance cost (per month)	No results
62. Cost of token (if applicable)	No results
63. Cost of sensor	No results
64. Cost of second sensor (if applicable)	No results
65. Cost of training a new user	No results
66. Does user have to pay for enrolment? If yes, how much?	1 result

The only one answer shows that we have to assume investments in the 100 Million Euro range for complete law-enforcement systems.

Table 12: Questionnaire: legal, organizational and data protection issues

Legal, organizational and data protection issues	
67. Is the system optional or mandatory?	6 results: 3 mandatory/ 3 optional (3 answers from manufacturer.)
68. Have the competent DPA authorities been consulted? Was there an approval mandatory?	3 results: " yes" No answers regarding approval mandatory
69. What specific safeguards did you implemented to ensure system security?	No useful results
70. Please specify if any, specific measures to ensure data protection and privacy?	2 results: smartcard, encryption of data on smartcard
71. Who owns the biometric information?	6 results (depending on application area) (3 answers from manufacturer.)
72. Do users have access to their data?	6 results (depending on application area) (3 answers from manufacturer.)
73. Are data shared with third parties?	6 results (depending on application area) (3 answers from manufacturer.)
74. Have any fallback procedures been implemented?	6 results: 2 yes 4 no (3 answers from manufacturer.)
75. Will training be offered to users (Y/N)	6 results: 5 yes 1 no (3 answers from manufacturer.)
76. If yes, duration of the training	4 useful results (2 answers from manufacturer.)

Ownership of biometric data depends on the application, e.g. a passport holder does not own his passport and therefore not the data on it. The challenge is to smoothly handle potential errors, since the normal user cannot see what's on his chip.

Due to the nature of Law enforcement the person in question neither owns nor shall have access to his data. But: it has not been stated what happens if there is something wrong with them.

For access control, usually the organisation running the system owns the data.

Data sharing also depends on the purpose, passport information and AFIS data are definitely shared in order to make sense. Data sharing and inquiries from third parties are a challenge for data protection whenever private companies are using them.

Table 13: Questionnaire: challenges and future plans

Challenges and future plans	
77. Are you satisfied with the type of biometrics applied in system? If not, what other biometrics would you propose?	6 results (3 answers from manufacturer.) All satisfied
78. Satisfaction of the user (if any information available)	4 results (3 answers from manufacturer.): high/yes
79. What are the main technical challenges? (E.g. scanning efficiency improvement, false rejection/acceptance rate decrease, cost decrease, more convenience for the user, better security protection).	6 results (2 answers from manufacturer.)
80. Do you plan further development / modification / replacement of the system? What and why would you like to change?	7 results (3 answers from manufacturer.)

Satisfaction with the type of biometrics / satisfaction of the users:

As expected only those who are satisfied have reported. This does not imply that all the others are not. A choice of the type of biometrics is not possible everywhere, for passports facial images and fingerprint are given, law enforcement takes everything what is reasonable.

Interesting was the fast lane access application where 90% of the enrolled users have renewed their membership although they have to pay for it.

Reported (technical) challenges can only discussed in generic, because usually only one item per system was reported:

'Decrease costs' (implies that they are high today).

'More convenience for the users' (came from a system already felt as convenient; but in general this is very important for low overall error rates and performance).

'Storage of data': has been already discussed with databases.

Further plans for the future:
- Improve performance: has been reported by manufacturers, so it can be concluded there is still a potential beginning at the devices over smart matching techniques up to good user interfaces and training.
- include further types of biometrics:
  Passports will include at least 2 flat fingerprints
  AFIS will extend to facial recognition, but this is currently in test state although there is pressure from politicians to develop solutions able 'to find the terrorist in a football stadium automatically'.

Others like hand geometry have not been reported as to be deployed in the later future.

Annex II Final Conference Agenda

Note: The speakers' presentations can be located and downloaded at the following link:

http://www.eubiometricsforum.com/index.php?option=com_content&task=view&id=687&Itemid=2

3rd EBF Research Seminar

"The impact of current biometric deployments on the European research agenda"

co-hosted with CYBION & EC/DG JRC

Date: 2/3 October 2007

Place: Crowne Plaza Hotel, Rue de La Loi, Brussels

Tuesday 2nd October, 2007	**The impact of current biometric deployments on the European research agenda**
08.30 – 09.00	Registration, Coffee & Croissant
09.00 – 09.15	Welcome **Mr Max Snijder, (CEO - European Biometrics Forum)**
09.15 – 09.30	**Keynote address** **Mr Jacques Bus, (EC- DG INFSO)**
09.30 – 10.45	***POLICY*** 'Enabling the development of European large scale id-management systems' **Chair: Mr Peter Hanel (EMEA Identity Management & Security Solutions, Motorola)**
	Mr Troy Potter, (US VISIT Program, Department of Homeland Security) *'Status and findings of the US VISIT Program'*

	Mr Marek Rejman-Greene (Senior Biometrics Advisor – Home Office Scientific Development Branch UK) *"UK policy on biometrics research – the emergence of multi modal biometrics"*
	Mr Nigel Jones (Cyber Security Knowledge Transfer Network – Qinetiq UK) *"Challenges for policy makers - a UK perspective"*
10.45 – 11.00	**Refreshment Break**

11.00 –12.15	EBF European Biometric Research Award 2007 *Finalists' Presentations* Introduced by **Prof Richard Reilly (University College Dublin)** Chaired by **Mr Jacques Bus (EC DG INFSO)**
	The 3 finalists of the EBF European Biometric Research Award 2007 are;
	Mr Hervé Bredin, GET-ENST, Paris, France 'Making Talking-Face Authentication Robust to Deliberate Imposture'
	Mr Hugo Gamboa, Institut Superior Tecnico, Lisbon, Portugal 'Web Biometrics: User Verification via Web Interaction'
	Mr Krzysztof Kryszczuk, (Swiss Federal Institute of Technology Lausanne (EPFL), Switzerland) 'Improving biometrics verification with class-independent quality information'
	The Jury Of the EBF European Biometric Research Award 2007 includes; **Mr Jacques Bus <Chair>** (EC- DG INFSO); **Prof Dr Christoph Busch**, (Fraunhofer-IGD, Germany); **Prof Bernadette Dorizzi,** (Technical Co-ordinator of the NoE BioSecure, France); **Prof Anil K. Jain,** (Dept of Computer Science & Engineering, Michigan State University, USA); **Prof Josef Kittler,** (School of Electronics and Physical Sciences, University of Surrey; UK); **Dr Gerasimos Potamianos,** (Thomas J. Watson Research Centre, IBM, USA); **Prof Richard Reilly,** (University College Dublin, Ireland); **Dr Günter Schumacher**, (EC JRC, IPSC); **Prof Massimo Tistarelli,** (University of Sassari, Italy); **Prof Raymond Veldhuis,** (Twente University, The Netherlands) and **Prof James L. Wayman,** (National Biometric Test Center, San Jose State University, USA**).**
	The Jury of the EBF European Biometric Industry Award 2007 includes**;** **Mr Michiel van der Veen <Chair>,** (Phillips Research); **Ms Elaine Dezenski, (**Crossmatch); **Mr Peter Went, (**WCC Group); **Mr Peter Hanel,** (Motorola); **Mr Nicolas Delvaux,** (Sagem) and **Mr Ger Daly, (**Accenture).

12.15 – 13.45	***RESEARCH*** *'Biometrics R&D : Drivers for World Class R&D in Europe'* **Chair: Mr *Ioannis Maghiros (Project Leader, EC DG JRC – Institute for Prospective Technological Studies)***
	Mr Paolo Salieri (EC / DG Enterprise & Industry) *"Security research under the 7th Framework Progra*m"
	Mr Ben Schouten, (BioSecure) *"Updating the European Biometrics Research Agenda"*
	Mr Dirk Van-Rooy (EC / DG INFOSO)
	"The role of biometrics in a digitally networked society"
	Mr Klaus Keus (Head of Unit "New Technologies" – BSI, Germany) *"Performance Data of Biometric Systems - Theory and Practice"*
13.45 – 14.45	**Lunch offered to you by Crossmatch**
14.45 – 16.15	***CITIZENS & END USERS*** 'Impact of biometric enabled ID-management systems on civil rights and managing the risks' **Chair: Mr Emilio Mordini (Director CSSC, Italy)**
	Mr Peter Hustinx, (European Data Protection Supervisor) *"Update on some key developments in the field of Data Protection"*
	Baroness Sarah Ludford (EU MEP, UK) "The implications of using biometrics in the VIS".
	Mr. Fred Carter, (Information and Privacy Commission of Ontario, Canada) *"White Paper - Privacy Enhancing Technologies in Biometrics"*
	Mr Max Snijder, (Study Leader) **"***JRC-IPTS Report of the study - Security and Privacy in Large Scale Biometrics Systems"*
	Mr Alessandro Alessandroni (Coordinator of Biometric Competence Centre BCC – Italian National Centre for Information technology in Public Administration CNIPA) *"The situation in Italy : Privacy Concerns"*
16.15 – 16.30	Refreshment Break
16.30 – 17.15	**Panel Discussion - Chair: Emilio Mordini (Director CSSC, Italy)** **Mr Peter Hustinx, (European Data Protection Supervisor)** **Mr Richard Rinkens (EC DG JLS Large IT Systems)** **Baroness Sarah Ludford (EU MEP United Kingdom)** **Mr. Fred Carter (Information and Privacy Commission of Ontario, Canada)** *"As large scale biometric systems are being developed are the necessary safeguards being implemented to protect the data contained in them?"*
17.15 – 17.40	Presentation of the EBF European Biometric Research Award 2007 **Mr Jacques Bus, EC DG INFSO**
17.40 – 18.00	*Closing Remarks* **Mr Max Snijder, (CEO EBF)**

18.00 – 19.00	**Complimentary Drinks Reception / Networking**
19.00	**End of Day 1**

Wednesday, 3rd October, 2007	**The impact of current biometric deployments on the European research agenda**
08.45 – 09.15	Coffee & Croissant
09.15 – 09.25	*Welcome* **Max Snijder, (CEO EBF)**
09.25 – 09.45	Keynote Address **Mr Frank Paul, (EC DG JLS)** *"The European Border Revolution"*

09.45 – 11.00	**Projects & Deployments – Session I** *'Update on the current status of deployments of Large Scale Biometric Systems'* **Chair: *Dr Günter Schumacher (EC JRC, Institute for Protection and Security of the Citizen)***
	Mr James Goldstein (Study Manager, Cybion Srl Italy) *"Challenges and Threats in Large Scale Biometrics Deployment in Europe – Findings and recommendations from results of IPTS Biometrics Deployment Study"*
	Prof Dr Reinhard Posch, (IAIPC, Austria) *"Biometrics in National eID Schemes"*
	Mr Richard Rinkens, (Biometric Matching System Manager, EC DG JFS) *"The New EU Visa Information System and Biometric Matching System"*
11.00 – 11.15	Refreshment Break
11.15 – 12.15	**Projects & Deployments – Session II** *'Update on the current status of deployments of Large Scale Biometric Systems'* **Chair: *Dr Günter Schumacher (EC JRC, Institute for Protection and Security of the Citizen)***
	BioDev II – TBC *"Biometric data capturing at consulates and embassies : lessons learnt from the field"*
	Mr Roman Vanek, (Head of Identity Documents Section - Federal Office of Police, Switzerland) *"The Swiss Passport Strategy - has reality met the expectations?"*
	Mr Eric Burgland / Frontex *BioPass: Study on Automated Biometric Border Crossing Systems for Registered Passengers at European Airports*

12.15 – 13.15	**Standards, Testing & Certification** 'What is Europe doing to meet the demands for the provision of independent assurance for biometric technologies?' **Chair: Mr Gavan Duffy, Genkey**
	Prof Dr Christoph Busch (Fraunhofer IGD, Germany) *"Testing and Certification in Europe – a report on the intermediate findings of the BioTesting Europe Project"*
	Dr Günter Schumacher (EC JRC, Institute for Protection and Security of the Citizen) *"Electronic Passports as a medium for trusted and interoperable Biometric data"*
	Mr Nicolas Delvaux (Sagem Sécurité, Head of French Delegation for SC37) *"International Standardisation & EBF's SIG Perspective"*
13.15 – 14.15	**Lunch offered to you by Phillips Research**
14.15 – 15.45	**INDUSTRY** 'What industry offers to support the development of a strong and competitive market in the European Union' **Chair: Will McMeechan, (COO, EBF)**
	Mr Peter Hanel (EMEA Identity Management & Security Solutions, Motorola) *"Why are Biometric Systems Being Developed?"*
	Mr Michiel van der Veen (CEO PrivID Biometrics, Phillips Research, Netherlands) *"Private Use of Biometrics"*
	Ms Elaine Dezenski (Senior Vice President, Global Government Relations, Crossmatch, Germany) *"Leveraging Industry Innovation, R&D and Standards, and to Meet Public Policy Goals"*
	Mr Ger Daly (Accenture) *"Considerations of a European Registered Traveler Scheme"*
	Mr Peter Went (CEO WCC, Netherlands) *"Security Through Predictability"*
15.45 – 16.30	**Panel Session –** *"The Biometric Landscape in Europe is characterised by diverse levels of intensity to which single member states are involved in the implementation of biometric systems. While some countries host key players of the biometric industry and have conducted various biometrics test, other countries are procuring large scale passport and visa projects without significant experience in the field.* *However, mainland Europe has only ONE land border and it is indisputable that the same level of security and interoperability must be achieved at all border crossing points.* *The panel discussion will discuss the mechanism through which the*

	goal of one security level can be achieved - be it through cross-country recognition of tested and certified products or be it through a registration of certified products under a European certification body. Furthermore the panel will discuss whether priority should be given to Biometric Performance Testing of the recognition components or to Security Testing of passport reading devices. Last but not least the impact of usability on performance and security will be considered." **Chair: Prof. Dr. Reinhard Posch, (IAIPC, Austria)**
	Panel Members: **Mr Max Snijder (CEO EBF)** **Mr Klaus Keus (Head of Unit "New Technologies" – BSI, Germany)** **Prof Dr Christoph Busch (Fraunhofer IGD, Germany)** **Mr Alessandro Alessandroni (BCC – CNIPA, Italy)** **Mr James Goldstein (Cybion Srl, Italy)**
16.30	**End of Conference**

Annex III Expert Meeting Agenda

Biometrics Deployment Study Expert Meeting

Brussels, 7 March 2007

Mercure Brussels Airport Hotel

10:00 **The Biometrics Deployment Study**
Presentation and objectives of project & objectives of Expert Meeting

Pawel Rotter, European Commission, Directorate-General Joint Research Centre, Institute for Prospective Technological Studies – IPTS

10:15 **Meeting Overview and Introduction of Participants**

James Goldstein, Biometrics Deployment Study coordinator – Cybion Srl

10:30 **Current challenges of Biometric large-scale deployment in the public sector**
Initial findings taken from Background Report and Questionnaire results from Biometrics Deployment Study

Manfred Holzbach, Managing Director – Secure Information Technology Centre - Austria (A-SIT)

Daniel Konrad, IT security expert – A-SIT

Mr. Goldstein – Cybion

Expert panel discussion moderated by A-SIT/Cybion to follow presentation.

11:15 **Experts presentations /discussion**
Experts below will present or discuss the latest situation and their respective views on various topics dedicated to challenges in biometrics deployment, including their analysis of the initial questionnaire results and Background Report.

A moderated discussion will immediately follow each of the experts' presentation and at the end of the session; experts will also have the opportunities to discuss other relevant issues. Estimated time for each expert is 10-15 minutes. The Expert session will be divided into 2 timeslots – one before the lunch break and one immediately after.
Moderators: *Mr. Holzbach & Mr. Konrad*, A-SIT

Current expert presentation/discussion line-up:

"Challenges in large-scale biometrics systems: Security and Privacy"
Discussion covering findings/conclusions from recent IPTS-supported study

Max Snijder, CEO Biometric Expertise Group & CEO Biometric Expertise Group

---

"The main drivers to implement a biometric system"

Peter Hanel, Director European Institutions, Biometric Identity Management and Security Solutions – Motorola

---

"Large-scale biometrics solutions in Italy with a focus on Multi-service ID Card applications for PA employees"

Alessandro Alessandroni, Coordinator of Biometric Competence Centre (BCC) – Italian National Centre for Information Technology in Public Administration (CNIPA)

12:30 Lunch Break

13:30 Experts Presentation / Discussion: Session 2

"Challenges in biometric systems: Data protection"

Dr. Waltraut Kotschy, Executive member – Austrian Data Protection Commission

---

"Performance data of biometric systems – Claimed vs. Achieved" (topic to be confirmed)

Klaus Keus, Head of section "New Technologies" – German Federal Office for Information Security (BSI)

"Standards and Interoperability in Biometrics"

Prof. Dr. Christoph Busch – Fraunhofer Institute for Computer Graphics (IGD)

"Cryptology: Challenge in linking with Biometrics"

Prof. Bart Preneel – K.U.Leuven, Belgium

14:15 **Panel Discussion amongst participating Experts on Conclusions from questionnaire and background report, findings and proposed solutions**
Moderated by A-SIT

14:45 **Current EU activity biometrics status (Other projects such as *BioTesting Europe*, other Expert Groups)**
Moderated by Cybion

15:15 **Next Steps in Biometrics Deployment Study**
Presentation on the remaining phases of the project, including the Draft Report, proposed Conference date and agenda & future involvement of Experts in the project

Mr. Goldstein – Cybion

15:45 Final Discussion/Conclusions: Open Topics for Discussion

16:00 End of meeting

Annex IV Questionnaire

Biometrics Deployment Study Questionnaire

For full information on the Biometrics Deployment Study project supported by IPTS and access to completing the questionnaire online, please visit the website at: http://www.cybion.it/biometrics/questionnaire/

If you prefer to fill out the questionnaire in this MS Word format, once completed, please send the questionnaire by e-mail to goldstein@cybion.it or by FAX at +39 06 6880 6997.

For any assistance, please contact James Goldstein at +39-06-6865975 or at the above e-mail address.

Thanks for your participation.

Date of filling the form [dd.mm.yy]: .....

I Company / public institution data

Data of Institution	
Name of institution/company	
Country	
Website	
Data of contact person	
Name	
Function	
E-mail (mandatory)	
Phone	

II Biometric system data

Basic information	
81. Name of the system	
82. Is system public or commercial?	
83. Status of deployment (being in use / planned / pilot)	
84. Date (or expected date) of launching the system [dd.mm.yyyy]	
85. If system is deployed for fixed time, please specify the period	
86. Description of application domain (e.g. ePassports, National Identity, Driving licences/ other kind of permits or licences)	

87. Manufacturer	
88. Provider of the system (if different from Manufacturer)	
89. Geographical scope (International / European/ National / Regional/ Local)	
90. Number of users enrolled into the system	
91. What type(s) of biometric technology is (are) used? (e.g. fingerprints, face, iris, retina-scan, voice scan, dynamic signature verification, keystroke dynamics, hand geometry, multi-modal biometrics, other, etc)	
92. Is biometrics used for identification (1:n) or verification (1:1)?	
93. Additional source of information about system (web page, newspaper article, etc)	
The main drivers – why the system has been developed **Rank from 0 (not relevant) to 5 (very relevant)**	
94. To increase security	
95. To increase convenience (e.g. shorter waiting time)	
96. To save costs	
97. To fulfil agreements with third parties	
Performance data claimed by manufacturer	
98. False Rejection Rate / False Non Match Rate (% of users wrongly rejected by system)	
99. False Acceptance Rate / False Match Rate (% of users wrongly accepted by system)	
100. Failure To Enrol Rate / Failure To Acquire Rate (% of users who cannot enrol into system / failure to capture and extract biometric data)	
101. Transaction time (time required for verification of single user): minimum, average and maximum	
Performance data based on practical observations and comments	
102. Type of biometric performance test that was conducted prior to system installation (e.g. 19795-1 technology test, scenario test, operational test)	
103. Crew size (test population)	
104. False Rejection Rate / False Non Match Rate	
105. False Acceptance Rate / False Match Rate	
106. Failure To Enrol Rate / Failure To Acquire Rate	

107. Time of identification/verification: minimum, average and maximum	
108. Average time of enrolment	
109. Is performance of the system close to expected?	
Standards and interoperability	
110. Claimed Standards (ISO, ANSI, ICAO, others)	
111. ISO SC37 standards that systems shows compliance	
112. Scheme that was used in the certification of the system	
113. What type of biometric data is stored (image, template, other)?	
114. Is all technical information about the system overt?	
115. Is system *able* to exchange information with other systems?	
116. Is system connected with other systems? If so, with what systems?	
117. Is information with other systems exchanged? If so, with what system? What data are transferred, when and what is the purpose?	
Token, if applicable	
118. Does user carry biometric token (any kind of device storing biometric data)?	
119. Kind of token (e.g. contact / contactless smart card, USB key, or other – **please specify**)	
120. Does the token allow comparison-on-card? Has it been considered as an option?	
Biometric database, if applicable	
121. Are biometric data kept in a database?	
122. Is the database centralised?	
123. Encryption of *stored* biometric data (yes/no)	
124. If yes, encryption method (DES, AES, other), size of encryption key	
125. Encryption of *transmitted* biometric data (yes/no)	
126. If yes, encryption method (DES, AES, other), size of encryption key	
127. Other means of template protection	
128. Authentication of transmission? (Yes/No)	
129. If yes, authentication method	
Who has ownership over the database?	

Biometric sensor	
130. Type of biometric sensor (e.g. b/w camera CCD, sweep thermal fingerprint sensor, etc…)	
131. Manufacturer	
132. Scheme that was used in the certification of the sensor (no medical impact on the subject?)	
133. Any other information about device	
Biometric sensor 2, if applicable (in multimodal systems)	
134. Type of second biometric sensor	
135. Manufacturer	
136. Scheme that was used in the certification of the sensor (no medical impact on the subject?)	
137. Any other information about device	
Costs (all fields are optional)	
138. Cost of setting up the system	
139. Cost of enrolment of new user	
140. Maintenance cost (per month)	
141. Cost of token (if applicable)	
142. Cost of sensor	
143. Cost of second sensor (if applicable)	
144. Cost of training a new user	
145. Does user have to pay for enrolment? If yes, how much?	
Legal, organisational and data protection issues	
146. Is the system optional or mandatory?	
147. Have the competent DPA authorities been consulted? Was there an approval mandatory?	
148. What specific safeguards did you implement to ensure system security?	
149. Please specify if any, specific measures to ensure data protection and privacy?	
150. Who owns the biometric information?	
151. Do users have access to their data?	
152. Are data shared with third parties?	

153. Have any fallback procedures been implemented?	
154. Will training be offered to users (Y/N)	
155. If yes, duration of the training	
Challenges and future plans	
156. Are you satisfied with the type of biometrics applied in system? If not, what other biometrics would you propose?	
157. Satisfaction of the user (if any information available)	
158. What are the main technical challenges? (e.g. scanning efficiency improvement, false rejection/acceptance rate decrease, cost decrease, more convenience for the user, better security protection).	
159. Do you plan further development / modification / replacement of the system? What and why would you like to change?	

European Commission
EUR 23564 EN – Joint Research Centre – Institute for Prospective Technological Studies
Title: Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats
Authors: James Goldstein, Rina Angeletti, Manfred Holzbach, Daniel Konrad and Max Snijder
Editor: Paweł Rotter
Luxembourg: Office for Official Publications of the European Communities
2008
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-10657-6
DOI 10.2791/5941

Abstract

With large-scale biometrics deployment in the EU still in its infancy and with stakeholders racing to position themselves in view of the lucrative market that is forecasted, a study to identify challenges and threats that need to be dealt with has been launched. This is the result: a report on Biometrics large-scale Deployment in Europe. The report tackles three main issues namely, the status, security / privacy and testing / certification processes. A survey was launched so as to help reveal the actual status of Biometrics large-scale Deployment initiatives in EU. The main outcome of the survey was that an open dissemination of implementation results policy is needed mainly on deployment plans, strategies, barriers and best practices. The security/ privacy challenges study identified a number of issues, the most important of which were related to proportionality and compliance to the existing regulatory framework while at the same time it revealed an important number of related actions aiming at ensuring both data security and privacy. The aim of the Bio Testing Europe study was double: to identify and collect comparable and certified results under different technologies, vendors and environments situations and to feed in this information to animate discussion among the members of a European network which would enhance the European testing and certification capacity. The study presents an integrated picture of the identified issues as well as a number of recommendations. With some of the systems that are being implemented involving millions of individuals as target users it is important for policy makers to adopt some of the options presented so as to address the identified through the study challenges.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

LF-NA-23564-EN-C

ISBN 978-92-79-10657-6