Grant Agreement BC/CEN/ENTR/000/2007-23

Final report

ATTACHMENT 2

FINAL VERSION OF THE CONFORMANCE/INTEROPERABILITY REPORT

Approved by the Biometrics Focus Group

2009-06-11

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Technical Report

A consensus on conformance and interoperability mechanisms, both for applications and sensors, in order to reach security evaluated interoperable solutions between the European Union Member States

V1.01

Focus Group on Biometrics

Distribution list:

Name (alphabetically)	**Department**	**Location**
Focus Group on Biometrics – members	CEN	Brussels

Author: Dr. Andreas Wolf
Inspector: Dr. Jean Salomon

File: report2-20090329
Status: final
Date: 2009-03-29
File:

Document Management

History of changes

Version	Status	Date	Person resp.	Reason for Change
0.20	1st draft (posted)	17/06/2008	JS	Wrong formatting – revisions required by Focus Group
0.22	draft	21/06/2008	AW	First update following D. Statham's early remarks
0.23	draft	30/06/2008	JS	Additional update following N. Delvaux' later remarks
0.35	draft (posted)	19/09/2008	AW	Ongoing preparation of the content material
0.45	draft	28/11/2008	AW/JS	Revised version considering results of the London meeting and comments to the authors from John Dale, Nicolas Delvaux, and John Larmouth
0.50	draft (posted)	01/12/2008	AW/JS	Draft for the next FG meeting in December in Berlin
0.51	draft (posted)	12/12/2008	AW/JS	ISO copyright inserted
0.60	draft (posted)	04/02/2009	AW/JS	Almost ready, contains executive summary and glossary plus references
0.61	draft	16/02/2009	AW/JS	Replaced annexes D1 and D2
0.7	draft	12/03/2009	AW/JS	Integration with resolved DoC from FGB meeting on March 3
1.01	Final (posted)	29/03/2009	AW/JS	Integration with comments from Asbjorn Hovsto and Philip Statham

Persons authorized to make changes

Dr. Andreas WOLF, Cross Match Technologies GmbH
Dr. Jean SALOMON, JSCP

Copyright acknowledgement

Annex A1 to A7 may refer to ISO ISO/IEC JTC 1 SC 17 WG 3, ISO/IEC JTC 1 SC 27, ISO/IEC JTC 1 SC 37, and TC 68 Standards under the form of abstracts, mainly those of the Scope of each Standard.

These abstracts are reproduced with the permission of the International Organization for Standardization, ISO. The concerned documents can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

Cooperation acknowledgement

The authors are grateful to CEN and AFNOR for enabling them to fulfil this work. Furthermore they want to thank the members of the Focus Group on Biometrics for their guidance, assistance and encouragements.

Document was created using the following tools:

Microsoft Word 2003

Microsoft Visio 2003

Table of Contents

1. Executive Summary

This report aims to support decision makers in European and national contexts who want to establish interoperable and reliable solutions based on biometric technology. Special emphasis is given to applications in context of air travel, that is, to border control, airline and airport processes, even if the suggestions and conclusions can also be applied to other similar fields. Although the report is written for Europe, it could also be used as a basis for considerations in other parts of the world, too.

The report lists its objectives and background information, followed by a description of the fields of interest, constraints, and the role of the various stakeholders of a European biometrics interoperability initiative. Based on an analysis of the current work and existing applicable standards and followed by a description of the main applications, recommendations and requirements are given to promote interoperable European biometric solutions. These requirements and recommendations form the main part of the report. They are based on common sense and the expertise of the authors of the report as well as of the members of the CEN Focus Group on Biometrics.

The topics that are covered in the requirements and recommendations Section include general considerations, the inclusion of biometric and non-biometric modalities, sensor properties, data quality aspects as well as data quality assurance, spoof prevention and other security aspects, interfaces and data exchange formats, scalability, reliability, robustness, maintainability and safeguarding aspects, environmental conditions, privacy and data protection related questions, accessibility, health, societal, cultural and ethnical aspects, usability, ergonomics, and user acceptance considerations, applications and reference implementations as well as certification schemes.

It is intended that the arguments given therein are used as a template by the European Union and its Member States to prepare decisions on planning, deploying and maintaining projects using biometric components and requiring long term and/or international interoperability.

In the following we summarize the most important recommendations of this report. Rationales are given in the body of the report. The structure of the following paragraphs reflects the structure of the recommendations Section 7.

General recommendations (see 7.1). Take advantage of EU's knowledge base, industrial biometric expertise and experience gathered from already existing biometrics pilots through each EU national body to further commonly support, from within the SC37, EU led initiatives in the future. The operational team for such project could result from a coordinated effort of the present CEN Biometrics Focus Group, or from any other ad hoc mission-critical entity based on a similar pool of EU-centric expertise which could operate, as an example, from within an existing EU Technical Committee, on standardization and certification harmonization and coordination issues.

Recommendations on biometric modalities (see 7.2). Concentrate efforts on face and fingerprint modalities. Anticipate iris as a potential modality for identity management in Europe. Set up mechanisms for conformance and interoperability assurance at the template level (and not only at the image level) to avoid a monopoly. Compliance to ISO/IEC 19794-2 is only the first step on the way to true interoperability. Ensure compliance to European and international regulations and standards for all data storage media including travel documents. Deploy multimodal solutions wherever affordable.

Recommendations on non-biometric data (see 7.3). Deploy multimodal solutions also integrating non-biometric data such as passengers' biographic data and travel history, which become an essential part of the mandatory information required by major non EU countries to pre-screen travellers before they actually depart. Seek alignment while collecting major common non-biometric fields from PNR and API data across EU Member States to further increase security across the entire common Schengen border.

Recommendations on sensors (see 7.4). Set up certification schemes for sensors to maintain a minimum application and modality specific quality level for face, fingerprint and (in the future) iris sensors.

Recommendations on data quality and data quality assurance (see 7.5). Introduce “best practice” rules for biometric data capture. Initial efforts should be concentrated on data acquired during the enrolment stage, as non conformances and poor quality in capturing a face or finger image would severely hamper any subsequent usage of an MRTD, e-visa or other token for ID management at the border, especially during ABC operations. If possible, ensure identical acceptance criteria for all quality assurance products. In the future, approve quality assessment algorithms and test procedures. An EU-wide deployment of unique quality assurance software could minimize technological risks, yet this might be impracticable because of political and commercial considerations. The lack of unified quality requirements for fingerprint images could cause compatibility problems for the EU Visa Information System (VIS).

Recommendations on spoof prevention and other security aspects (see 7.6). Evaluate the biometric performance of the algorithms to be used, the spoof resistance of a sensor, and the deployment characteristics separately for every application. Develop recommendations on standard FAR and FRR values for specific cross border applications and other security relevant application types across Member States.

Recommendations on interfaces and data exchange formats (see 7.7). Ensure that any ABC (Automated Border Control) system deployed in any EU Member State can interact with any other ABC system within the EU. Favour leadership of the EU industry when publishing requirements, through research programmes, and provide appropriate financial support. Where possible, adopt appropriate international biometric data interchange standards across the EU, including standards like CBEFF (ISO/IEC 19785-x), Biometric Data Interchange Formats (ISO/IEC 19794-x), especially Part 4 (Finger Image Data), Part 5 (Face Image Data), and, in the future, Part 6 (Iris Image data).

Recommendations on scalability and fallback solutions (see 7.8). Maintain a stable balance between security, throughput, and usability related requirements with respect to sensors, algorithms, and workflows to avoid security breaches. Maintain scalability also with respect to biometric discrimination power, and overall system performance. Fallback systems and backwards compatibility have to be in place to deal with people who do not possess the required biometrically enabled travel documents or whose biometric characteristics cannot be successfully verified.

Recommendations on reliability, robustness, maintainability and safeguarding (see 7.9). Ensure that the biometric components of all large scale and distributed biometric solutions have capabilities for automated quality assurance with respect to quality of the captured biometric data, sensor quality, and reference data quality. Include EU-centric and EU-specific criteria in SLAs to favour local maintenance.

Recommendations on environmental conditions (see 7.10). Evaluate the performance of a solution under realistic environmental conditions.

Recommendations on privacy and data protection (see 7.11). Develop guidelines for privacy-friendly systems which can be approved by the data protection authorities of the Member States. Involve data protection authorities as soon as possible and use any positive feedback as potential leverage to increase European supplier recognition outside the EU.

Recommendations on accessibility (see 7.12). Address the specific needs of disabled people in all relevant system specifications. Define specific accessibility requirements and design a test guideline. Provide alternative workflows ensuring that nobody is excluded from using a certain system because of his or her disability.

Recommendations on health, societal, cultural and ethnical aspects (see 7.13). Review and implement requirements of ISO/IEC TR 24714-1 in EU biometric systems.

Recommendations on usability, ergonomics, and user acceptance (see 7.14). Review and implement requirements of ISO/IEC TR 24714-1 in EU systems. Inform and seek citizens’ approval based on practical experiences, advantages and perceived value.

Recommendations on applications and reference implementations (see 7.15). Specify and where necessary develop appropriate profiles covering application characteristics for typical border control processes.

Recommendations on certification schemes and certification centres (see 7.16). Set up a certification procedure for accredited laboratories to evaluate the performance, interoperability and quality of biometric technology and biometric systems. Put the main focus on quality assurance of facial and fingerprint modalities as main modalities in ICAO Doc 9303 compliant travel documents in accordance with ISO/IEC 19794-4, 19794-5, 19794-6, 19795-x, and 29109-x standards. Create EU certification centres, which would rely mostly on agreed biometrics related ISO standards. Build up EU specific application profiles. Develop aligned verification scenarios for equipment, applications, and infrastructure compliance, while providing overall guidance to Member States.

Some concluding remarks:

- Biometric technology improves security if consistently applied across all processes.
- Continue involving the European biometrics community as early as possible.
- EU academic and industrial expertise is available and should be used.
- Rely on available ISO standards in setting up certification centres.
- Strive at enhancing perceived public value of biometrics.
- Challenge, yet support the European industry.
- Rely on standards whenever possible.

2. Report Objectives

2.1. Initial Terms of Reference

This report aims at answering the Terms of Reference document [TOR] which was issued by the CEN to the Focus Group. It first quotes some of the introductory guidelines of the CEN Terms of Reference document, to help focusing on the deliverable requested, namely providing guidance on the way to reach biometrics conformance and interoperability while specifically addressing European requirements.

In the original CEN document, the analysis and recommendations to the relevant DGs of the European Commission were expected:

- To ensure that Europe does not lose a market share in the emerging biometrics products market,
- To create awareness among all stakeholders on international standardization activities and their possible impact on the competitiveness of European companies involved in biometric technology,
- To identify any special European requirements,
- To ensure that the international biometrics standards meets those requirements,
- And to contribute to an accrued interoperable European security by leveraging on the deployment of identified goals and targeted standards.

2.2. Scope

This report identifies standards specifying conformance and interoperability mechanisms for biometric products and applications. It addresses the mechanisms emerging in various parts of the world for certification centres performing such tests and validation of products. The report takes into account other European projects such as the BioTesting Europe Project [BTE], and where appropriate, makes recommendations on any further European activity that may be needed.

The report addresses the following:

- Current work and standards,
- Understanding and description of existing architectures related to biometric technologies,
- Analysis of the goals of EU interoperable solutions,
- Suggestion of mechanisms to establish minimum requirements based on the analysis mentioned above,
- Suggestion of mechanisms that may ensure conformance with these requirements.

2.3. Goals

This report has the following purposes:

- Describe the state of the art,
- Understand and describe the needs of the EU with respect to border security, ID cards, and other aspects that require (or suggest) application of biometric technology,
- Understand and describe existing architectures related to biometric technology,
- Analyze goals of EU interoperable solutions with respect to security, recognition performance, throughput, and other aspects,
- Suggest minimum requirements based on the analysis mentioned above,
- Suggest mechanisms that may ensure conformance with these requirements,
- Suggest methods able to promote synergies between requirements and existing products and technologies,
- Suggest methods that may stimulate the scientific institutes and industry to close that gap,
- Suggest mechanisms that ensure that the EU gets and maintains a leading role in research, development, and standardization of biometric technology.

2.4. Non Goals

To separate this report from other projects, the following list determines the topics that are **not** part of our goals.

- Suggesting modifications of political goals,
- Suggesting products and technologies of certain manufacturers.

3. Background

The CEN Terms of Reference document [TOR] provides background information on the context of this report.

In June 2002, the Joint Technical Committee 1 of ISO/IEC established a new Subcommittee on Biometrics. The goal of this SC 37 was to ensure a high priority, focused and comprehensive worldwide approach for the rapid development and approval of formal international biometric standards. These standards have been considered to be necessary for supporting the rapid deployment of significantly better, standard-based open system applications of biometric technology.

The creation of SC 37 was strongly driven by the US National Standardization Body following the 9/11 events. Still today, SC 37 is strongly influenced by the US participants, mostly due to the extent of committing resources and experts to the Work Groups of SC 37 which develop the biometric standards.

Ensuring that European interests are taken into account, and strengthening the European influence in SC 37 and similar standardization organizations should be two important goals for the standardization policy of the EU.

3.1. Political Background

The topic of biometrics is not a new one for the European institutions. A Council regulation was adopted (December 2000) for the establishment of “EURODAC” [2725] which is a fingerprint database of asylum seekers and illegal immigrants. The European Council of Thessaloniki [11638] (June 2003) agreed to go ahead with biometric identifiers in third country nationals’ visas and citizens’ passports. As a consequence, the Council Conclusions proposed to introduce biometric data into travel documents in order to improve the accuracy of identification and make travel documents more secure against counterfeiting.

Regarding the European agenda, five documents originating from the EU institutions constitute the main European platform for the introduction of biometric identifiers:

- 24 September 2003: Proposal for a Council regulation amending (EC)1683/95 [1683] (uniform format for visa) and (EC)1030/02 [1030] (uniform format for residence permits),
- 8 June 2004: Council decision (2004/512/EC) [512] establishing the Visa Information System (VIS),
- 13 December 2004: Council regulation (EC) 2252/2004 [2252] on standards for security features and biometrics in passports and travel documents issued by Member States,
- 28 December 2004: Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2004) 835 [835],
- 28 February 2005: Commission decision C(2005) 409 [409] laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States,
- 28 June 2006: Commission decision C(2006) 2909 [2909] laying down technical specifications on the standards for security features and fingerprint biometric data in passports and travel documents issued by Member States.

The European Parliament passed the Commission Proposal on 2 December 2004 [73] stipulating that biometric data should only be used for verifying the authenticity of the passport and should be handled only by competent authorities. On the other hand the EU passports are just a result of the previous proposals on visa and resident permits. Both requirements are still valid and issuing biometric passports is also mandatory for a country to remain in the US visa waiver [VWP] programme.

In addition, biometrics will surely go beyond the immediate application for border control purposes, towards a wider adoption and use in society: "[that] biometric-based identification will proliferate in society, extending from initial government use to civil and commercial applica-

tions, and [that] this proliferation will have a profound impact on society" (JRC Report EUR 21585 EN [JRC]). As an enabler of identity verification systems, biometrics can play a role in most modern online public services, such as e-government, e-learning and e-health.

In this context, it can be noted that the paper "A Roadmap for a pan-European eIDM Framework by 2010" [eIDM] aims to reach the final objective of "secure means of electronic identification (eID) that maximize user convenience while respecting data protection regulations" by 2010.

An example in relation to biometrics of European specific sensitivities is data protection and privacy.

The Directive 95/46/EC [46] "Protection of individuals with regard to the processing of personal data and on the free movement of such data" applies to the processing of personal data including biometric data by Member States' authorities within the scope of EU Community law. While data protection has an international origin (OECD and the Council of Europe) and international objectives, the European and US approaches to data protection differ on certain points. The European interest has to be well represented in all relevant forums, including international standardization.

Europe's concern on privacy protection is further demonstrated by the recent Commission's Communication "Promoting Data Protection by Privacy Enhancing Technologies (PETs)" (COM(2007) 228 final [228]).

3.2. International Standards Activities

International standards activities include the projects of ISO/IEC JTC 1 SC 37 "Biometrics", which deal exclusively with biometrics standardization.

Specific questions on securing biometric data and on general IT security topics that are also important for biometric systems are discussed in ISO/IEC JTC 1 SC 27 "IT Security Techniques".

ISO/IEC JTC 1 SC 17 "Cards and Personal Identification" deals in Working Group 3 "Machine Readable Travel Documents" with standardization of passports, ID cards, visa, and other travel documents in cooperation with the International Civil Aviation Organization (ICAO). ISO/IEC JTC 1 SC 17 also deals in its Working Group 11 "Application of biometrics to cards and personal identification" with topics like the comparison of biometric data on a smartcard.

ISO TC68/SC 2 "Security management and general banking operations" offers guidelines that have already been applied for large scale heterogeneous banking systems and might be useful also in the context of biometric technology.

3.3. Market Impact

The first (preparatory) meeting of the CEN Biometrics Focus Group took place in early 2004. Since that first meeting, the Group has been well attended by national SC 37 delegates (coming from industry, academia and consumers) as well as by representatives of various European biometrics related projects. There has been regular participation from European Commission representatives. The European Biometrics Forum (EBF) [EBF] also participates in the Focus Group.

If implemented, contributors to the activity will achieve specific **benefits**:

- The European (biometrics) industry will be better prepared to efficiently participate in the SC 37 work and to utilize the results of that work with commercial products that can be certified by European centres.
- European service providers can ensure that the services they offer integrate well with the evolving biometric standards.
- European legislators can make use of expertise on biometrics technologies and standards, to which European requirements can be fed and from whom international trends can be obtained.

- The European citizens will find European requirements such as privacy better reflected in standards work.
- The implementers of European policies will progress in fields such as security, border and immigration management (biometrics in EU travel and identity documents), as well as in application areas such as e-Government (biometrics in support of e-Identity), e-Health, etc.

If not implemented, the result may lead to:

- A continued fragmentation of European expertise in the international standards work,
- A lack of awareness of international standards and their ramifications to the wider European stakeholder community,
- A continued de facto dominance of US interests in the international standards work,
- Security leaks due to a delayed implementation of harmonized visa procedures and common border control standards,
- A set of biometrics standards that do not go beyond the short term US homeland security needs,
- A set of biometrics standards that insufficiently reflect Europe's sensitivities (for example on data protection and privacy issues),
- Further difficulties in introducing and scaling up travel and identification documents of common European interest (e.g. ECC, the European Citizen Card),
- Failure to produce a European business presence in the sales of biometric products,
- The continued need to use US verification centres for certification of conformance to biometrics standards,
- Higher costs for Member States when implementing interoperable biometric applications.

3.4. US Initiatives in Related Areas

The National Science & Technology Council of the Executive Office of the President of the United States of America has established a Policy for Enabling the Development, Adoption and Use of Biometric Standards [NSTC].

The goal of this Policy is to establish a framework to reach consensus between the different stakeholders in the US government on biometric standards adoption. The adoption of appropriate and recommended standards, and associated conformity assessment programmes, shall enable necessary next generation biometric systems in the US, facilitate biometric system interoperability, and enhance the effectiveness of biometrics products and processes.

To enable biometric system interoperability and support the biometrics needs of the US government and its agencies, the following principles will be applied as a guideline:

- Continued development of voluntary consensus standards for biometrics. National and international voluntary biometric standards development activities will be supported.
- Rigorous testing to ensure vendor and system compliance with biometric standards. The development of harmonized conformance, interoperability, performance, security, human factors, and operational scenario testing programmes in support of procurement actions for biometric products, programmes and services shall be supported.
- Standards and conformity assessment processes must be identified and adopted to ensure full interoperability. Available standards shall be reviewed and consensus recommendations regarding which standards should be adopted shall be developed.
- The recommended biometric standards and conformity assessment processes shall be promulgated. A registry of adopted biometric standards will be published.
- The recommended biometric standards and conformity assessment processes will be integrated into governmental plans whenever feasible. Biometric systems should be built and operated based on recommended standards.

4. Towards a European Consensus on Conformance and Interoperability Mechanisms

This Section analyses the European organizations that require European consensus on conformance and interoperability. It explores the advantages of such consensus and reviews the barriers to gaining such consensus.

4.1. Objectives

This report discusses specific European requirements on biometrics standardization by:

- Planning and promoting a converging workflow, starting with input requirements from stakeholders in Europe, into the (necessarily small) group of ISO/IEC JTC 1 SC 37 committee experts, so that SC 37 activities represent the broadest possible consensus and its deliverables integrate the full scale of European stakeholder needs.
- Taking further a topic that cannot be addressed by SC 37 alone: As required in the title of this report, a European consensus is needed on conformance and interoperability mechanisms to ensure security evaluated interoperable biometric solutions.

4.2. Stakeholders

The main European stakeholders of a potential European biometric technology initiative are:

- European companies developing and manufacturing biometric products, technologies, and services,
- European system integrators which need awareness of available biometric technology and standards,
- National bodies that do or do not actively participate in the international standardization processes,
- Governments and Parliaments of the EU Member States that need to be aware of standards and recommendations of EU experts to be considered for future requirements and procurements,
- European universities, research institutes, and other academia,
- Data protection, privacy, and similar organizations including NGOs which have a certain influence on the public view and acceptance on biometric technology.

4.3. European Organizations Requiring Conformance and Interoperability

There are a number of bodies that require conformance and interoperability. Some requirements are defined at an International level, while others will only be relevant at an EU level.

Some international level requirements may benefit from European supporting documents to address specific EU legal conditions, or perhaps common user interfaces across EU member states.

The list of sectors with their associated bodies that have growing requirements for conformance and interoperability include:

- Border control and criminal justice,
- Cross border transportation,
- (e-)Healthcare,
- e-Government,
- Banking,
- Railway stations,
- Nuclear power facilities and other sensitive industrial sites,
- Military installations.

4.4. Advantages of Conformance and Interoperability

Some of the sectors listed in 4.3 already have standards, practices or protocols in place to provide conformance and interoperability, either at an international or European level. However, the freedom of movement of European citizens to live and work across the EU will continue to drive further development of these mechanisms. There will be an increasing demand of these mechanisms to employ biometrics as a means of personal identity or verification.

4.5. Barriers to Consensus

Although the entities represented in the sectors listed in 4.3 are either global commercial organizations or have inter-government bodies to operate at an international level, the sectors are generally fragmented, especially in the commercial domain. There is also no consistency across borders as to whether a sector is government led or commercially operated.

Each sector has different priorities and different timescales for cross border interoperability. Therefore, local-only solutions tend to get favoured and implemented. These may pick up on some standardization (in particular from ISO standards), but would all be likely to benefit from a cross border consensus and from coordinated projects.

5. Current Work & Relevant Existing Standards

There is a large body of work that has either been completed, is in progress, or is planned at international, European, and national level, that form a foundation for a European consensus on conformance and interoperability.

Much of this work is listed and detailed in Annexes A1 to A7. The list is not offered as being complete and does not address any other processes or protocols used by any cross border organizations to achieve conformance and interoperability.

There are some projects and infrastructures that are especially important for reaching EU-wide interoperability of biometric systems. These projects are reviewed in 5.1 to 5.4.

5.1. Visa Information System (VIS)

Originally an outcome of the events of September 11, 2001, the VIS has retained some of the initial anti-terrorist characteristics shared with its US-VISIT US contemporary counterpart, yet its main focus remains the fight against illegal immigration.

The VIS was established by a European Council Decision (2004/512/EC) on June 8, 2004 [512]. It is a particularly important tool for strengthening the area of security, freedom and justice.

The regulation governing the VIS allows the competent authorities (in particular visa, border and immigration agencies) to store and further retrieve in a central European database alphanumeric and biometric data (digital photo of the face plus ten flat fingerprints) on visa applicants and on visas which have been applied for, issued, denied, revoked, or withdrawn.

Benefits from implementing the VIS are manifold, and are geared to help prevent and investigate terrorism and other serious crime. The process efficiency was successfully tested in the initial BioDev programmes (see 5.4.):

- At the consular post, by preventing the so called “visa shopping” (whereby a given visa applicant, after being denied a visa by a certain EU Member State at its consulate, would probe other EU consulates in his home country, hoping to finally break through and enter the Schengen area through another Member State) early at the enrolment phase, together with improved consular co-operation,
- At a Schengen border check-point, by trapping holders of invalid or forged visas, as well as matching the biometric data of the visa holder vs. the data of the person to whom the visa was originally issued, thereby preventing this kind of identity theft.

The VIS relies on the BMS, a Biometric Matching System, which provides a “hit/no hit” reply for all Member States inquiries (e.g. a “hit” for an already known individual impersonating a “new” visa applicant). The BMS is expected to gradually evolve into the world’s largest biometric data base search and match engine. Yet, the present lack of existing common EU biometric data quality criteria may affect the accuracy and the efficiency of any BMS response, especially with the expansion of the overall data base size. Whether a VIS/BMS query would involve four fingers for a 1:1 verification of a visa holder or ten fingers for a 1:n identification of an unknown individual, consistency in the search outcome is clearly dependant on the quality of the biometric data captured initially. In the absence of standards and certification procedures (unlike NIST and the FBI in the US), and with little compatibility in quality control amongst the major AFIS providers, less than optimal query results are to be expected.

As all Member States would connect at their own pace to the VIS once the initial cutover is declared, there still is a sizeable time window to agree on a common platform to evaluate conformance and interoperability between biometric procedures, including image quality and the major biometric sensor properties.

Moreover, the inherent flexibility in the life span of visa granting would induce the later re-registration of a visa applicant, and further enhance security, as updated biometrics data sets with more stringent, EU-harmonized enrolment quality control would have become customary in the meantime.

5.2. Schengen Information System II (SIS II)

The Schengen Information System (SIS) has been operational since March 1995, initially enabling five EU countries to share a common text-only data base to record the details of millions of people and items of interest to police, customs and immigration authorities.

It worked since its inception as a police and border alert system for Member States of the Schengen Treaty containing data on persons wanted for extradition, on aliens for whom entry was refused, on missing persons or witnesses placed under police protection, on persons or vehicles potentially involved in serious crime, as well as on sensitive objects such as stolen vehicles, firearms, documents, or banknotes.

As it became necessary to connect the states which progressively joined the EU, and as Schengen's commitment was to abolish controls at the internal borders of these countries, the existence of a new larger scale generation of the SIS called SIS II, also catalyzed by the 9/11 events, was planned to include storage of biometric data and handle the increased data volumes required by all EU Member States.

Since the delivery of the SIS infrastructure was delayed, EU Member States decided at the end of 2006 to essentially clone the existing Portugal's national system's connection to the SIS across all current Member States, which was introduced as "SISone4all". This paved the way for the creation of common technical prerequisites to abolish controls at internal land and sea borders of the new Member States by late December 2007 and controls at air borders of these countries by Spring 2008 (except for Cyprus).

Delays continue to affect the SIS II project (presently at the life testing stage by separate EU Member States), thus extending the shelve life of the "SISone4all" interim solution to also include Switzerland.

The SIS II infrastructure will be used to control and regulate traffic of all BMS queries which Member States should be able to launch concomitantly, in particular with respect to eligibility of visa holders to enter the Schengen area.

5.3. BioTesting Europe

The BioTesting Europe project [BTE], partly funded by the European Commission under PASR2006, aims at setting out the prerequisites for the establishment of testing and certification capabilities on biometric components and systems in Europe.

Partners in this "think tank" project include German and UK academic institutions as well as the European Biometrics Forum.

The project members were sensitized to the lack of adequate testing criteria and of compliance tests to verify the conformity of the biometric components and systems to certain standards. They also reacted to the absence of any European testing centres able to perform these tests and publish a list of certified components that would meet certain standards.

The objectives of the project, therefore, include outlining the need for testing and certification schemes, making an inventory of existing capabilities, mapping user requirements and defining the business case. The project aims at establishing a European biometric testing and certification roadmap and a work plan for the further development of European biometrics testing and certification facilities.

It is worth endorsing the opinion stressed by the BioTesting Europe project leader, in particular with the expected need to set up objective criteria for compliance of testing schemes with international standards such as ISO/IEC JTC SC37, and with the recommended use of SC37 data interchange formats to support conformance testing.

5.4. BioDev

BioDev is a two-pronged programme approach of EU Member States which aimed at testing and developing operational experience within the EU towards the biometrics enrolment of third country nationals eligible for short term entry visas into the Schengen area.

In its first version, called BioDev1, capture, storage and verification of biometric data of visa applicants was conducted between 2005 and 2006 by Belgium and France at eight selected consulates abroad, some with high local demand for visas, with about 80 % financed by the European Commission.

The main project focus was on hands-on training and learning at each step of the process: technical aspects relevant to the staff (feasibility and performance), organizational matters (procedures and workflow redesign, partitioning IT resources and responsibilities between the Ministry of Interior and the Ministry of Foreign Affairs), biometric ergonomics (both at the enrolment centre and the immigration post), quality of ID flats biometric capture (different spread according to geographical origin), the acceptance by both the applicants and the general public, as well as the destination authorities.

Within 13 months, 70,000 visas were issued abroad and controlled at seven air terminals and one seaport in Belgium and France.

Amongst the initial lessons learned, some were favourable to increasing the biometric matching performance. These involved revisiting and securing the operational workflow at the foreign consulates: educating the consulate enrolment staff to re-establish control over the overall application sequence, and training them to achieve better biometric data quality during enrolment, were two of the major points.

In spite of an increased transaction time due to the biometric verification of the visa holder upon arrival, decreasing flow congestion at the arrival border control by ad hoc ergonomics adjustments and the progressive fine tuning of the immigration staff deployment proved to be beneficial to public acceptance, and helped focusing on future programme expansion.

Starting 2007, this programme was extended, as BioDev2, to six other EU Member States enabling the new Member States to become more knowledgeable in enrolment matters.

The major challenges of the programme's extension were to test the process interoperability across the existing nations' AFIS programmes, and to reinforce the cooperation between the Member States at the various consular posts, while preparing to run a reduced scale pilot of the VIS standards. The principle of common enrolment consular posts between several Member States was successfully tested in both possible configurations: common consular post limited to visa application and enrolment, or common consular post for all steps, including visa delivery. Encouraging results were obtained in catching false IDs as well as visa shoppers.

Thanks to the lessons learned, the dual BioDev experience turned into a fairly successful pilot testing for some of the future VIS system prerequisites, even if on a low deployment scale only. In view of the present data set size and the need for pre-existing conformance criteria, additional analysis needs to be performed on biometric image quality (NIST NFIQ spread), on true biometric interoperability and on controlling the error rates of biometric comparisons.

Some of the initial Member States did continue to expand their local biometric visa programmes beyond BioDev (like the VISABIO programme in France), aiming for a smooth and continuous integration into the generalized VIS as soon as the latter will reach cutover.

6. Targeted Applications

Applications which would benefit from such an approach are manifold. This report emphasizes two cases dealing with security at border control, mainly at airports. Other applications with a growing requirement for biometrics conformance and interoperability include railway stations, criminal justice, nuclear power facilities and other sensitive industrial sites, military installations as well as e-government, healthcare and banking, as listed in 4.3.

6.1. Enrolment for MRTD, Visa, and Registered Traveller Programmes

Within the scope of the targeted applications, three different cases of enrolment are reviewed as follows:

MRTD Enrolment

Enrolment processes for MRTD are a vital part of the quality assurance of the global security chain and key in the success of MRTD Border Control deployment. Enrolment is usually performed in a decentralized way, and, depending on the case, the presence of the applicant is required during the application and possibly also at the MRTD delivery time, so that impersonation cases and/or illegal MRTD pickups can be detected by qualified staff.

Besides the intrinsic secure character of the document itself (adequate hidden security features, resistance to tamper, durability, proper functioning of the electronic part including the network-maintained various electronic certificates, etc.) **two main factors** are to be considered with respect to any future use of biometrics and the Machine Readable Travel Document itself.

- The first factor deals with the **breeder documents** required to obtain or renew an MRTD and the associated task to clearly establish whether the applicant really owns the identity he claims at enrolment. Due to the different solutions taken to issue, use and control the necessary breeder documents by each nation (spread of types and number of different birth certificates, existence of a national registry, etc.), it appears that different nations, including EU Member States, may end up with bearing a different risk to deliver perfectly "legitimate" e-MRTDs with "secured" biometrics, yet based on a forged identity. Such a discrepancy in the trustworthiness of a given country's MRTD's issuance would negate the global efforts to harmonize the level of biometric control in the evolving Schengen environment. Both EU and ICAO have recognized the need to address the breeder document issue [EUBD, WP4]. It appears, though, that each nation may have to first tackle the problem separately, in order to come up with some common agreement on breeder documents at a later stage [Hist].
- The second factor concerns the **quality of the biometric data captured** to be loaded into an e-MRTD chip, which will impact the document's later use, say for ID verification at an ABC gate. With the introduction of the first e-Passport generation, a larger than expected variance in the quality of the digital face image collected (pixel distance between centres of eyes, front facial constraints, tilt angle, etc.) was initially found to hamper subsequent usage, both for verification and identification purposes in face recognition trials. A first level of adjustment was found necessary. ICAO was able to provide recommended specifications in Doc 9303. Acceptance criteria for the capture of the e-Passport face image were subsequently included in the image capture software. Such software is typically used in the photographer's kiosk, at the enrolment centre or off-premises. When performed at the enrolment centre back-office, the quality control of each digital image brought (or sent) by the citizen yielded a higher acceptance rate.

The same concern for data quality also applies for the other ICAO compliant biometric data (i.e., fingerprint and iris images) during initial capture at the enrolment centre. The cross-industry application of a conformance platform, of common quality controls and of acceptance criteria is paramount to increase the usability of the biometric data contained in the MRTDs.

Visa Enrolment

As explained earlier about the two BioDev projects in 5.4, the introduction of face and ID flats capture during visa enrolment at consular posts required significant changes in the application and processing workflows. To cope with the associated costs of expanding the biometric visas through enrolment centres at the major consulate posts, pooling visa applications for several EU member destinations in a single enrolment data centre abroad would become more attractive. Besides the favourable cost issue, the development of consolidated enrolment centres would also facilitate the task of early visa shopping deterrence at the country of origin. Such centres would also be good live environments to collect shared data of adequate quality while further promoting workflow harmonization, aligning procedures, training staff, and comparing equipment performance amongst many EU Member States, hence possibly leading to better biometrics compatibility.

Registered Traveller Enrolment

Whether for private or public Registered Travel (RT) Programmes, enrolment is performed by a nation's Control Authority, police, immigration, or border control. In some cases, a pre-registration is required prior to the actual interview with an officer. Enrolment includes the capture of one or more biometric modalities, as well as a comprehensive background check against various nation's or international police and security data bases, which may result in a deferred acceptance (or denial). Membership in RT programmes, whether free or involving payment, is always voluntary, but can be revoked any time at the Control Authority's sole decision. Some RT programmes, especially when private (such as the Dutch PRIVIUM), deliver a membership card containing a biometric feature or points to a record in the RT data base the incoming traveller's identity is compared with. The goal of RT programmes, by pre-discriminating lower risk, known travellers who did successfully enrol, is to facilitate and speed up their travel process, including border crossing (for all EU based RT programmes, which will be reviewed in 6.2 below).

Some non EU-based RT programmes (like VIP CLEAR in the USA, where both fingerprint and iris are captured) were originally targeting a paying fast track access to airport security check-points only, without connection to border control. More recently, the official May 2008 agreement between The Netherlands and the USA launched a bilateral international RT programme, where both the Dutch PRIVIUM and the new-born US Global Entry RT programmes would be extended (cross-linked) between selected US airports and Schiphol, allowing pre-registered travellers from one programme to use the other programme's facilities and privileges.

As both programmes did not originally use the same biometric modalities (iris for PRIVIUM, fingerprint and face for Global Entry), the potential need to extend each local enrolment in the future (to satisfy the remote country's enrolment and evaluation criteria) further increases the strong necessity for a fast and successful harmonization of biometrics interoperability criteria along a common platform.

Another US based example worth noting is the RTIC (Registered Traveler Interoperability Consortium) [RTIC], which sheds some light on a possible way to go.

After its initial 2005 launch by the American Association of Airport Executives, this consortium, mostly comprising US private companies liaising with the TSA, proposed through its ad hoc Technical Interoperability Standards Working Group a way to establish a technical interoperability standard that enables the inclusion of any airport and any service provider into a national RT programme, which was targeted to use four fingerprints and two iris images stored on a smart card. Of greater relevance to any future EU-centric RT programme development is their conclusion to establish conformance testing to expand the RTIC to new service providers, based on system interoperability, quality of service, existence of SLAs and strict compliance with common policies and procedures.

RTIC's practical recommendation was to establish an RT Conformance Lab, which would play a central role in both establishing initial interoperability, and maintaining it across multiple service providers.

This would also pave the way for more seamlessness, yet more control, in multi-centric RT enrolment processes in the future.

An RTIC Conformance Lab should house provider platforms and perform required tests with the active participation of the interested parties. As biometrics technology vendors have been an important part of the initial RTIC core team, some of the lessons learned by this consortium may well be taken into account to help focus the much anticipated EU-centred approach.

6.2. Automated Border Control (ABC)

Set-Up and Goals

In ICAO's Technical Report entitled "Guidelines for e-MRTD & Passenger Facilitation" [TAG18], an Automated Border Control (ABC) system "authenticates the e-MRTD, establishes that the passenger is the rightful holder of the document, queries border control records, and automatically determines eligibility for border crossing according to predefined rules.

While automation does not necessarily mean improving travellers' throughput across a border, one of the main advantages of ABC systems is to enable the redeployment of skilled immigration officers, border police, and customs agents previously attached to document inspection of all incoming travellers at the control points. The goal is to let the control authorities spend more time dealing with higher risk profile travellers in a dynamically risk-based approach.

Thus, the net gain expected in deploying ABC systems is in the overall security of the border crossing process. The use of biometric data is key in reaching such an objective, by performing the necessary verifications during all steps of the Automated Border Control procedures.

The traveller using an ABC system will be subject to a live biometrics capture (finger, face or iris, if ICAO compliant) at border crossing time. Access across a turnstile, a sliding gate or a full man-trap is either granted or denied following biometric matching, proper automated document inspection and multiple searches in various security data bases. Travellers are reverted to secondary manual inspection if access is denied, either by the ABC system itself (through a side door), or by an inspector in constant remote connection with the system, who can override the automated decision.

Implementation

Two types of ABC programmes can be implemented.

- The traveller does not need to be pre-enrolled, if the border control agency has opened its ABC lanes to legitimate e-MRTD holders from different countries. SEF, the Portuguese immigration agency, started running its automated "RAPID" border crossing programme at major domestic airports for EU e-Passport holding travellers. Authorized users could be called "trusted travellers", simply because of the "trusted" character (in SEF's eyes) of the e-Passport being used as common token.
- Contrary to the previous case, prior enrolment is mandatory in all so-called "Registered Travellers" programmes. Prior to the first travel, enrolment is performed by police or border control agencies and includes interviews, biometrics capture and (off-line) background checks. Successful vetting and credentialing afford a status of "registered" to the traveller. However, this status and all subsequent advantages coupled to it (e.g. use of "fast tracks" and ABC systems) are subject to discretionary revocation by the issuing control authority. This is the case for the privately owned "PRIVIUM" programme in The Netherlands.

Use of Travel Documents/Biometric Tokens

Two operational ABC solutions are available with different MRTD requirements during the process:

- Most ABC systems operational today require the traveller to present a token (a smart card or an [e]MRTD) to the system, in order to initialize the biometric matching process.
- Other systems, like the UK "IRIS" system deployed at many BAA airports, require no documentary claim of identity, and rely only on live biometrics capture of pre-enrolled qualified (vetted) travellers at border crossing. Immediate (1:n) checks against an up-to-date list of authorized travellers would, thus, take place without any document inspection during the ABC process. Some legislation might require that travellers carry a valid travel document. This can't be ensured in document-less processes.

Role of Biometrics in ABC

A number of European States have already implemented an Automated Border Control system, some as pilot initiatives and some intended as ongoing operational systems. Both public and privately owned systems have proven to be scalable, with the appropriate sensitivity to privacy and societal factors.

While no ABC programme can function without live biometric data capture during the process, there is, as of today, no convergence on the use of a given or preferred biometric modality, and few systems are using the e-MRTD as token. However, it is expected that, with its wider adoption, more states will decide to use the e-MRTD as a token in future systems for both types of ABC implementations described in the previous paragraph (with and without enrolment).

The most recent agreement signed between The Netherlands and the USA for the launch of an international Registered Traveller programme between several airports (May 2008) should also contribute to further ABC expansion, via appropriate international airport "Fast Tracks". Strict rules of biometrics cross-certifications, supporting for example remote biometrics capture at enrolment by each partner's organization, and all associated privacy concerns, need to further evolve and become harmonized.

Because of the high traffic load in and out of the Schengen area, EU may seem an attractive focal point for a future global Registered Traveller scheme, yet major challenges need to be addressed first (e.g. active links to a proper tallying of entries and exits).

Different Applications and Workflows for Different Traveller Categories

Several cases of ABC usage may be distinguished according to the different flight origins and destinations and depending on the nationality and MRTD of the bearer:

- **Schengen border crossing:** Installed ABC equipment should serve EU nationals holding an e-Passport, and could in principle also benefit third country nationals holding a valid biometric visa, although predefined separate immigration lanes for visa holders may preferably be used to better segment the incoming traveller flow and improve the inspection officer supervision.
- **Non-EU e-Passport holders:** Sharing the same ABC resources for RT programme members with non-EU nationality (instead of using other dedicated lanes) might be found attractive, although planning ahead to include the entire sensor range at the ABC gates is a necessity. As the traffic in large airport hubs is synchronized along several daily peak waves, flexibility in diverting incoming border controls to the most appropriate channel would be an additional workflow parameter, on top of the risk management approach controlling the extent of automation and of random secondary controls. However, multiple biometrics operating on the same ABC gates under different RT or other multi-national programmes necessitate an additional layer of performance monitoring to prevent drifts and security breaches. This should be carefully analyzed before on-site launching and maintained under close scrutiny.
- **Regular Passport holders with visas:** Third country nationals who have been pre-qualified during their remote consulate application by a careful background check, including a clearance following VIS visa shopper data base query, should be considered as bona fide travellers by the incoming country, as long as no identity substitution can occur at border crossing time. Their MRTD holds the required visa sticker through which a link

could be established to the collected face and finger biometrics. Thus, if so desired, they may well benefit from an automated immigration lane as well, provided that multiple biometrics capture could reduce the risk of identity substitution. They could even share a common ABC resource with RT programme members of a different type, depending on traffic, commercial as well as threat level considerations. These travellers would not qualify, however, in the absence of an e-Passport, for a fast track through an e-Passport driven ABC, such as the Portugal RAPID programme applicable to EU (and other visa waiver country) members.

- **Regular Passport holders from visa waiver countries:** At a large majority, the traveller population falling into this category will benefit from an e-Passport as soon as their current MRTD expires or gets filled up with stamped visas. Although the traveller mix and the airport location strongly influence the respective profile types on an airport-by-airport base only, the relative importance of this class of MRTD carriers will have decayed significantly in every airport within 5 years. In the meantime, ABC programmes most appropriate for this class of travellers include RT programmes using a proprietary e-token like PRIVIUM, as well as document-free ABC solutions such as the UK IRIS programme, both with prior enrolment.

All these four types of passengers will cross the European borders. Even if a preference with respect to fingerprint biometrics can be observed at the moment, it may not be assumed that all travellers will have fingerprint data in their travel documents (passport or visa), at least not in the foreseeable future. How to deal with those different kinds of passengers should be left to the discretion of the Member States, especially with respect to customizing Automated Border Crossing operations.

Promoting Europe's Experience

A list of major ABC systems deployed worldwide, including a summary of their features, can be found in Annex A of ICAO's "Guidelines for e-MRTD & Passenger Facilitation". In a few countries such as Singapore, comprehensive biometric enhanced ABC is deployed even beyond airports to include pedestrian, cycles and even car border crossing in- and out of Malaysia.

Data relevant to the major ABC EU projects, Amsterdam Schiphol ("PRIVIUM"), UK BAA airports ("IRIS"), Frankfurt Airport ("ABG"), Portugal ("RAPID"), and Paris CDG Airport ("PEGASE") is presented at Annexes C1 to C6 and summarized below.

PROJECT	**IRIS**	**PRIVIUM**	**RAPID***	**ABG**	**PEGASE****
Country	UK	NL	PT	DE	FR
Biometry used	Iris	Iris	Face	Iris	Fingerprint
Enrolment	Yes	Yes	No	Yes	Yes
Public/Private	Public	Private	Public	Public	Public
Membership fee	No	Yes	No	No	No
Eligibility	UK and permanent residents	EU citizens	EU citizens, Swiss citizens	EU citizens, Swiss citizens	French citizens

* Meanwhile (as of early 2009), the **RAPID** model has also been implemented as pilot in a few non Portuguese airports such as Manchester.

** It is worth noting that the **PEGASE** project will finally evolve (as of 2009) into its next generation, dubbed **PARAFES**, which extends the points of control beyond the original Paris Airport locations

In spite of the diversity of solutions implemented, the common factor for the five projects is a good acceptance by the travellers and a steady growth of enrolees/users and of total border crossings.

The international deployment of ABC systems is likely to provide major benefits to both travellers and government stakeholders via systematic travel document authentication, biometrics verification and black list search. EU installations with reduced direct manpower supervision would allow productive inspection resource redeployment, together with user friendly

automated border crossing by the travellers. They would also favour biometrically enabled passenger flow channels though an increased common use of MRTDs and other travel tokens.

On the other hand, ABC systems generate some challenges to be met. The deployment of automated systems will reduce the amount of human interaction for most travellers. That is, any necessary guidance must be given in some other way with a concerted, carefully planned learning programme. It is a challenge to adapt process flow management, traveller prompting, pictograms, signage, educational broadcasts, etc. This would be even more challenging for road border crossing. Furthermore, the reduction of human interaction causes completely new security threats which have to be addressed. That is, it is essential to perform a complete security assessment for any ABC solution in its application context: All aspects that are covered in staffed border gates by the expertise of the human border guards would need to be handled by automated systems. This would include, among other aspects, spoof prevention, document status verification, prevention of a second person illegally passing through a gate accompanying a legal traveller (sometimes known as piggybacking), data quality assurance, and user guidance. As of today, automated decisions made by ABC systems can be overruled by senior inspectors remaining in close vicinity and monitoring the activity of a pool of several gates. This "remote control" trend is also in line with EU recommendations on the limits of automated decision making processes affecting rights of individuals [CHR], and likely to remain in any case in the years to come.

6.3. Transportation & Airlines: Travel-related Data Aggregates

Bio Data (API)

Advanced Passenger Information data, or API, is identifying the traveller's name, date of birth, gender, citizenship or nationality and travel document data. This information can be obtained from the MRZ of the traveller's MRTD. It was previously requested by the US for incoming transatlantic flights only at or after flight departure time. Today, API data transmission to the receiving state is mandated ahead of each plane departure for most intercontinental flights.

Reservation Related Data (PNR)

Passenger Name Record data, or PNR data, are detailed data about passengers, mostly personal and confidential, which airlines have for many years collected for their own operational and commercial purposes, but which they are now increasingly obliged to communicate to the authorities of the country of destination. The prime purpose of this is the combating of terrorism and serious organized crime.

Many countries have been collecting the PNR data of incoming passengers for a number of years, using it to grant or deny them the right to visit; those countries include the United States, Canada, Australia, and, historically first among EU Member States, the United Kingdom. Long debates, including security and privacy considerations, especially between the EU and the US, have led to a "reduced" list of 19 commonly accepted fields, which are listed in Annex E.

Enhancing the Distributed Collection and Usage of Biometrics, integrating API and PNR data with Biometrics to improve the risk assessment process

Advanced API and PNR collection is bound to become a standard process for EU countries. This process completes and enhances advanced biometrics collection routinely performed by EU during e-Visa applications of non Visa Waiver Country citizens in the foreign consulates of EU and other states.

As soon as the visa application starts, the future traveller's API is remotely collected long before an actual booking is made. The initial risk assessment by the receiving country is performed following a first background check with biometrics collected at the receiving country's foreign consulate. Added PNR information from the airlines reservation systems passenger

records obtained closer to the expected arrival date provides additional input on ticket payment information, travel history, payment record, as well as other sensitive data. As the time for the actual travel gets closer, refined search transactions integrating biometric data on a given traveller's ID with his most up-to-date PNR and API collected data will further improve each risk assessment process and provide a better decision making tool for comprehensive border management.

Finally, over the years, more visa seeking applicants should hold an e-Passport, the biometric information of which may further facilitate the above data collection process and the overall risk analysis of each application.

6.4. Transportation & Airlines: Biometric Aspects

IATA's SPTIG

A collective effort has been made by major stakeholders in the Transportation Industry to try and expedite passenger processing while maintaining (and, actually, enhancing) the overall journey security.

This process was led under IATA's (International Air Transport Association) umbrella by the SPTIG (Simplified Passenger Travel Interest Group, a.k.a. SPT), which delivered and published an Ideal Passenger Flow (IPF V 2.0, 2006, see Annexes D1 and D2) to describe the successive steps of a passenger journey across the airport (from pre-travel to check-in, security check, border control, boarding and until arrival). The IPF is currently used as a reference, and implemented in part in many airport pilot trials in Europe and elsewhere.

The IPF strongly suggests to reduce as much as possible, via the systematic use of biometric identification, the number of redundant and useless inspection steps (e.g. presenting the same travel document on multiple occasions) encountered by the traveller on his way to the departure gate. The IPF suggests to use a continuous synchronization between the *physical flow* of the passengers across the airport and the *logical IT flow*, where passenger data (e.g. details about flight information, or the weight of a luggage just checked in, or a passenger's last security status) are available and could be retrieved whenever necessary for decision making purposes (e.g. automated boarding control or border clearance).

The requirement of the IPF to unequivocally link the correct physical identity with any query performed during the passenger journey across the airport (e.g. at the X-Ray security checkpoint, or at the boarding gate) should be stressed again. It requires the extensive use of biometric procedures and, possibly, also biometric tokens to establish and maintain each passenger's ID integrity across all airport steps.

Amongst the numerous trials reported by the SPT, the "MiSense" and "MiSensePlus" Heathrow twin pilot projects have been successfully implementing most IPF recommendations, including biometrics secured boarding as well as automated border crossing (see Annex C4).

Following the "Pre-Travel" step, typical passenger stop and control positions at any airport include some (or all) of the following: check-in/baggage drop-off, security (search for weapon on body and hand luggage), immigration, and boarding.

SPTIG's goal is to reduce the number of airport stops needed to authenticate a passenger and establish his right to fly. The main objectives are to reduce multiple, unnecessary ID checks, yet also maintaining an active data link between the passenger location during his progression on the airport premises by querying his most current security status at each used airport control point.

Biometric data usage coupled with MRTDs was recommended as the most effective way to proceed. The order and the number of the stops will depend on the traveller profile (e.g. a "Fast Track" or ABC user), the travel planned (e.g. domestic, international), the type of ticket purchased (e.g. e-ticket with home check-in), the topology of the particular airport terminal, and the governments procedures prevailing.

Even if no unique globally optimized solution can be designed for all airports, intra-Schengen travel means fewer hurdles in all cases with the disappearance of border control.

Check-In

Check-in counter agents currently use swipe readers to input the MRZ of the travellers' ID document linking his identity to the airline reservation systems. Unless instructed to do so by their respective governments, biometrics capture should not happen there. Yet, the initial June 2009 cut-over date set by US DHS for activating airport biometrics capture of all visitors departing from the US may open a Pandora box, should airlines end up being mandated to do so. Similarly, biometric technology is currently not utilized at airport check-in kiosks, which are designed to operate unattended. However, special programmes and Registered Travel enrolments, all involving biometrics, are performed using segregated airport kiosks, and only under a government representative's control.

Passenger Security Checks

The passenger security check is the only airport stop point which is not likely to disappear. It defends the entrance into the so-called "airside", "sterile", or "secure" area. This area is reserved to those passengers (and employees) who cleared both body and hand bag automated and/or manual searches.

It may be the first stop encountered by a traveller with no cargo bag, who already checked-in before reaching this airport (e.g. at home or via Internet) or is travelling "light" on any intra-Schengen or domestic flight.

Entrance control into the security check area is almost always limited to the visual display of a boarding pass (and a cursory look at a picture ID). Surprisingly, no systematic link is established with the departing control system to prove that an unknown incoming traveller really has any business entering the secure area at that time. This security breach has largely remained unchallenged over the years, although cheap and efficient fixes are easy to implement.

For those security check point lanes reserved to Registered Travellers or other operating "Fast Tracks" through the security checks, the above problem is solved, since the entrance filter to the priority lanes is a biometrics-activating token (like the "VIP" smart card from CLEAR, one of the private operators of the TSA-approved US Registered Traveler programme).

Boarding, Self-Boarding and Identity Management

Although very seldom used at the boarding gates, biometrics could help lowering a somewhat untapped risk, dealing with ID substitution, whereby two travellers legitimately cleared to enter a small boarding area or a very large concourse with many boarding gates downstream, may swap destinations because of lax travel document verification during the boarding process.

Such incidents are more likely to occur in countries like the US, where in- and out-bound traveller flows are mixed at major airport terminals, where most boarding gates are used for successive domestic and international departures, and where - in many instances - visual travel document inspection (performed "earlier", upstream at the security check point) is skipped altogether at the boarding gate.

In Europe, even if the above fundamentals are handled differently, ID substitution at boarding is not a totally unlikely event, because of time and passenger pressures.

To increase the agents' effectiveness during the ID matching (and to reduce manpower), parallel self-boarding gates could be appended with the appropriate biometrics equipment for selected token-holding travellers, under the remote supervision of a single agent.

The potential and effectiveness of biometrics usage to combat ID substitution has been established in several European airport trials. Before the UK "MiSense" described in Annex C4, an Air France test conducted in 2002 on the sensitive Paris to Tel Aviv route proposed to voluntary passengers a "one-shot", on-the-spot fingerprint enrolment at check-in, with biometric verification later at the boarding gate, with no document or electronic trace being recorded after boarding. Passengers were eager to enrol and satisfied with the process outcome.

6.5. Transportation & Airlines: Airport Employee Security Checks

Today, airline passengers of flights originating within the EU always undergo comprehensive security checks. Although manually, and sometimes in a cursory way, their identity is verified by the airlines for all travellers and by border guards for flights leaving the Schengen area. As all EU Member States start issuing passports containing facial as well as fingerprint image data by June 2009, and many Member States plan to introduce biometrically enabled ID cards or have already done this, systematic biometric checks for airline passengers become possible.

To promote EU airports as secure entrance and transit gates, it would be useful to claim that airport access control is managed appropriately not only for travellers, but also for staff. Today, airports can't claim conformity to any biometrics procedures, especially not for their staff. In fact, only a minority of airports have implemented biometrics staff access control to the airside (i.e. across the security check area).

ISO SC 37 has published an application profile for access control for airport employees (ISO/IEC 24713-2). This standard should be used as the basis for a EU specification requiring access control mechanisms for airport employees which are at least as complete as checks for passengers. This specification should also contain audit procedures to check compliance with ISO/IEC 24713-2 and security promoted by biometrics sensors reserved for the staff at the security check point and border control immigration points.

The importance of establishing such standard is mainly due to the high turnover rate of airport personnel, typically because of the large number of subcontracted and seasonal airport jobs. A large EU airport would typically have over 3 badges in circulation for 1 active one, with many of the inactive badges not being returned. Impersonation and other illegal uses need to be put under strict control. Thus, rigorous enrolment, vetting and revocation should be an important complement to the anticipated biometrics standards and profiles.

A few EU Member States have already taken legal steps which mandate the permanent use of biometric identification at each land- to air-side crossing for all airport staff, mostly using fingerprint verification. It should be about to shortly rise in the US as well, at least for selected airport pilots [HST].

7. Requirements and Recommendations

Using the EU sectors and applications previously described in this report, which would benefit from a European consensus on conformance and interoperability, the way ahead would be to map these applications against requirements for standards or further projects, aiming at an adequate level of conformance and interoperability across European borders.

This mapping would lead to a gap analysis of where international standards and projects would fall short of such provision. Such a gap analysis establishes a programme of work that would need to be undertaken at European level to obtain consensus.

The gap analysis would include assessing, for each sector and application, such issues as:

- Biometric (and non-biometric) modality selection,
- Sensors,
- Data quality and data quality assurance,
- Spoof prevention and other security aspects,
- Interfaces and exchange formats,
- Scalability,
- Reliability, robustness, maintainability and safeguarding,
- Environmental conditions,
- Privacy and data protection,
- Accessibility,
- Health, societal, cultural and ethnical aspects,
- Usability, ergonomics, and user acceptance,
- Applications and reference implementations,
- Certification schemes.

The following paragraphs stress some aspects which need to be reviewed and used as a starting point for a more thorough investigation.

Requirements related to data network infrastructure, data base architectures, data base throughput, encryption technology, PKI maintenance, physical integrity of the deployed equipment, logistical and political aspects are out of scope for this report and therefore not discussed here.

7.1. General

International standards which are currently being developed and for which priority consensus is found by European experts should be actively supported to ensure that European requirements are submitted and met in the largest possible international standardization framework.

Whenever standards are missing, but would meet an international need, such standards should be started as ISO new work items supported by the European National Bodies. The activities of the European National Bodies should be coordinated in an appropriate way. Ten out of the 24 countries participating in ISO/IEC JTC 1 SC 37 (Czech Republic, Finland, France, Germany, Italy, Norway, Portugal, Spain, Sweden, United Kingdom) and seven of the nine observing countries (Austria, Belgium, Hungary, Ireland, The Netherlands, Poland, Switzerland) are EU Member States or have strong cooperation with the EU [SC37], as of March 16, 2009. That is, the Europe and the EU are able to play a major role in the standards development process, as long as consensus is reached among the European National Bodies. The CEN Biometrics Focus Group might serve as a platform where such a consensus would be maintained.

Where standards are missing, which would not be appropriate for international use, but required by the EU Member States, a European work programme for the generation of such standards could be established. Again, the CEN Biometrics Focus Group could be part of the coordination of such activities.

As far as the Europeans being able to support a European agenda in the development of standards, there would be a clear path to ensure conformance to such requirements across

Europe, where appropriate. This may result in European certification, or some other mechanisms that ensure cross-border trust of compliance.

The EU could support the National Bodies, especially of the new Member States. Topics of common EU interest within SC 37 could be leveraged proactively, including but not limited to synchronizing the National Bodies in SC37 balloting processes. Moreover, on human and societal aspects, CEN could also, as demonstrated in the present Focus Group on Biometrics through its active Consumer Council representation, play a harmonizing role and help equalizing the EU-wide perception and the handling of sensitive privacy issues.

The EU could provide resources for standardization efforts, reference implementations, performance evaluation studies, and prototypical studies. The National Standardization Bodies of the EU Member States could be supported, including financially, ensuring appropriate representation of the EU via its member States in SC 37. This way, the EU could try to coordinate the action of the European National Bodies with respect to ISO. An instrument for that coordinating role could again be the CEN Focus Group on Biometrics, or any other ad hoc mission-critical entity based on a similar pool of EU-centric expertise which could operate, as an example, from within an existing Technical Committees.

In addition to a coordinated action with respect to ISO, the EU could also harmonize the technical level actions of Member States governments with respect to ICAO.

Recommendations

Take advantage of EU's knowledge base, industrial biometric expertise and experience gathered from already existing biometrics pilots through each EU national body to further commonly support, from within the SC37, EU led initiatives in the future.

The operational team for such project could result from a coordinated effort of the present CEN Biometrics Focus Group, or from any other ad hoc mission-critical entity based on a similar pool of EU-centric expertise which could operate, as an example, from within an existing EU Technical Committee, on standardization and certification harmonization and coordination issues.

7.2. Biometric Modalities

In this report, the biometric modalities considered are limited to those chosen by ICAO for Machine Readable Travel Documents applications. These three modalities are facial recognition, fingerprint, and iris. This does not mean that the other biometric modalities could not be useful, even for ABC or in other border control contexts.

To enable large scale interoperability even in heterogeneous systems with components from different vendors applying several algorithms, this report mainly focuses on biometric reference data in the form of images.

ICAO recommends the use of images in Machine Readable Travel Documents, and there is a good reason for that: Up to now, no enrolment data that is based on extracted features (so called templates) has proven to be as interoperable as enrolment based on high quality image data. In the case of finger, face and iris, there are well accepted standards for such images.

On the other hand, ICAO allows the storage of template data in addition to standardized images. Thus, it would be possible to enhance the electronic passports of the EU Member States in a way that they also contain, e.g., fingerprint templates.

Using templates for verification processes, e.g., to decide if the passport presenter is the rightful holder of the document, the use of templates would allow speeding up the process. Reading data from the RFID chip would be faster, and the feature extraction from the reference data stored on the chip would not be necessary.

On the other hand, as template based procedures are not interoperable enough (at least today), the decision for a certain algorithm of a certain vendor could create a monopoly which is probably not in the best interest of the EU.

Intellectual property should not prevent competition. One option for avoiding such a monopoly could be that for example the feature extraction and comparison algorithms become intellectual property of the EU provided free of charge to any licensee involved into a project of interest for the Member States. On the other hand, that approach could stifle developments in biometric technology by removing incentives to vendors to fund improvements. A second option could be to get inspiration from the crypto domain by establishing a development and competition schema supporting periodical performance evaluation of available technology and allowing suggestions on reference technologies.

For applications where only smaller numbers of comparisons have to be made (verification, identification in smaller groups), techniques using stored extracted features (template based techniques) can also be applied successfully. As said earlier, the interoperability between applications of that type might be limited as soon as algorithms from several vendors are involved.

For large scale homogeneous applications which are completely under control of one entity like, e.g., the PIV programme in the US, template based techniques might also be usable, as long as the controlling entity ensures the compatibility of the applied technology by organizational means.

It is obvious that a decision which relies on a broader data base can be more reliable. Due to that reason, the deployment of multimodal applications to increase/stabilize biometrics performance is recommended wherever possible. In the case of a border control process based on electronic passports of EU Member States, fingerprint data, facial data, and biographical data will be available.

Any acceptance decision might make use of all this data. That way, disadvantages of one biometric modality might be compensated by another one. Knowing specific biographical data of the traveller may improve the quality of the acceptance decision.

For example, if it is known that the facial image of an e-Passport is already nine years old, this could be taken into consideration. In another case, if it is known that the passport is owned by an older traveller, it may be assumed that his skin is (statistically seen) drier and his finger ridge structure less detailed that that of younger persons.

In case data bases of travel profiles could be legally assembled, such profiles could be considered to increase the validity of the acceptance decision, too.

It is known that all biometric modalities have advantages and disadvantages, and that the decision for a certain modality should always be made based on the application context. Modalities do have different properties in terms of reachable error rates, usability, intrusiveness, and dependencies from environmental conditions, required user interaction and so on. These specific properties should be considered as project specific, since generic recommendations can not be given.

Solutions that are based on biometrics still not present on current EU MRTDs like iris are already adopted by certain countries. It may become appropriate to extend the use of iris for ABC. However, even second generation EU passports can not be used, as they do not store iris images. In any case, such systems would need an additional enrolment (and a token), the scalability of which might become an issue.

It might turn out that a future generation of EU travel documents may require the storage of iris images, too. These do not necessarily need to be the e-Passports; they could also be the ID cards of the EU Member States. In any case, it is important to maintain the interoperability of the solution.

It is suggested to follow the recommendations from ICAO Doc 9303 Part 3 for designing such ID cards. If any Member State decides to have a deviating solution for his ID cards, there is a risk to end with many different (and incompatible) solutions.

Recommendations

Concentrate efforts on face and fingerprint modalities.

Anticipate iris as a potential modality for identity management in Europe.

Set up mechanisms for conformance and interoperability assurance at the template level (and not only at the image level) to avoid a monopoly. Compliance with ISO/IEC 19794-2 is only the first step on the way to a true interoperability.

Ensure compliance to European and international regulations and standards for all data storage media including travel documents.

Deploy multimodal solutions wherever affordable.

7.3. Non-Biometric Data

As far as non-biometric data as concerned, most of the additional concepts of interest in enhancing border controls lie in the capacity to initiate specific security checks including the travellers' MRTD data, his travel plans, travel payment methods and past travel history *remote* from the border to be crossed and *ahead* of the traveller's expected crossing time. Thus, further enhancements in assessing the threat level of a given passenger will include linking to the threat analysis advanced information about data contained in the various API and PNR fields (see 6.3) attached to both the travel reservation and the traveller ID. The USA has recently launched ESTA (Electronic System for Travel Authorization) [ESTA] in the USA.

In ESTA, an advance electronic application request made by citizens from Visa Waiver Countries through the Internet must be approved in order for them to visit the USA. This correlates well with similar programs already in place in Australia and New Zealand, where all non Australian (or non NZ) visitors need to obtain clearance (via an on line "e-visa" transaction) prior to actually flying "down under". On line and up to the last minute background checks, closely coupling biometric and non biometric data, are being routinely fed into sophisticated computerized decision making algorithms, the thresholds of which can be tuned according to specific intelligence-based threat situations. Practical limits to improvements brought by this coupling model include foreign States privacy limitations for PNR and API.

As this approach of coupling both biometric and non-biometric elements is key to bolster EU security, one additional way to explore is how to focus on a realistic common trunk for non-biometric data (i.e. on commonly agreed selected PNR and API fields) to ensure a sustainable performance level when this data is linked to feed queries and seek results from Schengen's SIS/VIS programs. Although it does not seem that a consensus can be found to agree on worldwide API "standards" because of the inherently different ways each nation is viewing its own security, the use of the same type of minimum (common) trunk, binding biometric data and non-biometric fields across EU-wide programs, seems quite possible and would bring EU Member States closer to aligning their major ABC processes.

Recommendations

Deploy multimodal solutions also integrating non-biometric data such as passengers' biographic data and travel history, which become an essential part of the mandatory information required by major non EU countries to pre-screen travellers before they actually depart.

Seek alignment while collecting major common non-biometric fields from PNR and API data across EU Member States to further increase security across the entire common Schengen border.

7.4. Sensors

Sensor quality has strong impact on the overall performance of a biometric system. The larger the user group to be addressed, the more heterogeneous the entire system is expected to be, and the higher the throughput of the system is intended to be, the better the quality of the deployed sensors should be.

In Automated Fingerprint Identification Systems (AFIS) which are the only large scale biometric systems with more than a decade of experience, the FBI EBTS (Electronic Biometric Transmission Specification) Appendix F has turned out to be a stable and reliable specification for the quality requirements of sensors to be used. As the functional requirements of

data to be used for border control purposes is similar to AFIS, EBTS/F might be a good starting point for specifying fingerprint sensors for e-Passport as well as e-Visa enrolment. In fact, the EU regulation for e-Passports [2252] indirectly refers to EBTS/F via ISO/IEC 19794-4.

The NIST also has published quality requirements for fingerprint sensors verifications in the FIPS PUB 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors [FIPS 201] and in the Biometric Data Specification for Personal Identity Verification [800-76]. These documents specify that enrolment devices shall comply with EBTS/F, while verification devices shall comply with slightly weaker requirements [VERI].

In fact, for truly interoperable EU-wide applications certain minimal sensor quality levels should be specified for enrolment as well as for verification applications. EBTS/F as well as the PIV specifications should be used as the initial point of such a European specification.

For facial cameras as well as for iris cameras there is no such detailed experience as with AFIS. Nevertheless, such specifications need to be prepared to ensure optimal performance of a EU-wide large scale and heterogeneous biometric installation. Considering sensors for facial and iris recognition means considering cameras. Pixel resolution values recommended for a facial as well as for an iris image are known and listed in the relevant ISO standards (ISO/IEC 19794-5 and ISO/IEC 19794-6).

As it is known that environmental (in this case: illumination) conditions have strong impact on the recognition performance of the biometric procedures, the camera properties should be discussed to define a set of requirements for face cameras as well as for iris cameras similar to those used for fingerprint scanners: Linearity, geometric accuracy, signal-to-noise ratio, dynamic range, special frequency resolution (MTF), and the ability to capture biometric sample data in appropriate size according to the application context. MTF is more than the reproduction scale; it also strongly depends on the quality of the lens system.

Another important property of a scanner is the capture speed and the time necessary for capturing data (an image in this case) from a biometric sample (finger, face, and iris).

As sensor properties usually are not easy to evaluate, requirement specifications as well as certification procedures according to these specifications should be defined.

Recommendations

Set up certification schemes for sensors to maintain a minimum application and modality-specific quality levels for face, fingerprint and (in the future) iris sensors.

7.5. Data Quality and Data Quality Assurance

Data quality depends on several factors. One of them is the sensor quality as discussed above. Others are the environmental conditions at the capturing location, usability as well as ergonomic and acceptance constraints. Additionally, all processes and workflows have to be designed accordingly, for enrolment as well as for verification/identification applications.

Such a formulation of best practices could be done based on experiences made in existing large scale applications as well as in recent pilot projects, like BIODEV II, US VISIT, etc. The experiences of the US DHS on capturing fingerprint and facial images should be evaluated in the EU. Furthermore, lessons learned by the US at the borders during the transition from capturing two index fingers to ten flat fingerprints at the US borders should be taken into account for the definition of European requirements. In particular, NIST studies on the quality requirements for ID flats [10flats] could be very valuable for several EU applications.

Data quality in its core means assurance that captured images are evaluated at time of capturing to ensure that they can be used for the intended purpose, immediately or even later on. For verification/identification purposes it is in most cases possible to ask an individual for a repeated presentation of the sample. Suboptimal quality in these cases usually only leads to decreased application speed and therefore to decreased throughput. For enrolment there is in many cases no realistic chance for data recapturing as soon as the individual has left the enrolment site.

Thus, enrolment applications have to ensure that the captured data have a quality that is sufficient for all intended applications. In large scale and long term endeavours like e-Passport or e-Visa neither all involved technological components (sensors, feature extractors, comparison algorithms, etc.) nor all potential applications can be known ten years in advance. Hence it is recommended to use only the best available technology for all enrolments.

To ensure that all deployed equipment is the best available technology, certification schemes should be developed and applied. This is extremely urgent considering the introduction of the second phase of EU electronic passports as of June 2009. Fortunately, for fingerprint devices there is a certification scheme available, which can be applied immediately (BSI TR-03104 Annex 2 (QA-Finger) V 2.1). Nevertheless, this schema probably should be reviewed and improved by the Member States in the course of time.

Experience with the first generation of European e-Passports should be used to establish a quality scheme for facial images. Looking ahead, it would be useful to develop a quality scheme for iris images, too.

On the other hand, compliance of an actually captured image with a certain quality scheme has to be determined at time of capturing. That is, quality assessment software has to be available which generates comparable results independent from the deployed scanners. Currently, several commercial image quality assessment software products are available together with a free NIST implementation [NFIQ].

To reach comparability and interoperability, the acceptance criteria should be the same for all quality assurance products. Even better, quality assessment algorithms and test procedures should be approved. From a technological point of view, the EU-wide deployment of unique software would be even more desirable to minimize technological risks. Due to political and commercial concerns, this might be impossible.

In fact, the global fingerprint capturing for the EU Visa Information System (VIS) might run into compatibility problems due to the lack of unified reasonable and applicable quality requirements.

Data quality also strongly depends on the ability of the individual to correctly present his biometric sample. That means, quality can be significantly improved by ergonomic device, application and process design, by educating the person presenting a sample, and by training the staff. When striving for low failure-to-enrol rates, the fact that for all biometric modalities there are always people who have poor quality samples should not be accepted as an excuse.

Research projects like BioP II in Germany or the Biometrics Enrolment Trial of the UKPS have demonstrated the capabilities of publicly used biometric systems. It turns out that education and training are the key success factors for any EU-wide or even global biometric system. As in very heterogeneous cultural, technological, and infrastructural environments all possible cases can never be considered in advance, the human factor gains importance to ensure optimal results.

Process designers and rollout specialists should consider the human factor: No training means suboptimal results. If the finger or the hand is not put on a fingerprint scanner in the appropriate way, high quality fingerprint images will never be captured, even with the best state-of-the-art scanner.

If an individual does not look into the camera, the facial images captured will always be suboptimal. That is, ergonomic design, user guidance, education, and training all together enable successful applications.

In spite of the extraordinary importance of data exchange format standards, these standards may only ensure that the data that is read is interpreted the right way. This does not mean that the interpreted data can be used as intended: As biometric feature extraction and comparison procedures deployed in an open system like a European ABC installation receiving international passports, it is not clear at all which specific properties of a presented biometric sample will be used for verification in detail.

That is, the higher the quality of the captured data, the higher the probability of a successful verification. As a consequence, data quality (that is, sensor quality) is indispensable for any enrolment. But it is also desirable for verification applications.

Whenever a high throughput is required and false rejection rates need to be optimized, high quality equipment even at the border control point is essential.

Recommendations

Introduce “best practice” rules for biometric data capture.

Initial efforts should be concentrated on data acquired during the enrolment stage, as non conformances and poor quality in capturing a face or finger image would severely hamper any subsequent usage of an MRTD, e-visa or other token for ID management at the border, especially during ABC operations.

If possible, ensure identical acceptance criteria for all quality assurance products.

In the future, approve quality assessment algorithms and test procedures.

An EU-wide deployment of unique quality assurance software could minimize technological risks, yet this might turn impossible because of political and commercial concerns.

The lack of unified quality requirements for fingerprint images across could cause compatibility problems for the EU Visa Information System (VIS).

7.6. Spoof Prevention and Other Security Aspects

As biometric samples could be presented using copies, records, body parts or other objects by someone pretending to be somebody else, preventive measures have to be taken. In contrast to knowledge based and possession based authentication technologies, biometric technology is bound to physical or behavioural properties of a human being.

That is, if a biometric system only captures data on features used for comparison with reference data, the system could be fooled by someone who is able to present the exact same data to the system.

Therefore a biometric system has to additionally ensure the authenticity of the captured data in an appropriate way, which might be context and application dependent. Biometrics related security aspects which should be considered to establish and maintain the trustworthiness of captured data are the following:

- **Spoof resistance.** Biometric systems could be attacked with artificial objects which can be used to present copies of the features used for differentiating people. Such objects obviously are modality and even sensor and application dependent. For fingerprints it is possible to produce membranes to put on the fingertips made of wood glue, gelatine, latex and other transparent and not transparent materials which can generate imprints being very close to the original. Thin membranes are probably difficult to detect by untrained staff. In unattended ABC systems, a visual examination of the fingertips might be impossible. That means, such fakes have to be detected otherwise. Cadaver fingers are not a likely problem for supervised enrolment application, but might be one for unstaffed environments. Similar problems might occur for facial and iris recognition with printed images, printed contact lenses, masks, or video sequences. Even completely artificial objects like artificial fingers, hands, heads, and eyes are imaginable. For a specific application, one needs to determine which spoof threats are possible, which ones are relevant, and what countermeasures can be taken to address them. Such a risk assessment has to be performed repeatedly, as it may be assumed that fakes evolve as soon as biometric applications get more common. It might be necessary to maintain an EU-wide list of known threats to allow immediate responses, applying a standardized definition of threats. This list should describe the threat, its importance for specific applications, and assess its relevance. Similar to virus scanners, information on relevant new threats should be provided to the industry by a trusted body to enable the quick development of countermeasures.

- **Aliveness check.** It is possible that attackers presenting biometric samples with spoofs as described before try to overcome biometric systems presenting cut-off body parts. Therefore, ensuring that a fingerprint is captured from a true human finger is not sufficient. One needs to also verify that this finger belongs to a living person. This task differs from the spoof prevention one: if a fingerprint scanner verifies a living finger but does not detect the thin membrane on the fingertip, the protection fails. As above, the relevance of such attempts will be application specific, and should be discussed in a threat and risk analysis.
- **Replay resistance.** The biometric installation has to ensure that the replay of samples recorded before is made more difficult or, better, prevented altogether. In case of the modalities considered here, this could be done for example by detection of latent images or watermarking of captured images. Such watermarks could contain date and time, or even the location where the image has been captured.
- **Skimming and eavesdropping resistance.** A possible threat to a biometric system is skimming of the sample data captured from the users, e.g., by sniffing from cables or an RFID interface. This could be made complicated or prevented by encryption of transmitted data between sensors and the processing components and/or by appropriately shielding the connections. Eavesdropping could also be addressed by data encryption as well as by device specific data signature. It is worth noting that a similar robustness has to be developed for all other peripherals of the local inspection station PC, since, for example, unencrypted data is eventually generated to load the officer's PC display with visible sensitive information.
- **Data authenticity verification.** Biometric data stored in electronic passports and other electronic ID documents is usually digitally signed. It is essential for any system that relies on these data that said signature is verified. All applicable ICAO protocols should be performed. At least it should be always required to perform Passive Authentication (PA) completely to prevent "successfully faked passports" as they have been regularly reported in the press.
- **Minimal security level.** It should be ensured that any biometric system deployed in the EU reaches a minimal security level (to be specified). One option to reach this goal would be to harmonize the process design which would also improve the citizen user perception.
- **Standards equivalence.** All EU entry point should have a unique minimum security standard.
- **Unstaffed gates.** Fake resistance is a major issue, especially for unstaffed ABC installations. Therefore the industry should be encouraged to develop fake resistant technology, especially for that purpose. The efficiency of such technology has to be evaluated according to standardized application specific criteria. These criteria should be developed by the EU Member States and become mandatory for all biometric installations which apply biometric technology. At present, all running ABC projects in Europe do maintain close control, say by remote CCTV of the operations at unmanned stations, so that a machine "accept" decision can always been reversed and a secondary check initiated by the remote controlling officer.
- **Facilitation versus security:** Biometric technology may contribute to security. However, if data formats, data quality and recognition performance of biometric systems deployed are not aligned between Member States, this might generate a major security risk with unpredictable consequences. Some countries might decide to increase the throughput of travellers by tuning their systems towards low false rejection rates and accepting higher false acceptance rates, while others may want to promote security aspects at the expense of passenger throughput by controlling false acceptance rates prevention of sensor spoofing, thereby accepting a higher number of false rejections. Further agreements between Member states to limit the range of variation between both parameters may thus be needed to prevent ill-intentioned travellers to flock into Schengen through notoriously porous inspection points.

Recommendations

Evaluate the biometric performance of the algorithms to be used, the spoof resistance of a sensor, and the deployment characteristics separately for every application.

Develop recommendations on standard FAR and FRR values for specific cross border applications and other security relevant application types across Member States.

7.7. Interfaces and Data Exchange Formats

Within the last few years, data exchange formats have been developed in the ISO/IEC 19494 standards family for almost all biometric modalities. All large scale applications that are intended to run for a longer period of time, as it is the case for passport and visa applications, should be mandated to require the formats defined therein: 19794-4 for fingerprint images, 19794-5 for facial images, and 19794-6 for iris images.

If it is additionally desired to store fingerprint minutia templates, 19794-2 should be applied. Deviations from these standards and proprietary data formats should not be accepted. Tests for compliance to the 19794 standards are provided in ISO/IEC 29109-x.

Another family of standards which improve interoperability is CBEFF (Common Biometric Exchange Formats Framework), which is defined in ISO/IEC 19785-x.

A third standard which has a rapidly growing importance in the context of heterogeneous and long term systems like ABC, passport, and visa applications, is BioAPI (ISO/IEC 19784-x). ISO/IEC 19794-x ensures that the biometric sample data is coded in an interoperability conserving way, BioAPI supports seamless interaction between components, hardware as well as software, from different vendors.

Even if it might be an advantage to use vendor specific interfaces that are fine tuned to the specific strengths of the vendor technology, the importance of interoperability necessitates a standardized approach. This does not mean that the required functionality should be lowered: The EU is a market that is important enough to challenge its local industry accordingly. Research guidance and financial support might be appropriate.

For fingerprint applications that include a certain workflow as it appears in tenprint applications, ISO is preparing the Tenprint BioAPI standard ISO/IEC 29141. This standard should always be taken into account as soon as several fingers are to be captured. It might be useful even for e-Passport enrolment applications where by default the two index fingers are captured.

If the process as recommended includes quality assessment of the captured prints and appropriate steps to capture other or additional fingers if necessary, ISO/IEC 29141 should be applied. For visa enrolments, the Tenprint BioAPI is indeed one of the applications the authors had in mind when they wrote this standard.

ABC applications which probably involve several workflows depending on the type of traveller (EU citizen, visa based traveller, visa waived traveller, etc.) should also consider ISO/IEC 29141.

To ensure especially the interoperability of ABC schemes, it is necessary that any ABC system deployed in an EU Member State can interact with the ABC system of any other Member State. The various ABC systems deployed in the EU should be interoperable as most as possible. An optimal solution would allow a person to enrol on one system and to verify on another. In a possible implementation of this principle biometric data from one system could be shared with other systems.

In any case, biometric data interchange standards should be compliant across the EU. It is recommended to apply ISO standards like CBEFF (ISO/IEC 19785-x), Biometric Data Interchange Formats (ISO/IEC 19794-x), especially Part 4 (Finger Image Data) and Part 5 (Face Image Data). This requirement is essential for all enrolment processes (passport application, visa application, airline check-in, etc.). For verification/identification processes the deployed applications must rely on data that complies with the applicable standards.

Recommendations

Ensure that any ABC system deployed in any EU Member State can interact with any other ABC system within the EU.

Favour leadership of the EU industry when publishing requirements through research programmes and provide appropriate financial support.

Where possible, adopt appropriate international biometric data interchange standards across the EU, including standards like CBEFF (ISO/IEC 19785-x), Biometric Data Interchange Formats (ISO/IEC 19794-x), especially Part 4 (Finger Image Data), Part 5 (Face Image Data), and, in the future, Part 6 (Iris Image data).

7.8. Scalability and Fallback Solutions

Scalability is a major objective for EU-wide interoperable biometric solutions. The lack of scalability can cause the failure of an entire biometrics based programme. Scalability considerations should look into several aspects:

- **Technical level.** The solution or the combined solutions that shall interact should be able to rely on data bases of sufficient size and speed. Furthermore, the distribution of certificates and encryption keys must be organized, so that all these credentials are present at all necessary places in time. For example, the inspection of electronic passports mandates performing Passive Authentication (PA) on these passports. PA evaluates the trust chain to certificates that are proven to be trustworthy, the so called Country Signer Certificates (CSC). These certificates must be available at all points of inspection. Otherwise any process based on data read from a passport would not be reliable, including for example biometric ABC. A minimal requirement should be the distribution of the CSC of the EU Member States. To allow biometrics based inspection of non-EU passport holders, all CSC from all countries issuing e-Passports that shall be inspected have to be available. For EU passports with Extended Access Control (EAC) the necessary certificates required for Terminal Authentication as well as for Chip Authentication also have to be available at the point of inspection. As these certificates usually will have a shorter validity period, the logistical task is probably more challenging than in the PA case. On the other hand, most countries issuing EAC passports are EU Member States. This will alleviate the task to provide all necessary certificates on time.
- **Level of political acceptance.** Interoperable solutions always imply common requirements understanding and implementation. It may be expected that passport and visa based applications will be very heterogeneous as the Member States will deploy solutions from different vendors, especially over the course of time. Many solutions will run under national authority, and interoperability will be maintained via links between the Member States or to EU central services. But these links are in most cases more on a “top level” of the system. That way, minor incompatibilities between the solutions of the Member States are hidden and lose importance. On the other hand, there are applications that suggest cooperation even at local level. If for example in certain countries several EU Member States decide to share a visa enrolment centre due to economical or other considerations, this centre must be able to fit all involved national schemes. To develop such EU enrolment centres, a common prior understanding of enrolment technology, enrolment processes, enrolment workflows and enrolment policies must be reached.
- **International recognition.** As many other regions are faced with the same or similar problems as Europe organizing interoperable solutions, especially for border control purposes, European solutions might find a strong recognition throughout the entire world, especially in Asia Pacific, Middle East, or the Americas. Many of these countries probably would like to reuse the experiences made in Europe developing and deploying well performing biometric solutions. Such recognition also would have positive effects for the involved European industry.

- **Biometrics.** Different biometric modalities, different sensor technology and different algorithms have different discrimination powers which impact usability with respect to the size of the population to be addressed. The applicability of a certain technology also depends on the intended use: Should the system be used in identification or in verification mode? This has to be analyzed very carefully by statistical studies, considering the special application context including sensors, algorithms, and workflows, to avoid security breaches. It gets even more important if enrolment data must be shared between applications. For example, a single fingerprint associated with a token such as a frequent traveller card is sufficient to perform (and secure) paperless "biometric boarding", yet it may fail in the absence of an appropriate accompanying token. On the other hand, the same single fingerprint could be sufficient for an ABC if combined with facial image verification and an e-Passport.
- **Time.** Biometric data ages. The longer the time between enrolment and actual authentication, the higher the probability of false rejections will be. Research is necessary to determine the exact amount of this degradation. It is recommended to initialize such a research project as soon as possible to be able to address the outcome accordingly. On the other hand, for biometric data stored in e-Passports, eID cards, and e-Visa databases the exact time of capturing is known. Hence comparison algorithms could and should take this knowledge into account. Furthermore, if a degradation of the recognition rates is observed for frequent users of a biometric system over time, an estimate can be made on how long it will take until the currently used document gets unusable.
- **Deployment.** As EU-wide interoperable solutions may grow up to huge and widely distributed installations, it is essential that the system design considers growth aspects appropriately. This should include the equipment to be used (e.g. technology providers' knowhow and staying power), the intended throughput (e.g. locally at a certain ABC gate, or system-wide), or the need for propagating certificate revocations. For border control applications, temporary revocations of the Schengen Treaty might even be considered, for example during major sports events or the yearly Davos world summit meeting. The border control infrastructure should be able to address such temporary changes without losing its general performance capabilities.
- **Public versus private.** On the short run isolated solutions for ABC will grow up in number all over Europe. Some of these solutions may be private Registered Traveller programmes; other would be public Registered Traveller programmes, while other may rely on data read from e-Passports. Whether public or private, non-passport based programmes might run into scalability problems by design due to limitations of the chosen biometrics technology. Non-passport based programmes are potentially competing against each other, and may be hit by the lack of willingness of participants to enrol into several schemes separately (and to carry several tokens). It is likely that the need for repeated enrolments will be the major scalability limit for non-passport based solutions whenever several of these schemas would have to coexist or if the user base becomes too large.
- **Backwards compatibility.** Any large scale solution should be backwards compatible. As MRTD have long validity periods of up to ten years, any change of the underlying functional principles which would lead to incompatibilities with the existing technological basis should have a strong justification. This also means that as biometric infrastructures are being introduced within Europe for the first time, future demands should be considered even today as early as possible.
- **Fallback solutions.** Biometric systems are based on probabilistic properties of human beings. A certain percentage of the population will not be able to participate in programmes that are based on a given biometric modality, either due to temporal conditions like injuries or sicknesses, or due to permanent anomalies like missing, lost body parts or other disabilities. This population won't be able to provide a biometric sample to the

scanner. Workflows must also consider the specific needs of these persons and fallback solutions should be provided.

- **Budget constraints.** Different processes, especially different ABC processes might require different equipment. That is, for travellers with a visa, ten flat fingerprints can be used for verification, allowing very reliable and fast processes due to the larger amount of data usable for comparison. People travelling on an e-Passport across an ABC system may only need to use two flat fingerprints, requiring simpler equipment. Such simpler scanners would require more complicated processes for visa travellers, and, therefore, decrease the global throughput of a common ABC system. As a consequence, different equipment for ABC gates would be required for different purposes, aiming an optimal throughput. Since a comprehensive deployment would necessitate excessive capital expenditure, a compromise would need to be found that would balance costs, throughput, the origin and destination passenger traffic (O&D), as well as available space and supervising manpower. With respect to data quality, however, no compromise should be made, since a common EU level to enable control over the (false acceptance) risk criteria is the only acceptable base for future interoperability. In short, even if budget constraints might impact scalability, this should not be under conditions which would affect interoperability which should remain the preferred channel to focus on.
- **Interoperability constraints:** In many of the existing ABC schemes, proprietary tokens like smart cards are used by a passenger to claim his identity, and to verify this claimed identity against the enrolled data. The scalability of these schemes may be affected by the willingness of member travellers to enrol into several schemes, especially against a membership fee for some of them. From the operator standpoint, scalability also might causes problems like bi-national and international extension as well as revocation. The only truly interoperable and fully scalable token based ABC programmes so far are those which are based on electronic passports and Doc 9303 compliant electronic ID cards.

Recommendations

Maintain a stable balance between security, throughput, and usability related requirements with respect to sensors, algorithms, and workflows to avoid security breaches.

Maintain scalability with respect to biometric discrimination power, and overall system performance. Fallback systems and backwards compatibility have to be in place to deal with people who do not possess the required biometrically enabled travel documents or whose biometric characteristics cannot be successfully verified.

7.9. Reliability, Robustness, Maintainability and Safeguarding

All large scale applications require special emphasis on quality assurance measures in operations mode. The quality of biometric data is in most cases not obvious. How does one know for example that a lens system of a camera is set up properly? How does one know when and if a fingerprint scanner has to be cleaned? How does one know if the biometric samples are presented properly?

Hence, it is particularly important that the biometric components of a large scale and distributed biometric solution have specific capabilities which allow an automated quality assurance with respect to:

- **Quality of the captured biometric data.** At capture time, the biometric samples need to be presented in the intended or at least in a tolerable manner. Examples include looking straight into the camera, not smiling, not closing eyes nor wearing sunglasses or hats, and laying the finger(s) flat on the scanner prism surface.
- **Sensor quality.** The scanning devices need to be kept clean, adjusted, and calibrated if necessary. Cleaning might require human interaction, so the system must be able to notify the operator whenever cleaning is necessary.
- **Reference data quality.** In large scale applications like ABC based on electronic passports the reference data used for comparison is read from a token provided by the travel-

ler, namely, his electronic passport. It is not known in advance how good the stored facial, fingerprint, or iris images read from that passport are with respect to the applied feature extraction and comparison algorithms.

As the applied biometric sensors are usually distributed in the field, any hands-on inspection of the system would be expensive, especially as biometric devices are often not off-the-shelf products which can be maintained by every service engineer. Therefore maintenance of the devices has to include in-field calibration capabilities of the scanning devices. Any biometric scanning device should have a service mode that can be accessed (preferably) remotely. Such access should be standardized to ensure easy adaptation to different devices, and security certified to prevent security breaches via the service channels.

Any biometric technology should be maintainable through the entire EU. Therefore adequate standardized Service Level Agreements (SLAs) should be applicable to any biometrics technology purchase. These SLAs would need to contain at least local/regional maintenance commitments from technology suppliers as well as from system integrators. It may be assumed that EU based companies will be able to fulfil maintenance requirements, e.g., on response times, better than companies not having close and reliable technology support teams in the EU.

It is recommended to examine a dual source strategy with respect to hardware provision, especially considering biometric sensors.

A highly interoperable and highly reliable large scale biometric application will be new to all participants in such a project. Therefore, all statements made by technology providers or system integrators which are dealing with reliability and maintainability issues should be verified during one or several pilot projects. It may be assumed that several adaptations will be necessary, considering the used products, workflows, design decisions, etc. Moreover, the level of commitment of all pilot project participants should be assessed, and supplier selection should be made based on observations during the pilots.

For mobile inspection purposes, mobile or at least portable equipment will be necessary. Mobile technology will have different requirements compared with the stationary one. In addition to biometric performance properties, mobile scanners should be sufficiently ruggedized. Other important criteria to be involved in future common specifications should include autonomous power supply and hot swap capabilities, weight, size, outdoor usability and system connectivity.

Under special circumstances the Schengen Treaty will be suspended for a period of time, e.g., during special sports events like world championships. Such a suspension will have to be supported by providing ad hoc border control stations, which shall operate during a certain period and then will be stored until needed next time. Ad hoc deployment, specific ergonomics and workflow requirements as well as storage requirements have to be considered. It might be useful to use prior experience made with so called “jump kits” that are already in use by military forces.

A possible method to achieve the reliability and serviceability goals might be to support prevalence of EU made products and solutions. An adequate market share for EU products and technologies, especially, but not only within the EU, should be maintained and supported.

Prevalence of products and services “Made in EU” does not only support the industry of the Member States, but also allows the EU to take influence on the offered products, for example by goal-oriented promotion and sponsorship of research and development.

Recommendations

Ensure that the biometric components of all large scale and distributed biometric solutions have capabilities for automated quality assurance with respect to quality of the captured biometric data, sensor quality, and reference data quality.

Include EU-centric and EU-specific criteria in SLAs to favour local maintenance.

7.10. Environmental Conditions

The performance of biometric technology is often influenced by environmental conditions. As an example, performance of facial recognition systems strongly depends on illumination. But fingerprint scanners as well as iris recognition cameras can also be disturbed by sunlight or spotlights.

As it may happen that border control gates are deployed at places in direct sunlight, this factor has to be considered while developing the overall solution, especially in the system and workflow design. Sensor technology which is more robust to ambient light should be preferred.

Many biometric modalities are not only dependent on illumination, but also on temperature and moisture. Cold fingers will worsen fingerprint images, as will dry fingers, especially after a long distance flight.

Such conditions which may have influence on real life equipment performance should also be considered in a pilot project, as lab experiences do not adequately mimic real life.

Whenever biometric technology is used outdoors, in addition to the changing conditions for capturing biometric data, modified requirements to the devices themselves should also be considered.

The devices probably need to be ruggedized; they should be water protected and climate proof. This might include for example heating for the prisms of optical fingerprint scanners or anti-steaming measures for cameras.

Recommendations

Evaluate the performance of a solution under realistic environmental conditions.

7.11. Privacy and Data Protection

Privacy and data protection requirements have to be considered according to the legal situation in the EU as well as in the EU Member States which might differ from State to State. In addition to the necessary compliance with requirements defined by laws, it is a common sense experience that respecting privacy demands of the citizens by a technical system regularly leads to higher acceptance of that system in the real life.

Moreover, it is also common sense experience that higher acceptance leads to higher willingness to participate and, at the end of the day, to higher performance rates and higher throughput. In fact, compliance to data protection regulations is not only a legal requirement, but also one with high technical relevance.

ISO has published a technical report (ISO/IEC TR 24714-1) on the cross-jurisdictional and societal aspects of implementation of biometric technologies. This report should be used as a basis for defining an EU specification for security sensitive interoperable solutions between the Member States which involve biometric technology. The ISO report lists the most important principles which should be maintained:

- Transparency and access rights of the data subject,
- Consent and limitation of purpose,
- Preference for opt-in and limitation of collection as well as of period of retention,
- Adherence to performance criteria,
- Data protection, secure audit, and responsible data transfer between different jurisdictions,
- Information on automated decisions,
- Accountability,
- Appropriate accuracy of biometric data, which should be kept anonymous whenever possible.

To promote public acceptance and to ensure compliance of biometric installations with privacy and data protection laws within each EU Member State, it is recommended to develop guidelines for privacy-friendly systems which could be certified by the data protection authorities of the Member States. These data protection authorities should always participate in the teams involved in the development of conformance projects, tools and infrastructures.

Adhesion to common privacy rules and standards all over Europe would bolster acceptance of biometric systems in the EU, and might find recognition even outside Europe. Hence, European technology implementing these values would also be able to globally support freedom and respect for civil rights and benefit from its economical market returns.

Recommendations

Develop guidelines for privacy-friendly systems which could be certified by the data protection authorities of the Member States.

Involve data protection authorities as soon as possible and use any positive feedback as potential leverage to increase European supplier recognition outside the EU.

7.12. Accessibility

In order to ensure a maximal performance of a biometric system, accessibility should be one of the major design goals. Legal requirements forbid discriminating people with inabilities. Furthermore, to ensure a seamless process flow in applications with high throughput requirements, it is necessary to process as many people as possible using the same workflow. Principles for the design of biometric systems are collected in the ISO technical report ISO/IEC TR 24714-1. These principles are a good basis for designing well accessible systems.

Many of the principles listed in the above mentioned report try to make applications as easily understandable as possible. Respecting this ease of use requirement will not only help making biometric systems more accessible and avoiding discomfort; it will also ensure that less experienced people get better guidance using these systems. It may, therefore, be assumed that accessible systems will have better performance in terms of error rates and throughput.

Main design goals for accessible systems should be the following:

- Flexible, simple and intuitive usage, easy to understand handling with clearly understandable prompts, supported by clearly indicated signs, using a range of tactile, audio and video interfaces,
- Error tolerant use, no need for high physical efforts, size adjustable equipment,
- Prevent disadvantaging persons with disabilities by designing devices that can be used by as many people as possible, and which, by design, fulfil the needs of disabled people (e.g. ADA compliance).

Disabled travellers might need extra training on the use of biometric systems. Thus, operating staff has to be trained on how to work with disabled people, too. Furthermore, tests covering the specific needs of disabled people should already be performed during the specification phase of a system. Alternative workflows should be provided too, ensuring that nobody is excluded from using a certain system because of his or her disability. Last but not least, there is no doubt that privacy and data protection requirements are the same for all EU citizens, disabled or not. This means that details on the disabilities of a certain person may only be stored (which sometimes might be necessary) after his written and informed consent.

Recommendations

Cover the specific needs of disabled people in all relevant system specifications.

Define specific accessibility requirements and design a test guideline.

Provide alternative workflows ensuring that nobody is excluded from using a certain system because of his or her disability.

7.13. Health, Societal, Cultural and Ethnical Aspects

Even though biometric technology is not new (fingerprints have been used for criminal investigations since more than 100 years), there might be fear in the public that biometric sensors might behave problematically with respect to health and safety. Such fears could lead to some users being unwilling to present their biometric characteristics to the respective scanners. Such behaviour might cause delays in processes, lead to worse quality of the presented data, even induce the refusal to use a certain system.

All required safety certifications must be provided by manufacturers of the equipment to be deployed. Moreover, educational advertising might be helpful to proactively prevent or eliminate fears.

It may be assumed that as soon as biometric technology gets increasingly common in the citizens' everyday life, such fears and concerns will gradually disappear. In this sense, governmental driven programmes are the enabler of the entire biometric industry to introduce civil (i.e., non criminal AFIS and non governmental) solutions to the general public. Such familiarity and acceptance will lead to better performance of solutions such as Automated Border Control (ABC).

Nevertheless, there might be some real health problems which do not relate to the physical principle of the biometric capturing device itself, but to some side effects. For example the prism surface of a fingerprint scanner used for border control purposes might be contaminated by germs, and therefore physical contact might lead to infections. A possible solution would be to clean the sensor between uses.

Physical principles that are used for capturing biometric sample data like illumination in several wavelengths must be addressed as well, e.g., the detrimental effect of UV light. In general, any physical exposure should be covered by standard safety certifications, especially if repeated or continuous.

Another health related aspect considers data protection issues. Only the absolutely necessary biometric data sample needs to be collected, and no health condition should be disclosed during a biometric process, neither directly nor indirectly (through additional processing or analysis).

Following the last decades of migration in Europe, the cultural diversity of many EU Member States has increased. Furthermore, systems in place at the borders of EU Member States are used by travellers coming virtually from any possible country in the world. As a consequence, the multiple cultural travellers' background from within and outside Europe should be considered and the workflows designed should respect different cultures, ethics and traditions.

Several health, societal, cultural, and ethnical aspects as well as best practice experiences are discussed in the ISO technical report ISO/IEC TR 24714-1.

Recommendations

Review and implement requirements of ISO/IEC TR 24714-1 in EU biometric systems.

7.14. Usability, Ergonomics, and User Acceptance

Usability and ergonomics are key factors for the optimal performance of a biometric system, as they lead directly to better data quality and recognition results, and indirectly to better user acceptance, resulting in increased performance.

Several aspects related to usability, ergonomics, and user acceptance are discussed in the ISO technical report ISO/IEC TR 24714-1. Those aspects include the context of use, climatic conditions, possible contaminations of the devices and other parts of the system, indoor/outdoor use, public/private areas, location/position related questions, throughput assumptions, information and education, or support topics. Privacy and data protection, convenience, reliability, performance, the legal context, invasiveness, and consideration of the cultural background have strong influence on user acceptance, too.

It is commonly agreed that user perception has strong influence on acceptance. Thus, the users of a biometric system must see a clear benefit in using the system to accept it and, eventually, endorse it. It is therefore essential for the designers of an EU-wide biometric system to convince the citizens that they have a tangible advantage in using these systems, both individually and for the entire EU.

Vice versa, biometric installations like ABC systems have a certain responsibility: If they fail to substantiate their perceived value along the road, this would definitively be a setback for the entire European biometrics industry.

Acceptance can be tested in advance within pilot projects. Such pilots should be used in any case for tailoring processes and workflows as well as defining the technology to be deployed before rolling out the final system.

It should be a main goal of any European biometrics initiative to strive for acceptance by the EU citizen users. Any biometrics technical system can only perform well if it is recognized and accepted by the citizens. This acceptance goal could be supported by a harmonized process design throughout Europe. Such a harmonized design will not only enable a consistent minimal security level. It will also generate a unique perception by the citizen; and that again will increase the throughput of the biometric systems deployed.

Recommendations

Review and implement requirements of ISO/IEC TR 24714-1 in EU systems.

Inform and seek citizens' approval based on practical experiences, advantages and perceived value.

7.15. Applications and Reference Implementations

The development of electronic passports has shown that the presence of a reference implementation may accelerate the development and the introduction of a new technology. Since the Golden Reader Tool (GRT) [GRT] was made available, all parties involved in the development of the system "e-Passport", both on the document and on the reader manufacturer sides, have taken advantage of referring to the GRT.

Even if the GRT was never meant to be "the" reference tool, it is now accepted de facto as such. For the biometric components of EU-wide border control systems, the complexity is at least similar to that of the RFID part. Thus, it may be assumed that the existence of a reference implementation that demonstrates the basic functionality and illustrates the requirements of a specific application will be helpful in speeding up development.

The GRT has been developed on request of a governmental authority (the German BSI) and has been provided to all interested parties. Here, a similar approach could be used: Seek public funding for a reference application that covers aspects which turn out to be most difficult to assess by technology vendors alone.

Reference implementations must always be application specific; thus, specific reference applications should be defined before any implementation can be developed.

Typical reference applications could include:

- Staffed border control booth,
- ABC gate,
- Biometric Airline check-in kiosk,
- Biometric boarding gate for self-boarding (including ID verification).

The rapid development of e-Passport technology for EU passports, especially all kinds of communication protocols like Basic Access Control (BAC) and Extended Access Control (EAC) has only be possible due to the strong commitment of the Brussels Interoperability Group (BIG).

BIG, supported by the Joined Research Centre of the EU Commission (EC JRC), in particular by the Institute for the Protection and Security of the Citizen and its Sensors, Radartechnologies and Cybersecurity unit, played a major role coordinating the efforts of EU Member

States maturing the RFID and cryptographic technology eventually deployed. This research and coordination infrastructure could be reused for the purpose of reaching biometrics interoperability. It would enhance the power of a successor to the BIG to look for cooperation with the industry, even earlier in the time scale than BIG ever did.

Even if prior coordination between the Member States governments is essential for the success of any multilateral project, and even if many technological components still have to be developed or optimized, the European biometric industry should be involved as early as possible.

References should be available for a certain number of application cases or profiles. The requirements analysis of all biometric applications should consider among other conditions:

- The guidance and supervision properties. An application can be:
    - **Attended:** An application is attended if a traveller is guided by a trained officer. Such an officer understands the main background of the application and is especially able to detect threats, for example attacks with fingerprint spoofs. A staffed border control booth is an example for an attended application.
    - **Semi-attended:** An application is semi-attended if there is staff present which may give some guidance to a traveller, but this staff has no training on the background of the system nor can he detect threats appropriately. An e-Passport enrolment application in a passport office of a municipality would be an example for that type of application.
    - **Unattended:** Unattended applications have no staff present or at most a supervisor inspecting a certain number of those applications remotely, for example via video cameras and/or computer monitors. An example for an application of that type is an ABC kiosk or gate.
- The authentication mode. An application can be used for:
    - **Enrolment:** An enrolment application shall take care of getting the best possible data quality and shall ensure the authenticity of the captured data. Data quality is the most important feature of such applications.
    - **1:1 Verification:** This type of application does not necessarily need the highest available biometric data quality captured at verification time, at least not because of (algorithmic) biometric recognition requirements. Throughput might be more important, for example in ABC gates.
    - **1:some Identification:** This type of application is used for example for black list search. Another application case might be biometric boarding of an aircraft: The number of passengers is comparatively small and forms a flight specific data base. As long as all travelling passengers can be mapped into the passenger list (the so called flight manifest), an application of that kind performs well enough. It may be expected that many 1:some identification solutions will need to have very high throughput to sustain the intended application workflows.
    - **1:many Identification:** This type of application will probably be used mostly for detecting multiple entries in large databases. Here, throughput will not be the most important requirement, especially when compared with data quality.

All these different types of applications have specific requirements. These requirements should be addressed in a more detailed list of profiles to be prepared in the future. A partner who is also interested in analyzing application specific requirements especially for air travel related processes is IATA's SPTIG (see 6.4).

Successful national implementations should be expanded to the entire European Union. Application specific requirement specifications already being proven to be useful and applicable should be used as a basis and reference for any project with a similar application focus.

Recommendations

Specify and where necessary develop appropriate profiles covering application characteristics for typical border control processes.

7.16. Certification Schemes and Certification Centres

To ensure conformance and interoperability of applications requiring European cross-border operation, a European certification scheme should be considered. Certifications for compliance to privacy and data protection principles are a desirable goal. As an initial step, recognition of compliance by data protection officers of EU Member State governments as well as by non-governmental organizations dealing with data protection and consumer protection should be obtained. This would already improve the acceptance of biometric technology. Better acceptance will lead to more user cooperation, which in turn will lead to better performance of biometric systems.

The next stage of work could address how such a certification scheme would be established across Europe. The commercial viability of such a scheme should be considered, as well as the need for state funding. Consideration would also have to be given as to how to validate certification bodies across European borders: Who certifies the certifiers?

One should take into account the fact that any certification consumes significant resources; therefore any certification scheme requirements will have impact on prices. Thus, the EU should on one hand try to harmonize European schemes internationally, while, on the other hand, balancing financial, logistical and research support which might all be appropriate to reach the required results as quickly as possible. An existing certification scheme which could be used as a blueprint for the scheme to be developed is the Common Criteria (CC) [CC]. Many European organizations have comprehensive experiences on CC evaluation and certification: Their know-how should be re-used. Another established reference in the field of testing and certification are the ISO SC37 standards 19795-4 (Biometric Performance Testing and Reporting – Interoperability performance testing) and 29120-1 (Machine readable test data for biometric testing and reporting).

The creation of EU Certification Centres might be one possible development. Alternatively, a network of national Certification Centres of the EU Member States approved by the EU could be established. These centres could develop application specific profiles and give guidance to Member States. Early discussion of technical requirements can also be initialized there. These centres could be made responsible for the generation of compliance verification procedures. The EU could establish certification programmes whenever appropriate and necessary.

It might also be useful to set up a certification procedure for biometrics standards which could apply to all EU's travelling citizens. As this appears to be a long term goal project, it is suggested in the meantime to establish and maintain an EU registry for biometric standards to be applied in all border control related projects.

A certification procedure should be set up for laboratories that are allowed to evaluate the performance of biometric technology and biometric systems. The main focus should be on the quality assurance of facial, fingerprint and iris modalities which are the main modalities in ICAO Doc 9303 compliant travel documents. Compliance with ISO/IEC 19794-4, 19794-5, 19794-6, 19795-x, and 29109-x standards should always be maintained.

Recommendations

Set up a certification procedure for accredited laboratories to evaluate the performance of biometric technology and biometric systems.

Put the main focus on quality assurance of facial and fingerprint modalities as main modalities in ICAO Doc 9303 compliant travel documents in accordance with ISO/IEC 19794-4, 19794-5, 19794-6, 19795-x, and 29109-x standards.

Create EU certification centres, which would rely mostly on agreed biometrics related ISO standards. Build up EU specific application profiles. Develop aligned verification scenarios for equipment, applications, and infrastructure compliance, while providing overall guidance to Member States.

8. Conclusion

Biometrically enhanced identification is a valid way to improve security, both on national and European level, as it will facilitate the extended usage of eMRTDs, eID and other electronic tokens, and provide the required infrastructure to develop automated procedures beyond the present Schengen IT infrastructure.

However, the deployment of biometric systems intended to serve EU Member State border control needs may fail because of several reasons. These are mostly related to the current lack of harmonization and standards. The quality of stored data at time of enrolment is not guaranteed. It is still necessary to provide rules to develop a scalable and interoperable framework the Member States could use for determining minimal operational and quality requirements.

Another area in which EU Member States need to cooperate closely is the appropriate way to improve the perceived value of gathering and utilizing biometric data to bolster collective security, while unequivocally complying with stringent privacy and data protection schemes for each and every single EU citizen.

Involving all stakeholders, both public and private, and enticing them to strive for the creation of competent EU certification centres which would leverage on existing ISO standards and provide application-specific testing and compliance scenarios for biometric applications is an essential step in maintaining EU-specific solutions and achieving dominance of the EU in present and future biometric technology.

Summing it all up in a few bullets paving the way to future in-depth study:

- Biometric technology improves security if consistently applied across all processes.
- Continue involving the European biometrics community as early as possible.
- EU academic and industrial expertise is available and should be used.
- Rely on available ISO standards in setting up certification centres.
- Strive at enhancing perceived public value of biometrics.
- Challenge, yet support the European industry.
- Rely on standards whenever possible.

References

In this Section, Standards that have been referred to in earlier Sections are not mentioned again. Here, only relevant documents together with a way to access them are listed.

[1030] COUNCIL REGULATION (EC) No 1030/2002 of 13 June 2002 laying down a uniform format for residence permits for third-country nationals. Official Journal of the European Communities L 157, 15.6.2002, pages 1-7.

[10flats] Elham Tabassi. Quality Directed Processing of Slap Fingerprints. Biometrics Consortium Conference 2008. http://biometrics.org/bc2008/presentations/124.pdf

[11638] 11638/03. Thessaloniki European Council 19 and 20 June 2003. Presidency Conclusions. 1 October 2003.

[1683] Council Regulation (EC) No 1683/95 of 29 May 1995 laying down a uniform format for visas. Official Journal L 164, 14/07/1995 P. 0001 – 0004.

[2252] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L 385, 29/12/2004 P. 0001 – 0006.

[228] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs). 2.5.2007. COM(2007) 228 final.

[2725] 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. http://europa.eu/scadplus/leg/en/lvb/l33081.htm

[2909] Commission Decision C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States. (No official English version available.)

[409] Commission Decision C(2005) 409 of 28 February 2005 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States. (No official English version available.)

[46] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050.

[512] 2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS). Official Journal L 213, 15/06/2004 P. 0005 – 0007.

[73] European Parliament legislative resolution on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 — C5-0101/2004 — 2004/0039(CNS)).Official Journal 208 E, 25/08/2005 P. 0050 – 0054.

[EUBD] EUROPEAN DATA PROTECTION SUPERVISOR Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (2008/C 200/01) http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-03-26_Biometrics_passports_EN.pdf

[WP4] GUIDE FOR ASSESSING SECURITY STANDARDS FOR HANDLING AND ISSUANCE OF TRAVEL DOCUMENTS, Montréal, 5 to 8 May 2008. http://www.icao.int/icao/en/atb/Meetings/2008/TagMrtd18/TagMrtd18_wp04.pdf

[Hist] MACHINE READABLE TRAVEL DOCUMENTS (MRTDs): HISTORY, INTER-OPERABILITY, AND IMPLEMENTATION. Version: Release 1. Status: Draft 1.4. March 23, 2007. http://www2.icao.int/en/MRTD/Downloads/Technical%20Report/ICAO_MRTD_History_of_Interoperability.pdf

[HST] Bill Would Mandate Airport Worker Biometric Study. HS Today, Friday, 09 May 2008. http://www.hstoday.us/index.php?option=com_content&task=view&id=3278&Itemid=149

[800-76] NIST Special Publication 800-76-1Biometric Data Specification for Personal Identity Verification, January 2007. http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

[835] Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas. COM/2005/0835 final – COD 2004/0287.

[Biopass] BIOPASS: Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports. Frontex TR 1/2007. ISBN 978-92-95033-00-9.

[BTE] European Biometrics Forum (EBF), Joined Research Centre (JRC), National Physical Laboratory (NPL), Fraunhofer IGD: BioTesting Europe. Towards European Testing and Certification of Biometric Components and Systems (from personal communication with Max Snijder, project coordinator). June 2008.

[CC] The Common Criteria Portal. http://www.commoncriteriaportal.org/

[CHR] Council of Europe, Commissioner for Human Rights. Protecting the right to privacy in the fight against terrorism. https://wcd.coe.int/ViewDoc.jsp?id=1380905

[EBF] European Biometrics Forum. http://www.eubiometricforum.com/

[eIDM] European Commission. Information Society and Media Directorate-General. eGovernment Unit. A Roadmap for a pan-European eIDM Framework by 2010. v1.0. http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf

[ESTA] Electronic System for Travel Authorization. http://www.esta.us/

[FIPS201] Federal Information Processing Standards Publication: Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST, March 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[GRT] Bundesamt für Sicherheit in der Informationstechnik (BSI). Golden Reader Tool. http://www.bsi.de/literat/faltbl/F25GRT.htm

[JRC] EC JRC. Institute for Prospective Technological Studies (ipts). Biometrics at the Frontiers: Assessing the Impact on Society For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE). Technical Report Series EUR 21585 EN. http://ftp.jrc.es/EURdoc/eur21585en.pdf

[NFIQ] NIST Fingerprint Image Quality. http://fingerprint.nist.gov/NFIS/

[NSTC] National Science and Technology Council: NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards. NSTC Subcommittee on Biometrics and Identity Management, September 7, 2007. http://ts.nist.gov/Standards/Biometrics/upload/NSTC_Policy_Bio_Standards_Final_091307_1.pdf

[Reg] Registry of biometric standards adopted by the US Government: www.standards.gov/biometrics

[RTIC] Registered Traveller Interoperability Consortium. http://www.rtconsortium.org/about.cfm

[SC37] ISO Website for SC 37: http://www.iso.org/iso/standards_development/technical_ committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770

[SD2] ISO/IEC JTC 1 SC 37 Standing Document 2 — Harmonized Biometric Vocabulary (ISO/IEC JTC 1 SC 37 N 2777) 2008-01-20.

[TAG18] Guidelines on electronic – Machine Readable Travel Documents & Passenger Facilitation.Version – 1.0. April 17, 2008. http://www.icao.int/icao/en/atb/meetings/2008/TAGMRTD18/TagMrtd18_wp03.pdf

[TOR] Centre Européen de Normalisation :CEN-FOCUSGROUPBIOMETRICS_N0100_Call_for_experts_FG_BIometric.doc. Annex I: Terms of Reference for a Project Team in the Focus Group on BIOMETRICS.

[VERI] Personal Identity Verification (PIV): Image Quality Specifications For Single Finger Capture Devices. July 2006. http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf

[VWP] US Department of State. Visa Waiver Program. http://travel.state.gov/visa/temp/without/without_1990.html

Abbreviations & Glossary

AA	Active Authentication. An ICAO defined protocol
ABC	Automated Border Control
AC Bio	Authentication Context for Biometrics. A SC 27 concept.
Active Authentication	See AA
AFIS	Automated Fingerprint Identification System.
APDU	Application Protocol Data Unit. A concept defined in ISO 7816.
API	Advanced Passenger Information (See also PNR).
API	Application Programming Interface.
BAA	British Airport Authorities. An airport company owning 7 UK airports
BAC	Basic Access Control. An ICAO defined protocol.
Basic Access Control	See BAC.
BDB	Biometric Data Block. A BioAPI concept.
BFP	BioAPI Function Provider. A BioAPI concept.
BioAPI	A SC37 concept for APIs of biometric technology.
BIODEV	BIOmetrics Data Experimented in Visas. A European biometrics application evaluation project.
BIR	Biometric Information Record. A BioAPI concept.
BSI	Bundesamt für Sicherheit in der Informationstechnik. German Federal Office for Information Security.
BSP	Biometric Service Provider. A BioAPI concept.
CA	Chip Authentication. Part of EAC, an ICAO defined protocol.
CBEFF	Common Biometrics Exchange Formats Framework. A SC 37 concept.
CC	Common Criteria. An SC 27 concept.
CEM	Common Methodology for Information Technology Security Evaluation.
CEN	Centre Européen de Normalisation. European Standardization Body.
Chip Authentication	See CA.
Country Signer Certificate	See CSC.
CSC	Country Signer Certificate. Trust Anchor for Passive Authentication.
DHS	US Department of Homeland Security.
EAC	Extended Access Control. An ICAO protocol.
EAL	Evaluation Assurance Level. A CC concept.
EBTS	Electronic Biometric Transmission Specification. The FBI fingerprint standard.
EBTS/F	Electronic Biometric Transmission Specification, Appendix F. Requirements for AFIS fingerprint scanners.
ECC	European Citizen Card.
eID	electronic ID.
e-MRTD	electronic Machine Readable Travel Document
Extended Access Control	See EAC.
ESTA	Electronic System for Travel Authorization. Advance electronic application request through the Internet
FAR	False Acceptance Rate.
FBI	US Federal Bureau of Investigation.

FIPS 201	Federal Information Processing Standards. A US class of standards.
FRR	False Rejection Rate.
IATA	International Air Transport Association.
ICAO	International Civil Aviation Organization.
ID flats	Flat (i.e., not rolled) imprints of all ten fingers.
IPF	Ideal Process Flow. An IATA concept.
ISO/IEC	International Standards Organization/International Electrotechnical Commission.
LDS	Logical Data Structure. Description of data storage in e-passports.
MOC	Match On Card. Better: Comparison On Card.
MRP	Machine Readable Passport.
MRTD	Machine Readable Travel Document.
MRZ	Machine Readable Zone (of an MRTD).
MTF	Modulation Transfer Function. An optical concept.
NIST	US National Institute for Standards and Technology.
NTWG	ICAO New Technology Working Group.
OECD	Organization for Economic Cooperation and Development.
PA	Passive Authentication. An ICAO protocol.
Passive Authentication	See PA.
PIV	Personal Identity Verification. Specified by FIPS 201.
PKI	Public Key Infrastructure.
PNR	Passenger Name Record (See Also API).
PP	Protection Profile. A CC concept.
RFID	Radio Frequency Identification. The technology behind the use of contactless chips in e-Passports and e-MRTDs
SBH	Standard Biometric Header. A BioAPI concept.
SC 17	Subcommittee 17 of ISO/IEC JTC 1. Standardizes smartcards including travel documents.
SC 27	Subcommittee 27 of ISO/IEC JTC 1. Standardizes IT security technology.
SC 37	Subcommittee 37 of ISO/IEC JTC 1. Standardizes biometrics.
SIF	Standard Interchange Format. A BioAPI concept.
SIS II	Schengen Information System II.
SOF	Strength of Function. A CC concept.
SPI	Service Provider Interface. A BioAPI concept.
SPT	See SPTIG.
SPTIG	Simplified Passenger Travel Interest Group. An IATA initiative.
ST	Security Target. A CC concept.
TA	Terminal Authentication. Part of EAC, an ICAO protocol.
Tenprint BioAPI	BioAPI add-on for tenprint applications.
Terminal Authentication	See TA.
TOE	Target of Evaluation. A CC concept.
USG	United States Government.
US-VISIT	United States Visitor and Immigrant Status Indicator Technology. The US immigration and border management system.
VIS	EU Visa Information System.

Annexes

Annex A1: ISO/IEC JTC 1 SC 37 Standards

Copyright acknowledgement

This Annex makes references to ISO/IEC JTC 1 SC 37 Standards under the form of abstracts, mainly those of the Scope of each Standard.

These abstracts are reproduced with the permission of the International Organization for Standardization, ISO. The concerned documents can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

ISO/IEC JTC 1 SC 37 "Biometrics" is responsible for all kinds of biometrics related standards developed by ISO. The following table contains the most relevant standards in the context of interoperable European biometric applications.

ISO/IEC IS 19784-1:2005	Information technology — Biometric application programming interface — Part 1: BioAPI specification
The BioAPI specification is applicable to a broad range of biometric technology types. It is also applicable to a wide variety of biometrically enabled applications, from personal devices, through network security, to large complex identification systems. This part of ISO/IEC 19784 defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this part of ISO/IEC 19784 and to other International Standards. This part of ISO/IEC 19784 supports an architecture in which a BioAPI Framework supports multiple simultaneous biometric applications (provided by different vendors), using multiple dynamically installed and loaded (or unloaded) biometric service provider (BSP) components and BioAPI Units (provided by other different vendors), possibly using one of an alternative set of BioAPI Function Provider (BFP) components (provided by other vendors) or by direct management of BioAPI Units.	

ISO/IEC WD 19784-1 Amd 3	Information technology — Biometric application programming interface — Part 1: BioAPI specification- Amendment 3: Support for interchange of certificates and security assertions, and other security aspects
This amendment to ISO/IEC 19784-1 adds support for biometric fusion and security assertions to the Standard. It extends the API and the SPI of BioAPI by specifying new functions and new values for existing data types. ISO/IEC 19784-1:2006 provides no direct support for biometric fusion. In addition, the use of FARs in the representation of matching scores is not suitable, in general, for performing score-level fusion (although it does allow some limited forms of fusion). This amendment adds support of biometric fusion to the standard. The current version of ISO/IEC 19784-1 provides no support for ACBio instance, standardized in ISO/IEC JTC 1 SC 27 as ISO/IEC 24761. This amendment adds support of biometric fusion to the standard.	

ISO/IEC WD 19784-4.2	Biometric application programming interface — Part 4: Biometric sensor function provider interface
This part of 19784 specifies a sensor module interface for a Biometric Service Provider (BSP) – ISO/IEC 19784-1. The interface supports a BSP wishing to provide the BioAPI SPI interface functions, whilst removing device handling activity from the BSP. This part of 19784 provides an interface that can be used by all types of biometric sensor, including inter alia, image streaming sensors (infrared, face, iris, finger, etc), voice streaming sensors, digital tablets providing dynamic signature data, and signature tablets providing voice data.	

ISO IS 19785-1:2005	Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification
This part of ISO/IEC 19785 defines structures and data elements for biometric information records (BIRs). It defines the concept of a domain of use to establish the applicability of a standard or specification that complies with CBEFF requirements. It defines the concept of a patron format, which is a published BIR format specification that complies with CBEFF requirements, specified by a CBEFF patron. It defines the abstract values (and associated semantics) of a set of CBEFF data elements to be used in the definition of CBEFF patron formats. It specifies the use of CBEFF data elements by a CBEFF patron to define the content and encoding of a standard biometric header (SBH) to be included in a biometric information record (i.e. the definition of a CBEFF patron format). It provides the means for identification of the formats of the biometric data blocks (BDBs) in a BIR, but the standardization and interoperability of BDB formats is not in the scope of this part of the standard. It also provides a means (the security block) for BIRs to carry information about the encryption of a BDB in the BIR and about integrity mechanisms applied to the BIR, but the structure and content of security blocks is the responsibility of CBEFF patrons and is not in the scope. Further, the specification of encryption mechanisms for BDBs and of integrity mechanisms for BIRs is not in the scope of this standard. It specifies transformations from one CBEFF patron format to a different CBEFF patron format. The encoding of the abstract values of CBEFF data elements to be used in the specification of CBEFF patron formats is not in the scope. Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the scope of this standard, but may be subject to national regulation.	

ISO/IEC IS 19785-2:2005	Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority.
This part of ISO/IEC 19785 specifies the procedures to be followed by the Biometric Registration Authority in preparing, maintaining, and publishing registers of identifiers for biometric organizations, CBEFF patron formats, BDB formats, security block formats, and biometric products.	

ISO/IEC IS 19785-3:2007	Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications
This part of ISO/IEC 19785 specifies and publishes registered CBEFF patron formats defined by the CBEFF patron ISO/IEC JTC 1/SC 37, and specifies their registered CBEFF patron format identifiers and resulting full ASN.1 Object Identifiers.	

ISO/IEC IS 19794-1:2006	Information technology — Biometric data interchange formats — Part 1: Framework
This part of ISO/IEC 19794 specifies, general aspects for the usage of biometric data structures, the types of biometric data structure, a naming concept for biometric data structures, a coding scheme for format types. Biometric data include but are not limited to finger minutiae, finger pattern, finger image, face image, iris image and signature/sign behavioural data. This standard is currently under revision in SC 37 (CD status in 2008).	

ISO/IEC IS 19794-2:2005	Information technology — Biometric data interchange formats — Part 2: Finger minutiae data
This part of ISO/IEC 19794 specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. It is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. This part of ISO/IEC 19794 contains definitions of relevant terms, a description of how minutiae shall be determined, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided in an informative annex. This standard is currently under revision in SC 37 (CD status in 2008).	

ISO/IEC IS 19794-4:2005	Information technology — Biometric data interchange formats — Part 4: Finger image data
This part of the ISO/IEC 19794 standard specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 CBEFF data structure. This can be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with this part of the ISO/IEC 19794 standard can be recorded on machine-readable media or may be transmitted by data communication facilities. This standard is currently under revision in SC 37 (CD status in 2008).	

ISO/IEC IS 19794-5:2005	Information technology — Biometric data interchange formats — Part 5: Face image data
This part of ISO/IEC 19794 specifies a record format for storing, recording, and transmitting the information from one or more facial images within a CBEFF data structure, specifies scene constraints of the facial images, specifies photographic properties of the facial images, and specifies digital image attributes of the facial images. Each requirement is specified for the following Face Image Types, respectively. **Basic:** This is the fundamental Face Image Type that specifies a record format including header and image data. All Face Image Types adhere to the properties of this type. No mandatory scene, photographic and digital requirements are specified for this image type. **Frontal**: A Basic Face Image Type that adheres to additional requirements appropriate for frontal face recognition and/or human examination. Two types of Frontal Face Image Types are defined in this document, Full Frontal and Token Frontal (or simply Token). **Full Frontal**: A Face Image Type that specifies frontal images with sufficient resolution for human examination as well as reliable computer face recognition. This type of Face Image Type includes the full head with all hair in most cases, as well as neck and shoulders. This image type is suitable for permanent storage of the face information, and it is applicable to portraits for passport, driver license, and “mug shot” images. **Token Frontal**: A Face Image Type that specifies frontal images with a specific geometric size and eye positioning based on the width and height of the image. This image type is suitable for minimizing the storage requirements for computer face recognition tasks such as verification while still offering vendor independence and human verification (versus human examination which requires more detail) capabilities. This standard is currently under revision in SC 37 (CD status in 2008). It has two technical corrigenda.	

ISO/IEC 19794-5:2005 Amd 1:2007	Information technology — Biometric data interchange formats — Part 5: Face image data. Amendment 1: Conditions for taking photographs for face image data

The purpose of this amendment is to provide expert guidance (i.e., best practices) for the photography of faces, especially when the resulting images are to be used for purposes of identification, either by automated face recognition systems or by human viewers. This guidance is intended for owners and operators of photography studios, photo stores and other organizations producing or requiring either conventional printed photographs or digital images of faces that may be used in applications for passports, visas, or other identification documents and when those images are required to conform to the frontal image types of this part of ISO/IEC 19794. This guidance is also intended for the designers and operators of photo booths, if those booths are required to provide face images conforming to the specifications of this standard. This amendment may also be appropriate source material to application developers, application profile standard developers, or others making more general use of this standard.

There are many factors that affect face recognition system performance, including the individual's appearance, such as his or her facial characteristics, hair style, and accessories, and the acquisition conditions, such as the camera's field-of-view, focus, depth-of-field, background, and lighting. The acquisition conditions have, potentially, a greater influence on face recognition accuracy than the individual's appearance and, of course, are controllable by the preparer of the face images. This amendment provides recommendations for acquiring two-dimensional (2D) face images directly with an analogue, digital, or video camera, as well as for image data acquired through traditional photo printing and digital scanning. The acquisition of three-dimensional (3D) images is out of the scope of this amendment. This amendment may also be appropriate source material for application developers, application profile standard developers, or others making more general use of this standard.

ISO/IEC IS 19794-6:2005	Information technology — Biometric data interchange formats — Part 6: Iris image data

This part of ISO/IEC 19794 specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition.

The first is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format such as that specified by ISO/IEC 15444. The second format is based on a polar image specification that requires certain pre-processing and image segmentation steps, but produces a much more compact data structure that contains only iris information. Data that comply with either one of the iris image formats specified in this part of ISO/IEC 19794 are intended to be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB) as specified in ISO/IEC 19785-1.

This standard is currently under revision in SC 37 (WD status in 2008). In that WD the scope is defined as follows: This part of ISO/IEC 19794 specifies an image interchange format for biometric authentication systems that utilize iris recognition. Within this format the image information may be stored as raw, uncompressed array of intensity values or in a compressed form such as that specified by ISO/IEC 15444.

ISO/IEC IS 19795-1:2005	Information technology — Biometric performance testing and reporting — Part 1: Principles and framework

This part of ISO/IEC 19795 establishes general principles for testing the performance of biometric systems in terms of error rates and throughput rates for purposes including prediction of performance, comparison of performance, and verifying compliance with specified performance requirements; specifies performance metrics for biometric systems; specifies requirements on test methods, recording of data and reporting of results; and provides a framework for developing and describing test protocols, to help avoid bias due to inappropriate data collection or analytic procedures, to help achieve the best estimate of field performance for the expended effort, and to improve understanding of the limits of applicability of the test results.

This part of ISO/IEC 19795 is applicable to empirical performance testing of biometric systems and algorithms through analysis of the matching scores and decisions output by the system, without detailed knowledge of the system's algorithms or of the underlying distribution of biometric characteristics in the population of interest.

ISO/IEC IS 19795-2:2006	Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation
This part of ISO/IEC 19795 provides requirements and recommendations on data collection, analysis and reporting specific to two primary types of evaluation: technology evaluation and scenario evaluation. This part of ISO/IEC 19795 specifies requirements in the following areas: development and full description of protocols for technology and scenario evaluations; and execution and reporting of biometric evaluations reflective of the parameters associated with biometric evaluation types.	

ISO/IEC TR 19795-3	Information Technology – Biometric Performance Testing and Reporting – Part 3: Technical Report on Modality-Specific Testing
In biometric performance testing and reporting, careful consideration should be made regarding the characteristic differences of each modality, such as fingerprint, face, iris, etc. These differences naturally require variations within the general methodology described in ISO/IEC 19795-1, Biometric Performance Testing and Reporting – Part 1: Principles and Framework. This Technical Report is intended to describe the methodologies relating to these modality-dependent variations. The purpose of this document is to present and define methods for determining, given a specific biometric modality, how to develop a technical performance test.	

ISO/IEC IS 19795-4:2008	Information technology — Biometric performance testing and reporting — Part 4: Interoperability performance testing
This part of ISO/IEC 19795 prescribes methods for technology and scenario evaluations of multi-supplier biometric systems that use biometric data conforming to biometric data interchange format standards. It specifies requirements needed to assess performance available from samples formatted according to a standard interchange format (SIF), performance available when samples formatted according to a SIF are exchanged, performance available from samples formatted according to a SIF, relative to proprietary data formats, SIF interoperability, by quantifying cross-product performance relative to single-product performance, performance available from multi-sample and multimodal data formatted according to one or more SIFs, and performance interoperability of biometric capture devices. In addition, this part of ISO/IEC 19795 includes procedures for establishing an interoperable set of implementations, defines procedures for testing interoperability with previously established sets of implementations, and gives testing procedures for the measurement of interoperable performance.	

ISO/IEC CD 19795-5	Information Technology — Biometric Performance Testing and Reporting — Part 5: Scenario Evaluation of Biometric Access Control Systems
This part of ISO/IEC 19795 defines a common biometric access control scenario for use in scenario evaluation of biometric verification systems used in access control systems, provides a framework for expressing quantitative biometric system requirements and achievement, provides a common basis for the conduct of scenario evaluations suitable to a particular testing facility and/or specific biometric system. This part of ISO/IEC 19795 is applicable to empirical performance testing of biometric systems without detailed knowledge of the comparison algorithms or of the underlying distribution of biometric characteristics in the population of interest. The “general purpose” nature of the standard is centred on the most common access control applications, and acknowledges the fact that this framework will not be suitable for highly specialized applications (very high levels of protection, very specialized user populations like elderly, students, etc.). Specialized applications will warrant specialized testing processes. The minimum FAR tested by this standard is 0.1%. If a lower FAR is required, special testing may be appropriate. Not within the scope of this part of ISO/IEC 19795 is the measurement of error and throughput rates for people deliberately trying to circumvent correct recognition by the biometric system (i.e. active impostors). In addition, this standard does not assess Human Factors, Reliability, Maintainability, or Suitability requirements of the final product. This assessment is the responsibility of the purchasing authority for such devices.	

ISO/IEC WD 19795-6	Information technology — Biometrics performance testing and reporting — Part 6: Testing methodologies for operational evaluation
This part of ISO/IEC 19795 provides guidance on the operational testing of biometric systems, specifies performance metrics for operational systems, recommends data to be retained by operational systems to enable performance monitoring, specifies requirements on test methods, recording of data, and reporting of results of operational evaluations.	

ISO/IEC CD 19795-7	Information Technology — Biometric performance testing and reporting — Part 7: Testing of ISO/IEC 7816-based verification algorithms
This standard establishes a mechanism for measuring the core algorithmic capabilities of fingerprint matching algorithms running on standardized ISO/IEC 7816 smart cards. Specifically the standard instantiates a mechanism for MOC testing, standardizes procedures for the measurement of the accuracy of match-on-card (MOC) implementations, standardizes procedures for the measurement of durations the various operations, and gives examples for matching ISO/IEC 19794-2:2005 compact card minutiae templates.	

ISO/IEC IS 24709-1:2006	Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 1: Methods and procedures
This part of ISO/IEC 24709 specifies the concepts, framework, test methods and criteria required to test conformity of biometric products claiming conformance to BioAPI (see ISO/IEC 19784-1). Guidelines for specifying BioAPI conformance test suites, writing test assertions and defining procedures to be followed during the conformance testing are provided. It is concerned with conformance testing of biometric products claiming conformance to BioAPI. It is not concerned with testing other characteristics of biometric products or other types of testing of biometric products (i.e. acceptance, performance, robustness, security, etc.). Testing by means of test methods which are specific to particular biometric products are not the subject of ISO/IEC 24709. This standard is applicable to the development and use of conformance test method specifications, BioAPI conformance test suites and conformance testing programmes for BioAPI-conformant products. It is intended primarily for use by testing organizations, but may be applied by developers and users of test assertions and test method implementations.	

ISO/IEC IS 24709-2:2006	Information technology — Conformance testing for the biometric application programming interface (BioAPI) — Part 2: Test assertions for biometric service providers
This part of ISO/IEC 24709 defines a number of test assertions written in the assertion language specified in ISO/IEC 24709-1. It specifies what subset of all the test assertions defined herein are to be executed for each of the five conformance subclasses of BSPs defined in ISO/IEC 19784-1 (BioAPI 2.0). It also specifies additional assertions that are to be executed depending on the optional features of BioAPI 2.0 that the implementation under test claims to support. Test assertions specified in this part of ISO/IEC 24709 are not claimed to be exhaustive. Biometric service provider implementations that are tested according to the methodology specified in ISO/IEC 24709-1 and with the test assertions specified in this part of ISO/IEC 24709 can (only) claim conformance to those aspects of ISO/IEC 19784-1 that are covered by these test assertions.	

ISO/IEC WD 24709-3	Information Technology — Conformance Testing for the biometric application programming interface(BioAPI) — Part 3: Test assertions for BioAPI frameworks
This part of ISO/IEC 24709 defines a number of test assertions written in the assertion language specified in ISO/IEC 24709-1:2007. It specifies all the test assertions that are to be executed for conformance testing of BioAPI frameworks claiming conformance to BioAPI 2.0. It also specifies additional assertions that are to be executed depending on the optional features of BioAPI2.0 that the implementation under test claims to support. Test assertions specified in this part of ISO/IEC 24709 are not claimed to be exhaustive. Implementations of BioAPI2.0 that are tested according to the methodology specified in ISO/IEC24709-1:2007 and with test assertions specified in this part of ISO/IEC 24709 can (only) claim conformance to those aspects of ISO/IEC 19784-1 that are covered by these test assertions.	

ISO/IEC WD 24709-4	Information Technology — Conformance Testing for the biometric application programming interface(BioAPI) — Test assertions for biometric applications
This part of ISO/IEC24709 defined a number of test assertions written in assertion language specified in ISO/IEC 24709-1. It specifies all test assertions defined herein are to be executed for conformance testing of biometric applications claiming conformance to BioAPI 2.0. It also specifies additional assertions that are to be executed depending on the operational features of BioAPI2.0 that the implementation under test claims to support. Test assertions specified in this part of ISO/IEC 24709 are not claimed to be exhaustive. Implementations of BioAPI2.0 that are tested according to the methodology specified in ISO/IEC24709-1 and with test assertions specified in this part of ISO/IEC24709 can (only) claim conformance to those aspects of ISO/IEC 19784-1 that are covered by these test assertions.	

ISO/IEC IS 24713-1:2007	Information technology - Biometric profiles for interoperability and data interchange - Part 1: Overview of Biometric Systems and Biometric Profiles
This part of ISO/IEC 24713 identifies and defines the functional blocks and components of a generic biometric system, and the distinct characteristics of each component. It also defines a generic biometric reference architecture incorporating the relevant biometric-related base standards to support interoperability and data interchange.	

ISO/IEC IS 24713-2	Information technology — Biometric profiles for interoperability and data interchange — Part 2: Physical access control for employees at airports
This part of ISO/IEC 24713 specifies the biometric profile including necessary parameters and interfaces between function modules. (i.e. BioAPI based modules and an external interface) in support of token-based biometric identification and verification of employees, at local access points (i.e. doors or other controlled entrances) and across local boundaries within the defined area of control in an airport. The token is expected to contain one or more biometric references. The standard does not specify a complete Access Control System for deployment at access points within the secure area of an airport. It is assumed that such systems exist and that a biometric component that is the subject of this part of ISO/IEC 24713 is being added to an existing system. It therefore excludes such things as device features, and exception and incident reporting and handling. This information is contained in an annex for information only. This standard includes recommended practices for enrolment, watch list checking, duplicate issuance prevention, and verification of the identity of employees at airports. It also describes architectures and business processes appropriate to the support of token-based identity management in the secure environment of an airport. It is recommended that the confidentiality, integrity, and availability of biometric data be safeguarded in accordance with local, regional, or national policy considerations.	

ISO/IEC FCD 24713-3	Information Technology — Biometric Profiles for Interoperability and Data Interchange — Part 3: Biometric Based Verification and Identification of Seafarers
This International Standard specifies a biometric profile including data interchange formats, system requirements, and the operation of biometric procedures on a Seafarers' Identity Document (SID). Note that the domain of applicability may extend to other situations where an interoperable biometrics-based identity document is required, but the main focus is on the use of biometrics on a Seafarers' Identity Document (SID). The use of biometric data includes identification checks during the issuance of the document, when watch lists may be checked and the entire database of existing seafarers may be searched to prevent a single seafarer from establishing multiple identities. It also includes the use of biometric data for verification when a card is presented at a control point by a person claiming to be the seafarer to whom the card was issued. Such control points may include port entrances, ship gangplanks, border crossing points where a seafarer must verify themselves to immigration authorities and any other situation where the seafarer needs to verify their identity as a seafarer. This verification is expected to be performed not only indoors under controlled conditions, but also outdoors in difficult conditions, including harsh wet weather, salt spray, high humidity and high temperatures. Biometric equipment and credentials have to be capable of functioning in all such environments. This International Standard notes that ILO Convention No. 185 already provides the overarching policy guidance on biometric verification and identification of seafarers and it relies on that guidance. Determining any matters of policy beyond those or in contradiction to those included in ILO Convention No. 185 is explicitly out of scope for this standard.	

ISO/IEC DTR 24714-1	Biometrics — Cross-jurisdictional and societal aspects of implementation of biometric technologies
This Technical Report gives guidelines for the stages in the life cycle of a system's biometric and associated elements. This covers the capture and design of initial requirements, including legal frameworks, development and deployment, operations, including enrolment and subsequent usage, interrelationships with other systems, related data storage and security of data, data updates and maintenance, training and awareness, system evaluation and audit, controlled system expiration. The areas addressed are limited to the design and implementation of biometric technologies with respect to legal and societal constraints of the use of biometric data, accessibility for the widest population, health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information	

ISO/IEC FCD 29109-1	Information Technology — Conformance Testing Methodology for Biometric Data Interchange Formats defined in ISO/IEC 19794 — Part 1: Generalized Conformance Testing Methodology
This part of the multi-part standard specifies the concepts, test types and conformance testing methodologies to test biometric data interchange records or computer algorithms that create biometric data interchange records. The biometric data interchange records are specified in the multi-part ISO/IEC 19794 biometric data interchange format standard. This standard defines two types (A and B) and three levels (1, 2 and 3) of conformance testing, with a general description and methodology for each one. In the case of the first two levels, there are many common test elements, and so the assertion language for specifying Level 1 and Level 2 test assertions is defined in this standard. This multi-part standard is not concerned with testing of other characteristics of biometric products or other types of testing of biometric products (i.e., acceptance, performance, robustness, security).	

ISO/IEC CD 29109-2	Information Technology — Conformance Testing Methodology for Biometric Data Interchange Records defined in ISO/IEC 19794— Part 2: Finger Minutiae Data
This part of ISO/IEC 29109 specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to biometric data interchange format standard – part 2: finger minutiae data. The standard establishes tests of assertions of the structure of the finger minutiae data format as specified in ISO/IEC 19794-2:2005, tests of assertions of internal consistency by checking the types of values that maybe contained within each field.	

ISO/IEC CD 29109-4	Information Technology — Conformance Testing Methodology for Biometric Data Interchange Formats defined in ISO/IEC 19794— Part 4: Finger Image Data
This part of ISO/IEC 29109 specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to biometric data interchange format standard – part 4: finger image data. The standard establishes test assertions of the structure of the finger image data format as specified in ISO/IEC 19794-4:2005, test assertions of internal consistency by checking the types of values that maybe contained within each field.	

ISO/IEC CD 29109-5	Conformance Testing Methodology — ISO/IEC 29109-5: Face Image Conformance Testing
This part of ISO/IEC 29109:2007 specifies elements of conformance testing methodology, test assertions, and test procedures applicable to the ISO/IEC 19794-5 biometric data interchange format for face image data. The standard establishes test assertions of the structure of the face image data format as specified in ISO/IEC 19794-5:2005, test assertions of internal consistency by checking values across fields.	

ISO/IEC WD 29109-6	Information Technology — Conformance Testing Methodology for Biometric Data Interchange Formats Defined in ISO/IEC 19794–6: Iris Image Data
This part of ISO/IEC 29109 specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to biometric data interchange format standard – part 6: iris image data. The standard establishes test assertions of the structure of the iris image data format as specified in ISO/IEC 19794-6:2005, test assertions of internal consistency by checking the types of values that maybe contained within each field.	

ISO/IEC FCD 29141	Information Technology — Tenprint Capture Using BioAPI
This standard specifies requirements for the use of BioAPI 2.1, specified in ISO/IEC 19784-1 with Amendment. 1, a software interface standard, for the purpose of performing a tenprint capture operation.	

ISO/IEC FCD 29794-1.2	Information Technology — Biometric Sample Quality— Part 1: Framework
This part of ISO/IEC 29794, for any or all biometric sample types as necessary establishes terms and definitions that are useful in the specification, and use of quality metrics, recommends the purpose and interpretation of biometric quality scores, defines the format and placement of quality data fields in biometric data interchange formats, and suggests methods for developing biometric sample datasets for the purpose of quality score normalization.	

ISO/IEC PDTR 29794-4	Information Technology — Biometric Sample Quality — Part 4: Finger Image
This part of ISO/IEC 29794, for aspects of quality specific to the finger image modality specifies terms and definitions that are useful in the specification, use, and test of finger image quality metrics, defines the interpretation of finger image quality scores, identifies or defines finger image corpora for the purpose of serving as information for algorithm developers and users, and develops statistical methodologies specific to finger image corpora for characterizing quality score to facilitate interpretation of scores and relation with matching performance.	

ISO/IEC PDTR 29794-5	Biometric Sample Quality - Part 5: Face Image Data Sample Quality — Technical Report —
This part of ISO/IEC 29794, for aspects of quality specific to the face image modality specify terms and definitions that are useful in the specification, use and testing of face image quality Metrics, and define the purpose, intent, and interpretation of biometric quality scores.	

Annex A2: ISO/IEC JTC 1 SC 17 WG 3 Standards

Copyright acknowledgement

This Annex makes references to ISO/IEC JTC 1 SC 17 WG 3 Standards under the form of abstracts, mainly those of the Scope of each Standard.

These abstracts are reproduced with the permission of the International Organization for Standardization, ISO. The concerned documents can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

ICAO Doc 9303 and related documents

ICAO's 1946 mandate to develop MRTDs is provided by Articles 22, 23 and 37 of the 1994 Chicago Convention which oblige Contracting States to develop and adopt international standards for customs, immigration and other procedures to facilitate the border-crossing processes involved in international air transport.

MRTDs were developed with the assistance of ICAO's Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), through ICAO's NTWG (New Technology Working Group), which receives technical and engineering input from ISO Working Group 3 (ISO/IEC JTC 1 SC 17 WG 3). These specifications are published in ICAO Doc 9303 and endorsed by ISO as ISO/IEC 7501.

As automation of the passport inspection has been recognized from early on as the way to meet the continuous increase in passenger flows across borders, ICAO published the first edition of Doc 9303 as a one part Volume, in 1980, under the title "A Passport with Machine Readable Capability". Doc 9303 is now published in three separate Parts.

- Part 1 - Machine Readable Passports:
  - The Sixth Edition, in two volumes, was published in September 2006.
  - Volume 1 sets forth the specifications for a machine readable passport (MRP), characterized by a visual inspection zone and a machine readable zone (MRZ) containing essential identification and document details in OCR-B typeface.
  - Volume 2 sets forth the specifications for biometric enhancement of the MRP to become an "e-Passport".
- Part 2 - Machine Readable Visas:
  - The Third Edition was published in 2005.
  - Specifications provide for a visa format in two sizes - Format A, sized to fill a passport page, and the smaller format B. Like the MRP the machine readable visa is a standard format consisting of a visual inspection zone and a machine readable zone. However, the Third Edition requires that a space be provided for a portrait of the holder, and fewer layout options than the previous edition allowed.

- Part 3 - Size-1 and Size-2 Machine Readable Official Travel Documents:
    - The Second Edition was published in 2003. Specifications provide for machine readable cards in two sizes: TD-1, an ID-1 size plastic card, and TD-2 having the dimensions defined for the ID-2 type card (ISO/IEC 7810). In addition to the visual inspection zone and the machine readable zone the specifications provide for the addition of "optional capacity expansion technologies" to increase data storage on the documents.
    - The Third edition, still in working draft form, will specify only the contactless integrated circuit (ISO/IEC 14443) for capacity expansion. This edition will integrate, therefore, many late additions to Doc 9303, some of which were previously published in early Doc 9303 Supplements (see paragraph below).
- Supplement:
    - The Supplement to Doc9303, now in its Release 6 (2007), is intended to serve several purposes. It provides periodic guidance, advice, update, clarification and amplification on travel document issuance. It also serves as a “bridge” between the formal drafting of Standards and Technical Reports and the needs of the travel document community to have timely and official direction on which to rely.
    - The Supplement is issued on an as-needed basis, generally twice each year. Previous Releases 1-5 have been limited to ICAO’s Doc 9303-part 1. Release 6 is the first release covering all three parts of Doc 9303.

e-MRTD Implementation Progress and Country Status

Following the first biometrics e-MRTD implementations (contact smart card National IDs) in the Far East in 2000, which predated ICAO’s NTWG specifications and deliverables, over 52 countries had implemented an ICAO compliant e-Passport by end 2007, including virtually all EU members. As of 2008, over 80% of the world passports being issued to citizens are e-Passports, yet only 108 countries (out of the 190 ICAO member states) have introduced a machine readable passport (including an e-Passport). It is expected that by 2010 approximately 80 countries will be delivering e-Passports to their citizens.

Evolution of ICAO reference documents and standards

A standardized Logical Data Structure (LDS) is used to enable global interoperability while accessing and retrieving data from the e-MRTD chip. The originating ICAO document describing the LDS came as a Technical Report which evolved till its latest version (V1.7). Currently the LDS specification is integrated in Doc 9303 Part 1 Volume 2. The LDS layout consists of 16 data groups (DGs) presently under use, which are described in Annex A (of Doc 9303). The biometrics elements are stored in DG2 to DG4. The data groups 17 to19 were reserved for future developments in which both issuing and receiving states could write back some data into the chip. Work along this line and new LDS developments are expected to start under the umbrella of ICAO’s NTWG as of 2009.

ISO/IEC 10373-6:2001 / FPDAM 6:2008	Identification cards — Test methods — Part 6: Proximity cards Amendment 6: Test methods for ePassport
Annex L: e-Passport PICC test methods: This annex defines a test plan for the PICC contactless part of the e-Passport oriented PICC. These tests are divided into tests of the physical and electrical parameters, and tests of the initialization & anticollision and the transport protocol. In order for the PICCs to operate correctly, many functional layers of technology should work together. The purpose of this annex is to define in depth the tests to be performed to minimize the probability that an error or fault remain undetected before the design is approved. For e-Passport compliance testing, this annex is normative. Annex M: PCD test methods: This annex defines a test plan for the contactless part of the e-Passport PCD. These tests are divided into tests of the electrical parameters, according to ISO/IEC14443-2:2001 and tests of the initialization & anti collision and the frame protocol according to ISO/IEC14443-3:2001 and ISO/IEC14443-4:2001. In order for the PCD to operate correctly, many functional layers of technology should work together. The purpose of this annex is to define in depth the tests to be performed to minimize the probability that an error or fault remain undetected before the design is approved. For PCD compliance testing, this annex is interpreted as mandatory.	

(Part of) Doc 9303 6th Edition Part 1 Volume 1	Draft Informative Appendix 1 to Section III: Security Standards for Machine Readable Travel Documents
This Appendix provides advice on strengthening the security of machine readable travel documents made in accordance with the specifications set out in Doc 9303, Part 1 (Machine Readable Passports), Part 2 (Machine Readable Visas) and Part 3 (Machine Readable Size 1 and Size 2 Official Travel Documents). The recommendations cover the security of the materials used in the document's construction, the security printing and copy protection techniques to be employed, and the processes used in the production of document blanks. Also addressed are the security considerations that apply to the personalization and the protection of the biographical data in the document. All travel document-issuing authorities shall consider this Appendix.	

(Part of) Doc 9303 Attachment B	RF Protocol and Application Test Standard for E-Passport - Part 2. Tests for Air Interface, Initialization, Anticollision and Transport Protocol
This document defines a test plan for the contactless part of the e-Passport. These tests are divided into tests of the physical and electrical parameters according to ISO/IEC14443-1 and -2, and tests of the initialization & anticollision and the transport protocol according to ISO/IEC14443-3 and -4. In order for the SCIC to operate correctly, many functional layers of technology MUST work together. The purpose of this document is to define in depth the tests to be performed to minimize the probability that an error or fault remain undetected before the design is approved.	

(Part of) Doc 9303 Attachment C	RF Protocol and Application Test Standard for E-Passport – Part 3. Tests for Application Protocol and Logical Data Structure
An essential element of the new ICAO compliant e-Passport is the addition of a Secure Contactless Integrated Circuit (SCIC) that holds securely biometric data of the e-Passport bearer within the ICAO defined Logical Data Structure (LDS). Successful integration of the SCIC into the e-Passport depends upon active international cooperation between many companies and organizations. The e-Passport has been specified and designed to operate correctly across a wide variety of reading infrastructures worldwide. The risk profile for the e-Passport indicates a high impact if that design includes a widespread error or fault. Therefore it is essential, that all companies and organizations involved make all reasonable efforts to minimize the probability that this error or fault remains undetected before that design is approved and e-Passports are issued. This test specification covers the application interface, i.e. the ISO7816 conformance of the e- Passport Chip and the conformance of the LDS.	

(Part of) Doc 9303 Attachment D	RF Protocol and Application Test Standard for E-Passport - Part 4. E-Passport Reader Tests for Air Interface, Initialization, Anticollision and Transport Protocol
The e-Passport and the e-Passport reader (proximity coupling device or PCD) have been specified and designed to operate correctly across a wide variety of infrastructures worldwide. The risk profile for the e-Passport and the reader indicates a high impact if that design includes a widespread error or fault. Therefore, it is essential that all companies and organizations involved make all reasonable efforts to minimize the probability that this error or fault remains undetected before that design is approved and e-Passports and e-Passport readers are issued. This document defines a test plan for the contactless part of the PCD. These tests are divided into tests of the electrical parameters, according to ISO/IEC14443-2 and tests of the initialization & anti collision and the frame protocol according to ISO/IEC14443-3 and -4.	

ISO/IEC 7501-1:2007	Identification cards — Machine readable travel documents — Part 1 : Machine readable passport
This ISO standard is the ISO reference to Doc 9303 Part 1.	

ISO/IEC 7501-3:2007	Identification cards — Machine readable travel documents — Part 3: Machine readable official travel documents
This ISO standard is the ISO reference to Doc 9303 Part 3.	

Doc 9303	Part 1 – Machine Readable Passports. Volume 1. Passport with Machine Readable Data Stored in Optical Character Recognition Format, Sixth Edition
Volume 1 sets forth the specifications for a machine readable passport (MRP), characterized by a visual inspection zone and a machine readable zone (MRZ) containing essential identification and document details in OCR-B typeface.	

Doc 9303	Part 1 - Machine Readable Passports. Volume 2. Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition
Volume 2 defines the specifications for biometrically enhanced MRPs to become an "e-Passport".	

Doc 9303	Part 2 – Machine Readable Visas
The third Edition was published in 2005. Specifications provide for a visa format in two sizes – Format A, sized to fill a passport page, and the smaller format B. Like the MRP the machine readable visa is a standard format consisting of a visual inspection zone and a machine readable zone. However, the Third Edition requires that a space be provided for a portrait of the holder, and fewer layout options than the previous edition allowed.	

Doc 9303	Part 3 - Machine Readable Official Travel Documents. Volume 1. MRTDs with Machine Readable Data Stored in Optical Character Recognition Format
Third Edition — 2008. Doc 9303, Part 3, Volume 1 defines the specifications for two sizes of machine readable official travel documents (MRTDs), providing for global data interchange using both visual (eye readable) and machine readable (optical character recognition) means. The specifications lay down standards for identity documents that can, where issued by a State or organization and accepted by a receiving State, be used for cross-border travel purposes. The MRTDs shall, as a minimum, contain the mandatory data specified in this volume, in the prescribed standard format. This volume also includes specifications for the mandatory and discretionary incorporation of security features. The specifications of Part 3 may be used by a State or organization for the issuance of a machine readable passport in the form of a Size 1 card.	

Doc 9303	Part 3 - Machine Readable Official Travel Documents. Volume 2. Specifications for Electronically Enabled MRTDs with Biometric Identification Capability
Third Edition — 2008. This document defines the specifications, additional to those for the basic td1 and td2 set forth in Volume 1 of Doc 9303, Part 3, to be used by States wishing to issue an electronically enabled machine readable official travel document (e-MRTD) capable of being used by any suitably equipped receiving State to read from the document a greatly increased amount of data relating to the MRTD itself and its holder. This includes mandatory globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems. The specifications require the globally interoperable biometric data to be stored in the form of high-resolution images on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. The specifications also permit the storage of a range of optional data at the discretion of the issuing State. Since the use of the contactless integrated circuit is independent of the size of the document, all specifications apply to both the td1 and td2 in their electronically enabled form. Differences between td1 and td2 format e-MRTDs relate to the MRZ, with consequences for the storage of the MRZ in the contactless IC. These differences are indicated in the specifications in this volume.	

Doc 9303	Supplement to Doc 9303. Release 6
To as great an extent as possible, the Supplement will address any issue that comes within the scope and purpose of the ICAO TAG, and in particular, the NTWG. The development of the Supplement and its content shall be a collegial undertaking, with Government officials working hand-in-hand with SC 17 WG 3 and other private sector entities. While the vehicle for developing revisions of the Supplement shall be the WG 3 Task Force One, all members of the ICAO community are expected to contribute to substance and content. The Supplement shall only be authorized for issuance, or shall be issued directly, by the NTWG. The Supplement will be published on a regular schedule as well as on an as-needed basis.	

TAG TR	Guidelines electronic- Machine Readable Travel Documents & Passenger Facilitation, Technical Report, ICAO Version - 1.0, April 17, 2008
The aim of these guidelines is to offer suggestions as to the use of an e-MRTD within a semi or even fully automated inspection process, in order to facilitate enhanced passenger flows within airlines, airports, seaports or at land borders. The scope consequently includes official immigration and border control procedures at such points of entry and exit.	

Annex A3: National Quality Schemes

In this Annex, the most relevant national standards on biometric data formats are mentioned which do not have a direct equivalent in SC 37 standards. As they have international importance and could be the basis for European requirements, they are mentioned here.

In particular, the standards in the context of Automated Fingerprint Identification Systems (AFIS) which have been set by FBI and NIST in the US should be observed. These standards have proven to be usable for a large scale heterogeneous biometric system for more than a decade. The Electronic Biometric Transmission Specification (EBTS), especially the Appendix F thereof, have been the prototype for similar specifications all over the world.

For application in e-Passport and e-Visa projects, the German Federal Office for Information Security (BSI) has published the technical guideline document TR 03104 as a modification and extension of the EBTS/F especially containing requirements for fingerprint scanners.

Best Practices	Best Practices in Testing and Reporting Performance of Biometric Devices, Mansfield, A. J.; Wayman, J. L. Version 2.01, August 2002
Focuses on all aspects of testing FAR, FER, and FRR. Version 2 is improved and extended.	

UK Government Biometrics Working Group	Biometric Device Protection Profile (BDPP), Draft Issue 0.82, 5 September 2001
Describes all kind of attacks on biometrics authentication systems.	

BEM CC Biometric Evaluation Methodology Working Group - United Kingdom	Common Criteria - Common Methodology for Information Technology Security Evaluation - Biometric Evaluation Methodology Supplement [BEM]. Version 1.0, August 2002
This document is aimed mainly at evaluators and ITSEFs. Its purpose is to clarify the Common Criteria evaluation methodology applicable to the assurance requirements for evaluations of biometric systems and products. It also includes additional guidance relating to the definition of an evaluation Security Target (ST), for example the selection of appropriate security functions; vulnerabilities and threats; and testing for statistical and security features.	

FBI/PIV	Personal Identity Verification (PIV). Image Quality Specifications for Single Finger Capture Devices
These specifications apply to fingerprint capture devices which scan and capture at least a single fingerprint in digital form. They provide criteria for insuring that the image quality of such devices is sufficient for the intended applications; a primary application is to support subject authentication via one-to-one fingerprint matching in the United States government's PIV programme. The fingerprint capture device must be capable of producing images which exhibit good geometric fidelity, sharpness, detail rendition, gray-level uniformity, and gray-level dynamic range, with low noise characteristics. The images must be true representations of the input fingerprints, without creating any significant artifacts, anomalies, false detail, or cosmetic image restoration effects. The fingerprint capture device is expected to generate good quality finger images for a very high percentage of the user population, across the full range of environmental variations seen in the intended applications.		

MTR 060170. MITRE Technical Report	Test Procedures for Verifying Image Quality Requirements for Personal Identity Verification (PIV) Single Finger Capture Devices
This document defines the test procedures used to verify compliance with the Federal Bureau of Investigation (FBI)'s image quality specification for Personal Identity Verification (PIV) single fingerprint capture devices. FBI certification of a PIV single fingerprint capture device is the major step in obtaining formal approval of the device for use in the federal government's PIV programme [FIPS]. The single fingerprint capture device, with its associated image processing, must be capable of producing images which exhibit good geometric fidelity, sharpness, detail rendition, gray level uniformity, and gray level dynamic range, with low noise characteristics. The fingerprint capture device is expected to generate good quality finger images for a very high percentage of the user population, across the full range of environmental variations seen in the intended applications; a primary application is to support subject authentication via one-to-one fingerprint matching.		

NIST Special Publication 800-76-1	Biometric Data Specification for Personal Identity Verification
FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors, defines procedures for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS also defines the structure of an identity credential which includes biometric data. This document contains technical specifications for biometric data mandated in the PIV programme. These specifications reflect the design goals of interoperability and performance of the PIV Card. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The goals are addressed by citing biometric standards normatively and by enumerating requirements where the standards include options and branches. In such cases, a biometric profile can be used to elucidate required versus optional content. This document goes further by constraining implementers' interpretation of the standards. Such restrictions are designed to ease implementation, assure conformity, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.		

NISTIR 7151. August 2004	National Institute of Standards and Technology. Fingerprint Image Quality (NFIQ)
In this report, we propose a new definition of quality of fingerprint impressions and present detailed algorithms to measure image quality for fingerprints. We define fingerprint image quality as a predictor of matcher performance before a matcher algorithm is applied. This means presenting the matcher with good quality fingerprint images will result in high matcher performance, and vice versa, the matcher will perform poorly for poor quality fingerprints. We also have carried out an objective evaluation of the quality assessment of fingerprint images. Our quality measure is implemented in the C programming language and has been tested on 20 different live scan and paper fingerprints datasets collected in different operational settings. Our implementation is publicly, but export controlled, available as part of NIST's fingerprint software distribution.		

FIPS PUB 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors
This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. The standard contains two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, Interfaces for Personal Identity Verification. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.	

IAFIS-DOC-01078-8.002	Electronic Biometric Transmission Specification (EBTS)
The appendices of this document contain all the information needed regarding a particular type of electronic transaction when communicating with the FBI. Appendix F gives IAFIS Image Quality Specifications for fingerprint scanners, both for traditional rolled prints and “Identification Flats,” and printers, and gives Fast Track Certification procedures. Appendix N provides definition descriptors and field edits of Type-14 records for Civil Background Checks using flat impressions.	

ANSI/NIST-ITL 1-2007	Information Technology: American National Standard for Information Systems — Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information – Part 1
This standard defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mug shot, scar mark & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images. This information is primarily intended for interchange among criminal justice administrations or organizations that rely on automated fingerprint and palm print identification systems, or use facial/mug shot, SMT, iris, or other biometric data for identification purposes. This standard does not define the characteristics of the software that shall be required to format the textual information or to compress and reconstruct the associated digital fingerprint image information. Typical applications for this software might include, but are not limited to, computer systems associated with a live-scan fingerprinting system, a workstation that is connected to or is part of an Automated Fingerprint Identification System (AFIS), or an image storage and retrieval system containing fingerprints, facial/mug shot, SMT, or other biometric images.	

BSI-TR-03104	Technische Richtline zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe
This Technical Guideline specifies the requirements for capturing, quality assessment, and transmission of data to be stored in passports for the Federal Republic of Germany.	

BSI-TR-03104 Annex 1 (QA-Face) V 2.1	Technical Guideline for the acquisition, quality assurance and transfer production data for passports. Quality requirements for the acquisition and transfer of facial images as biometric features for electronic passports
In this document, quality assurance of biometric data means the compliance to the effective standards concerning the characteristics of captured facial images as well as the applicability of captured data for the biometric verification with a matching value as high as possible for the legitimate document holder.	

BSI TR-03104 Annex 2 (QA-Finger) V 2.1	Technical Guideline for the acquisition, quality assurance and transfer production data for passports. Quality requirements for the acquisition and transfer of fingerprint images as biometric features for electronic passports
In order to ensure the world-wide application of biometrically enabled travel documents, their interoperability, i.e. their applicability within technical applications from different producers and the infrastructure of different states has to be warranted. Therefore the storage of facial images and fingerprints according to international standards has been decided as a consistent reference. Different verification procedures all over the world will use these digital data to execute biometric verification of the document owner. In the present document, quality assurance of biometric data means the compliance to the effective standards concerning the characteristics of captured fingerprints as well as the applicability of captured data for the biometric verification with a matching value as high as possible for the legitimate document holder.	

NSTC Subcommittee on Biometrics and Identity Management	Registry of USG Recommended Biometric Standards. Version 1.0. Approved June 5, 2008
This Registry lists recommended biometric standards for USG-wide use. Only standards finalized and approved by a standards developing organization are eligible for analysis by the Subcommittee. Inclusion of a standard in this Registry requires consensus agreement of USG agencies through the Subcommittee's deliberative process. For dated references to standards, only the edition cited applies. For undated references to standards, the latest edition of the referenced standard (including any amendments) applies. Therefore, along with recommended biometric standards, some high level guidance is often provided with respect to implementation, migration, and grandfathering of existing implementations. Additional biometric standards will be added to this Registry as other standards are approved by the standards developers and evaluated by the USG for USG-wide use. Source: http://ts.nist.gov/Standards/Biometrics/upload/Biometric_Standards_Registry_Version_1_June_5_2008.pdf	

Annex A4: Relevant Pilot Projects

This Annex contains a non-complete list of documentations and reports on important biometrics trials which are relevant to ABC.

UKPS	UK Passport Service. Biometrics enrolment Trial. Report May 2005
The goal of the UKPS Biometrics Enrolment Trial was to test the processes and record customer experience and attitude during the recording and verification of facial, iris and fingerprint biometrics, rather than test or develop the biometric technology itself – it was not a technology trial. A one-off, integrated solution, which used the latest technologies available at the beginning of the Trial, was designed to address the specific objectives of the Trial. The Trial covered testing the use of biometrics through a simulation of an application process, inclusion of exception cases, e.g. people who may have difficulties in enrolment, measurement of the process times, assessment of customer perceptions and reactions, and testing fingerprint and iris biometrics for one-to-many identification and testing facial, iris and fingerprint biometrics for one-to-one verification. The purpose of this report is to document the key findings of the UKPS Biometrics Enrolment Trial. The report does not investigate the reasons behind the findings, nor does it suggest technology fixes for any of the issues encountered – these may be addressed in further trials. Evidence contained within the report has demonstrated that the above objectives have been successfully achieved.	

BSI	Public Final Report. BioFace I & II Study, Comparative Study of Facial Recognition Systems. Version 2.1, June 2003
In the sub-projects BioFace I and BioFace II, a comparative study of the recognition performance of facial recognition systems was carried out. The studies were conducted firstly at the level of pure algorithm tests (laboratory tests) in the area of verification (1:1 comparison) and identification (1:n comparison) and secondly at the level of a test under realistic conditions of use in the area of identifycation (practical tests/system test). The primary aim was to analyse the capability of the systems with large volumes of data and the influence of noise factors. The present report documents the framework conditions, the data material used and the procedure and results of the studies themselves.	

BSI	BioP I - An investigation into the performance of facial recognition systems relative to their planned use in photo identification documents. Version 1.1, 2004-04-07
The BioP I project examined the feasibility and the following technical implementation issues. Is facial recognition technically suitable for use with photo identity cards? In what form and quality do the biometric characteristics have to be provided? What are the main parameters that influence facial recognition? How difficult is it to outwit facial recognition systems? Which of the facial recognition systems tested achieves the best recognition performance? In addressing these issues, the underlying international situation, especially the ICAO guidelines on facial images that can be used with biometric systems, are the primary yardstick. The photo identity cards included in the study were the current German federal identity card, the German passport, the EU visa, papers documenting the long-term right of abode following the EU model and the new provisional passports and identity cards of the Federal Republic of Germany.	

BSI	BioP II - Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen. Version 2.0, 2005-08-23
The goal of the BioP II project was to obtain a solid basis of information for forthcoming, fundamental decisions on the biometric characteristic that should be incorporated in German identity documents. The project should help to acquire more experience on planning and operation of biometric systems. The BioP II project included practical trials of the biometric processes for face, finger and iris recognition in a comparative system test. Especially with regard to its suitability for international interaction, it analyzed the extent to which the use of images of biometric details in conformance with ICAO requirements is practicable as a basis of reference for biometric verification. Alongside the practical system test, usability and acceptance research was carried out. A series of trials over two times six weeks with 1000 volunteer test candidates from Fraport AG and Lufthansa AG and another 100 people from the Federal Police Service started with enrolment in March 2004. The trials began in April. Three different biometric recognition methods (iris recognition, face recognition and fingerprint) were subjected to comparative evaluation.	

BSI	Evaluation of Fingerprint Recognition Technologies – BioFinger. Version 1.1, 2004-08-06
As a biometric identification property, fingerprints have had a long tradition and are a synonym for the uniqueness (of man). Up until recently, it was only the resulting fingerprint image that was exclusively used as an identification feature; no further processing was carried out. Human fingerprints were almost solely used for forensic purposes in dactyloscopy. Dactyloscopists examine fingerprints with regard to details that can be used to identify people. Evidence of a fingerprint found at a scene of a crime can thus be allocated to a person as the one who left that trace. Since fingerprints can be classified, they can be categorized into various finger classes by making use of the fact that due to the ridge flow so-called patterns (loops, arches, whorls) are formed and that due to the interruptions of the ridges, anatomic characteristics (minutiae) are shaped. Thanks to the large dactyloscopic information content in individual prints, a dactyloscopic expert can determine, by comparison, whether individuals are identical or not. In the past, it took a lot of time to find one person in a hard copy database (identification) and then to prove that the fingerprints at the site of the crime and in the database were identical. The initial use of computers for identification purposes was limited by a quick searching of an electronic database. Dactyloscopic experts provided the details necessary for that searching process. Since computer performance capacities have increased, image processing of fingerprints and thus their electronic evaluation became possible. Initially, dactyloscopic systems analyzed and extracted all known details. As far as their application in an access control system was concerned, the use of these comprehensive details resulting from fingerprints proved to be impractical. Processing time was too long and the amount of extracted details too large. As a result, the amount of data was reduced, i.e. certain patterns were treated as negligible. Additionally, the number of minutiae was reduced. Mostly, for today's access control systems, minutiae are simply defined as ridge endings or ridge bifurcations. Within this context, a number of examinations are carried out in the BioFinger Project, which are to clarify the suitability of some chosen products. The question is this: Using today's systems or components, are there fingerprint recognition systems that have verification characteristics, or can they be assembled. Due to the special demands on personal documents, i.e. usable lifetime of ten years, the ageing of fingerprints with regard to their characteristic to identify people, is very significant.	

Annex A5: ISO/IEC JTC 1 SC 27

Copyright acknowledgement

This Annex makes references to ISO/IEC JTC 1 SC 27 Standards under the form of abstracts, mainly those of the Scope of each Standard.

These abstracts are reproduced with the permission of the International Organization for Standardization, ISO. The concerned documents can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

ISO/IEC CD 24761.3	Information technology - Security techniques - Authentication context for biometrics
This International Standard defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. This International Standard specifies cryptographic syntax of ACBio. The cryptographic syntax of ACBio is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML mark up.	

ISO/IEC WD 24745	Information technology - Security techniques - Biometric template protection
Within the scope of this international standard, the following topics are addressed: Security aspects of biometric system to discover the vulnerability and clarify the security threats and countermeasures. Biometric system application models and their related security and privacy issues. Description on the relationship between the biometric reference and other user data and the various cryptographic techniques that bind the biometrics reference with subject's data under various requirements for confidentiality and integrity. Biometric information privacy to be considered as the right to control over subject's own biometric information in it's lifecycle of collecting, transferring, using, storing, archiving, and disposing process. And also, the responsibility of the biometric information receiver.	

Common Criteria for Information Technology Security Evaluation V 3.1 Part 1	Introduction and general model September 2006 Version 3.1 Revision 1
This multi-part standard, the Common Criteria (CC), is meant to be used as the basis for evaluation of security properties of IT products. By establishing such a common criteria base, the results of an IT security evaluation may be meaningful to a wider audience. Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC.	

Common Criteria for Information Technology Security Evaluation V 3.1 Part 2	Security functional components September 2007 Version 3.1 Revision 2
This part of the CC defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.	

Common Criteria for Information Technology Security Evaluation V 3.1 Part 3	Security assurance components September 2007 Version 3.1 Revision 2
This CC Part 3 defines the assurance requirements of the CC. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component Targets of Evaluation (TOEs), the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of PPs and STs.	

CEM Common Methodology for Information Technology v3.1	Security Evaluation Evaluation methodology September 2007 Version 3.1 Revision 2
The Common Methodology for Information Technology Security Evaluation (CEM) is a companion document to the Common Criteria for Information Technology Security Evaluation (CC). The CEM defines the minimum actions to be performed by an evaluator in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC.	

ISO/IEC 15408-2:2005	Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components
ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.	

ISO/IEC 15408-3:2008	Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components
ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component Targets of Evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets. ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.	

ISO/IEC 18045:2008	Information technology -- Security techniques -- Methodology for IT security evaluation
ISO/IEC 18045:2008 is a companion document to ISO/IEC 15408, Information technology - Security techniques - Evaluation criteria for IT security. ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. ISO/IEC 18045:2008 does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.	

Annex A6: European Citizen Card

CEN/TS 15480-1	Identification card systems – European Citizen Card – Part 1: Physical, electrical and transport protocol characteristics
This document specifies Electronic Citizen Card (ECC) requirements .The ECC, is a smart card issued under the authority of a government institution, either national or local and carries credentials in order to provide all or part of the following services: verify the identity, act as an Inter-European Union travel document, facilitate logical access to e-Government or local administration services. A Public Administration authority may entitle a private organization to provide all or part of the ECC services. The requirements described in the document are used to: define a plastic body card with associated physical and logical securities, specify the electrical interface and data transport protocols for the ECC, and support the basic set of Identification and, Authentication elements visible at the card surface.	

CEN/TS 15480-2	Identification card systems – European Citizen Card – Part 2: Logical data structures and card services
This document specifies the logical characteristics and security features at the card/system interface for the European Citizen Card. The European Citizen Card is a smart card with Identification, Authentication and electronic Signature (IAS) services. Therefore the supported services are specified, the supported data structures as well as the access to these structures are specified, and the command set is defined. The document has the objective of ensuring the interoperability at card/system interface in the usage phase. This specification is also compliant with ICAO specifications. It does not mandate the use of a particular technology. It encompasses mandatory and optional features. Optional features make up a toolbox of modular options from which issuers can pick up the necessary protocols to fulfill the requisites of their use cases. Interoperability requires a specific agreement between issuers and governments in order to determine which cross-border services are to be shared, and consequently which protocols are to be supported by the terminals in each country. All the APDU commands described in this document are in accordance with ISO/IEC 7816 Part 4 or Part 8.	

CEN/TS 15480-3	Identification card systems – European Citizen Card – Part 3: European Citizen Card Interoperability using an application interface
CEN/TS 15480 part 3 provides an interoperability model, which will enable a client application to interoperate with different implementations of the European Citizen Card using an application interface. It also defines a set of on-card data structures enabling the communication between the card and a client application compliant with ISO 24727-3. This standard offers the card issuer and application provider a generic interoperability framework • Proposing a standard middleware for the ECC • Based on a set of standard data set in the card Any card compliant with 15480-2 and –3 able to provide IAS services to any client application compliant with ISO 24727-3.	

CEN/TS 15480-4	Identification card systems — European Citizen Card — Part 4: Recommendations for European Citizen Card issuance, operation and use
CEN/TS 15480-4 will recommend card issuance and operational procedures including citizen registration. CEN/TS 15480-4 will also identify a set of standard ECC use cases (National ID card, e-Government Card, City Card, etc.) For each use case the standard will select a subset of technical requirements from ECC parts 1 and 2, and consider the operation of the ECC in its particular environment.	

Annex A7: ISO TC 68/SC 2

Copyright acknowledgement

This Annex makes references to ISO/IEC TC 68 Standards under the form of abstracts, mainly those of the Scope of each Standard.

These abstracts are reproduced with the permission of the International Organization for Standardization, ISO. The concerned documents can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at the following address: www.iso.org. Copyright remains with ISO.

TC 68/SC 2 is responsible for “Security management and general banking operations”.

Many of the standards developed in this SC deal with the protection and authenticity assurance of business relevant data in large scale applications. Many experiences, especially in the field of cryptography, should be considered to be reused in biometric systems.

ISO 19092:2008	Financial services - Biometrics - Security framework
ISO 19092:2008 describes the security framework for using biometrics for authentication of individuals in financial services. It introduces the types of biometric technologies and addresses issues concerning their application. ISO 19092:2008 also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner. The following topics are within the scope of ISO 19092:2008. Usage of biometrics for the authentication of employees and persons seeking financial services by: verification of a claimed identity, identification of an individual, validation of credentials presented at enrolment to support authentication as required by risk management, management of biometric information across its life cycle comprised of the enrolment, transmission and storage, verification, identification and termination processes, security of biometric information during its life cycle, encompassing data integrity, origin authentication and confidentiality, application of biometrics for logical and physical access control, surveillance to protect the financial institution and its customers, and security of the physical hardware used throughout the biometric information life cycle. ISO 19092:2008 provides the mandatory means whereby biometric information may be encrypted for data confidentiality or other reasons.	

Annex B: Data Group Reference Numbers Assigned to LDS

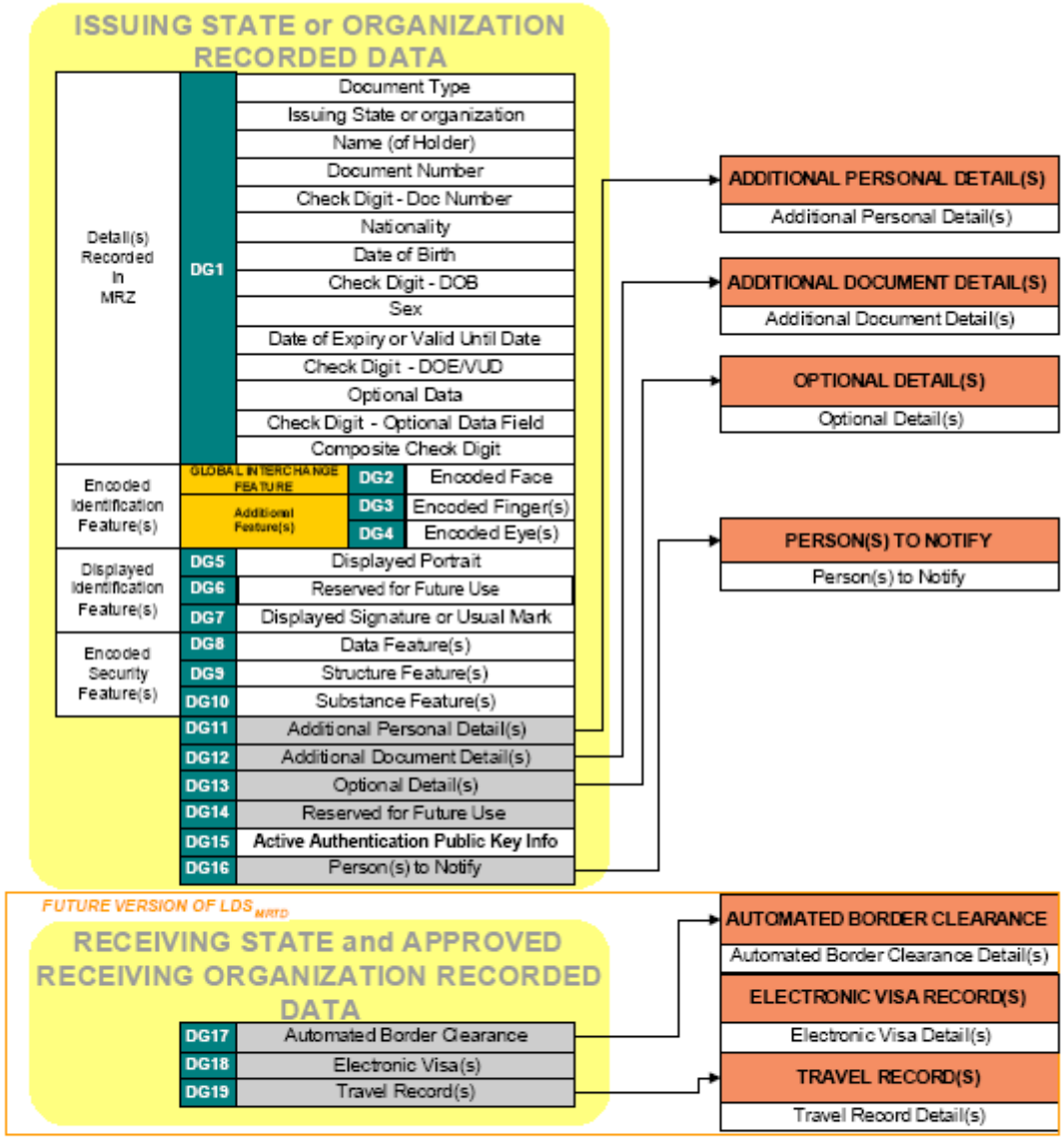


FIGURE V-2. DATA GROUP REFERENCE NUMBERS ASSIGNED TO LDS [Version 1.7]

Annex C1: Features of PRIVIUM ABC

Location	Schiphol-Airport Amsterdam, The Netherlands
Introduction date	1st October 2001
ABC or semi ABC	Fully automated with intervene option immigration service
Responsible authority	Airport Authority in cooperation with Ministry of Justice, IND and Royal Marechaussee
Target group	Frequent Flyers with an EU-nationality
Fee	Yes
Enrolment centre	Yes
Entry control	Yes
Exit control	Yes
Number of gates	3 exit, 2 transfer, 5 entry and 3 Schengen transit points
Biometric used	Iris recognition
Token	Smart card
Storage biometric	On smart card as a template
Average process time	10 – 15 seconds
Performance & Security	Not reported
Description system	
Upon application, an enrolment record is created and biographical and iris biometric data collected. A smart card containing the iris template is then issued to the traveller.	
Description process	
On arrival at the airport, travellers are asked to present the card to the automated border control system and look into a camera so a live iris scan can be collected. The iris template is retrieved from the card and compared to live iris scan to verify the card holder's identity. This process takes approximately 10-15 seconds to complete. If system is unable to verify the traveller's identity then they are referred to manual processing.	
Additional information	
www.privium.nl	
Content updated	01 January 2007

Annex C2: Features of IRIS (Iris Recognition Immigration System) ABC

Location	London-Heathrow Terminals 1, 2, 3, 4 & London-Gatwick North, Manchester Terminals 1 & 2 and Birmingham
Introduction date	3rd January 2006
ABC or semi ABC	IRIS barriers are fully automated
Responsible authority	United Kingdom Immigration Service
Target group	Frequent Flyers, Returning Residents, Visa Holders
Fee	None
Enrolment centre	Enrolment Stations available at all the above eight terminals
Entry control	Yes
Exit control	No
Number of gates	8 - LHR 4, LGW 1, MAN 2, BRH 1
Biometric used	Iris recognition
Token	No
Storage biometric	In database
Average process time	15-20 seconds to pass through the IRIS barrier
Performance & Security	Not reported
Description system	
The IRIS system was introduced in order to expedite the clearance of bona fide, pre-enrolled passengers through the United Kingdom Immigration control. Enrolment onto the scheme takes place in the IRIS Enrolment Stations situated in the airside departure lounges of the participating airport terminals. Enrolment is carried out by forgery trained Immigration Officers. The checks carried out on enrolment mirror those carried out on the primary arrivals control. At enrolment there is a 1:many n search of the IRIS database and a photograph is taken of the passenger together with their iris patterns and this information is linked to their passport data, together with their immigration status in the UK.	
Description process	
On arrival at the airport and for as long as their entitlement to use the scheme is valid, enrolled passengers are able to use the IRIS automated barriers to enter the United Kingdom, by looking into an iris recognition camera, which performs a 1:many search against the database and provides a response within 2/3 seconds. If the passenger's registration is valid, the landside glass doors of the barrier open to allow the passenger to enter the United Kingdom without the need to be seen by an Immigration Officer. The entire transaction, from entering the first gate of the IRIS barrier to exiting the second gate into the United Kingdom takes approximately 15-20 seconds.	
Additional information	
Roll out to Gatwick South is planned by the end of March 2007 increasing the number of enrolment stations and barriers to nine. www.iris.gov.uk	
Content Updated	01 January 2007

Annex C3: Features of RAPID (Automatic Identification of Passengers Holding Travelling Documents)

Location	Main Airport in Lisbon and on other national airports.
Introduction date	May 2007
ABC or semi ABC	ABC
Responsible authority	Serviço de Estrangeiros e Fronteiras (SEF) (Portuguese Immigration)
Target group	EU Citizens, EEA citizens and citizens from CH older than 18
Fee	No
Enrolment centre	No enrolment required
Entry control	Yes
Exit control	Yes
Biometric used	Face
Token	e-Passports
Storage biometric	Contact less chip in travel document
Average process time	15 seconds
Performance & Security	Not reported
Description system	
This is the first system worldwide to allow an automatic control of passengers who hold electronic passports, thereby removing the need for human action. This system combines the operations of reading and checking electronic passports with an innovating feature for assessing the biometric data which operates an automatic door opening device. This feature checks, on a first instance, the genuineness of the electronic passports and validates all data stored in the chip and check the Schengen and Internal Database (Restrict Measures), and, on a second instance, it appraises the passenger's identification by establishing a comparison between the photo stored in the chip and the image of the passenger in loco, automatically opening the passage door when the features of both images are coincident. RAPID was made secure by an intelligent system that allows the entry of one passenger alone and automatically adjusts the reading camera to his / her height. After that, it performs a live match-to-chip verification of facial biometrics, therefore providing passengers a quick and simple way to get clearance at the border.	
Description process	
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 15 seconds it will speed up the movement of passengers at border control significantly.	
Additional information	
We aimed to install e-gates in all border Posts until the end of this year. For more information, please check the following websites: www.sef.pt; or http://tv.sef.pt; or www.rapid.sef.pt	
Content updated	February 2008

Annex C4: Features of MiSense and MiSensePlus Trials

Location	London- Heathrow Terminal, 3 United Kingdom
Introduction date	November 2006
ABC or semi ABC	Trial System with elements of manual intervention around background and routine checks
Responsible authority	United Kingdom Immigration Service
Target group	European Economic Area Travellers
Fee	None
Enrolment centre	Yes
Entry control	Yes
Exit control	Yes
Number of gates	3 plus (1 arrivals 2 ticket presentation 6 portable devices for boarding)
Biometric used	Fingerprint (all 13 bio's captured at enrolment)
Token	2nd Generation ICAO Passport Smartcard
Storage biometric	Template on Card
Average process time	7-12 Seconds at arrivals gate (to be confirmed at end of trial)
Description system	
The system is a Registered Traveller system design to expedite passenger travel through a port terminal– Passengers are assessed for eligibility and travel documents scrutinized – at enrolment 13 biometrics captured and subjected to background and routine checks against watch lists and database records – card is tested with passenger and card issued – passenger registered following successful background checks and maintained subject to successful routine checks.	
Description process	
Enrolled passengers arrive at an automated arrivals gate, their card is scanned, their biometrics taken from the chip in the card and verified against their fingerprint (1:1) to verify their identity. A check is also made against the core system to verify their registered traveller card is activated. If a match is not found the passenger is referred to manual processing.	
Additional information	
www.misense.org	
Content Updated:	25 January 2007

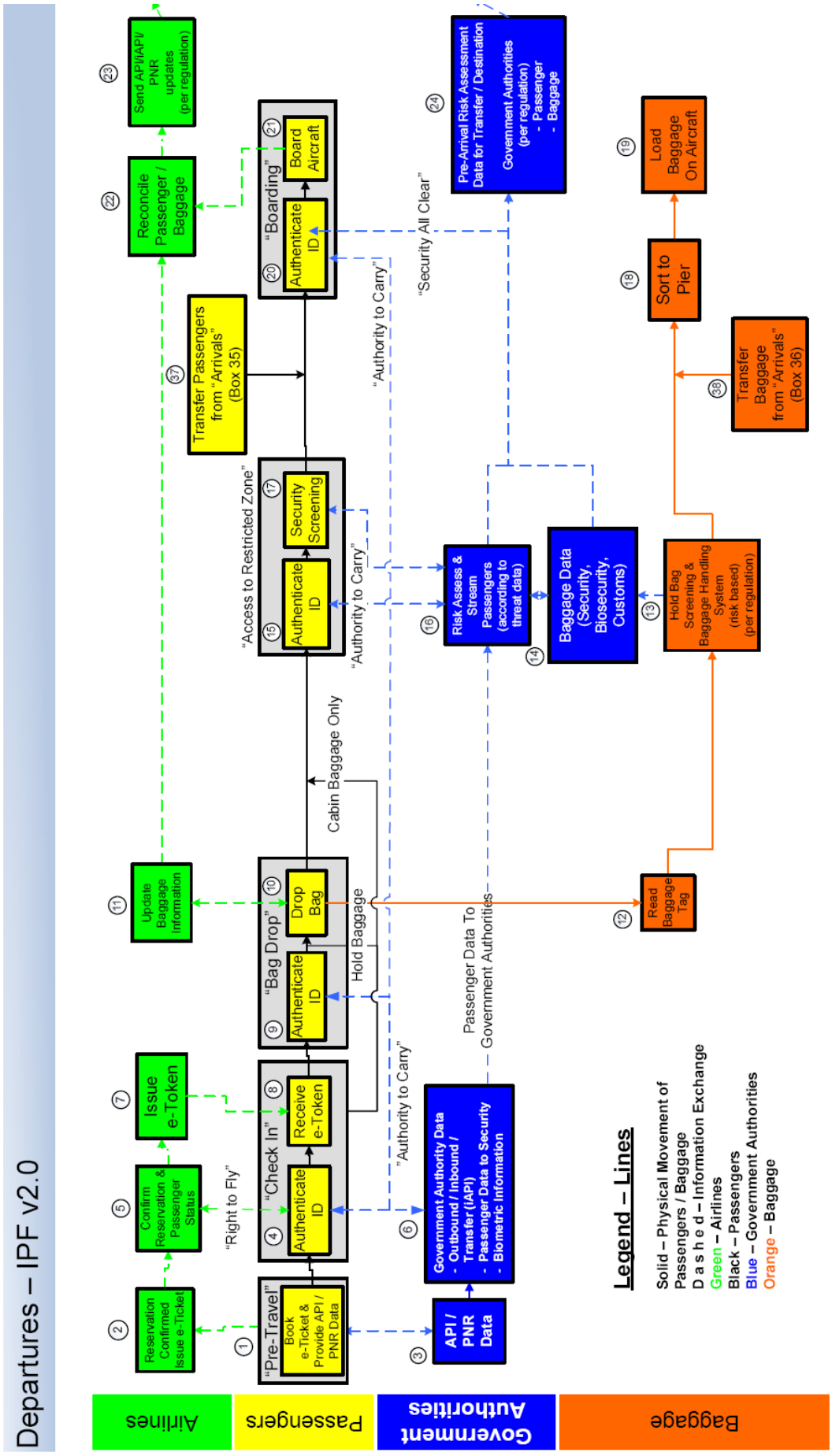
Annex C5: Features of ABG (Automatic Border Gate)

Location	Frankfurt Airport.
Introduction date	February 2004
ABC or semi ABC	ABC
Responsible authority	Bundespolizei (Federal Police of Germany)
Target group	EU Citizens, Swiss citizens
Fee	No
Enrolment centre	Frankfurt Airport
Entry control	Yes
Exit control	Yes
Biometric used	Iris
Token	Passports
Storage biometric	Database
Average process time	10-15 s
Performance & Security	Not reported
Description system	
The ABG system at Frankfurt Airport is based on OKI's IRISPASS iris recognition system. A key element in the ABG procedure is the machine-readable zone of the passport, which all travellers must have with them whenever they cross the border. The procedure is made up of two steps: Enrolment initial registration in the project and verification/automated control check when crossing the border.	
Description process	
Enrolment: Passengers wishing to enrol are asked to sign a statement of consent -declaring their voluntary participation. At the enrolment centre, Federal Police officers check to see whether the passport is genuine and valid. Passengers are allowed to enrol multiple passports. This is followed by a query of the INPOL police information system (German national system) and the Schengen Information System (SIS). If the passenger has no border police record, he/she will be asked to look into an iris recognition camera - four pictures are taken of each eye – which produces a biometric template. This is added to the passenger's personal data, encrypted and filed under his or her passport number in a local Federal Police database. In case of problems occurring during the enrolment process, the passengers are allowed to try to enrol not more than three times. The enrolment software also verifies the person has not been previously enrolled. After the enrolment process has been completed successfully, the passengers are given a statement describing their stored data and explaining how they will be used. No specific card is issued upon the enrolment since passengers are required to use their registered passport to enter the automated control lane. Enrolment takes on average 10 minutes. Enrolment is followed by a simulated border control check. **Verification:** To enter the automated border control lane, the passenger must place his passport on a document reader. If the passport is valid (the same travel document used for enrolment has to be used), the data from the MRZ will be transmitted electronically to the ABG database. If matching data are found in the database, the automatic doors to the control lane will open and the passenger's name, birth date and passport number will automatically be sent to INPOL/SIS to be checked. After passing through the doors, the passengers enter the inner control area where an iris recognition camera is located. When a passenger looks into the camera, a current template of the iris is generated, which is then compared to the enrolled template and filed in the local ABG database. Every two seconds an iris image is taken and processed with maximum time set to 20 seconds. If verification is successful and the passenger is not listed as a wanted person, he/she may cross the border. Otherwise, the passenger will be directed to a conventional border control booth.	
Additional information	
Frontex TR 1/2007 (BIOPASS - Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports)	
Content updated	August 2007

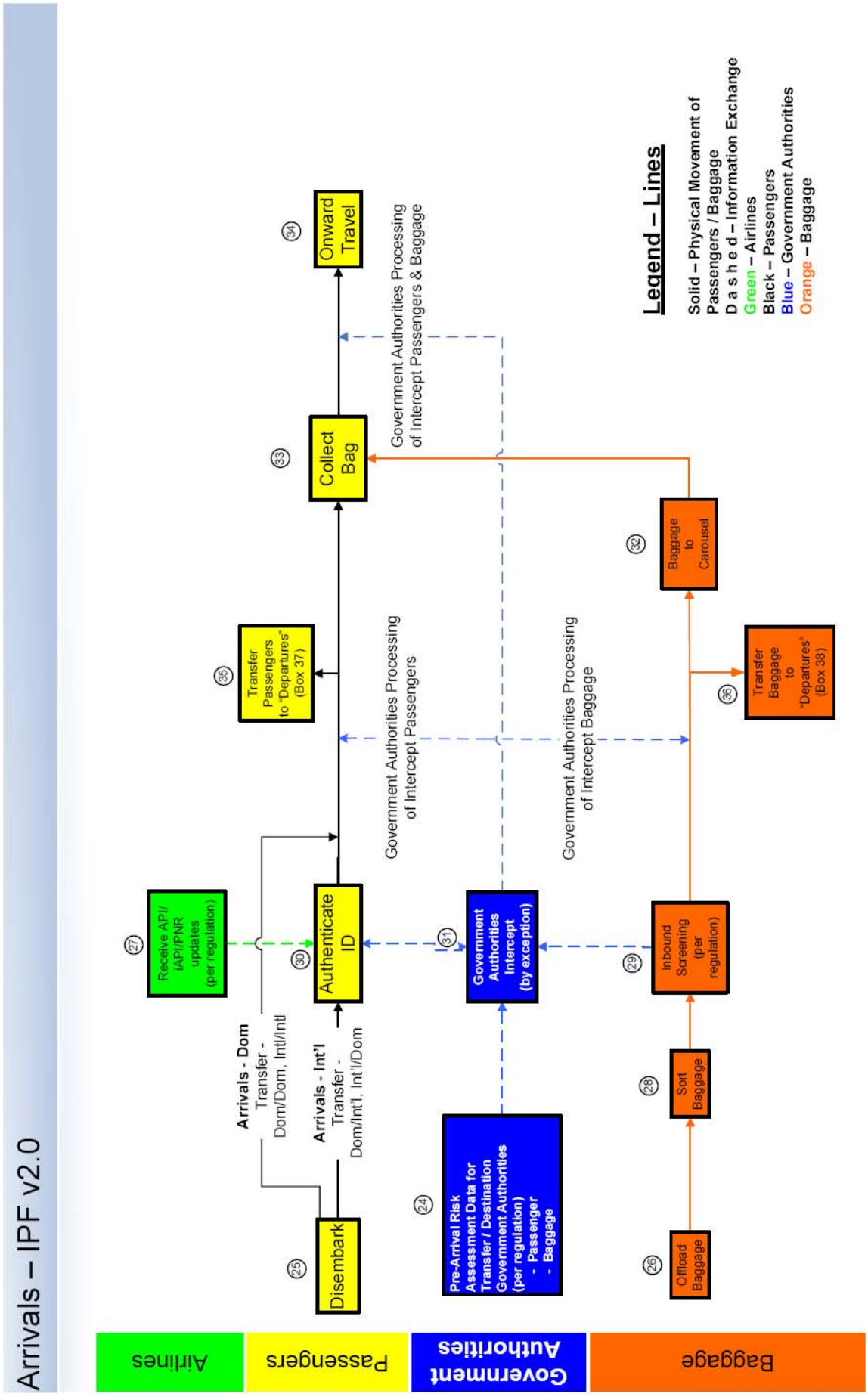
Annex C6: Features of PEGASE (Programme d'Experimentation d'une Gestion Automatisée et SEcurisée)

Location	Paris Charles de Gaulle Airport
Introduction date	June 2005
ABC or semi ABC	ABC
Responsible authority	DCPAF (Central Directorate of French Border Police)
Target group	EU citizens, Swiss citizens (mainly Air France frequent travellers)
Fee	No
Enrolment centre	Charles de Gaulle Airport
Entry control	Yes
Exit control	Yes
Biometric used	Fingerprint
Token	Smart Card
Storage biometric	Database
Average process time	12.5 seconds
Performance & Security	FRR 1.6% (biometrics), 3-6% (uniqueness test)
Description system	
The PEGASE system is based on fingerprints. At enrolment, prints of two fingers are taken. The templates are stored in a local database of the French Border Police at the CDG airport and at the time of automated border control the verification is performed. The system is using SAGEM technology.	
Description process	
Enrolment: During the enrolment biometric and passport data are captured, stored in a database and a contactless MiFare Smart Card is issued to the registering passengers. For data acquisition two fingerprints are scanned, preferably the two index fingers. Biometric data are used to derive minutiae templates and then the complete database is searched to locate potential dual identities of the same person. Before a passenger can participate in the PEGASE system a background check is performed. This check makes a lookup in the French database of searched persons. The same check is done twice a day against the list of enrolled PEGASE participants. Cards of people who match one of these lists are deactivated. The data from the MRZ of the passport together with the biometric data are stored in the database of the French Border Police at the CDG airport. Passengers wishing to participate in the PEGASE programme have to sign a registration form. The enrolment centre is equipped with a sample border crossing system and all passengers are given brief training on how to use the system. The overall process of the passenger enrolment takes 4 minutes and 35 seconds on average. In case of difficulties with the biometric enrolment, there is no upper limit of enrolment attempts. **Verification:** In the PEGASE system, the passenger first presents his or her smartcard to the contactless reader in front of the booth. If the booth is available and the passenger's card is active the door opens. The passenger's personal and biometric data are located in the database. The passenger's current biometric data are captured and verified against the two stored templates. If the match is not close enough, the passenger can re-try the biometric data capture, altogether 3 attempts within 30 seconds are allowed. If both the biometric verification and the unicity detection succeed the door opens and the passenger can proceed. If this is not the case the side door opens and the passenger proceeds to the immigration office. The average duration of the automated border check is 12.5 seconds. If the biometric verification does not succeed within 30 s the side door opens and the passenger must proceed to the classical border check. Even when using the automated border check the passenger is obliged to carry a valid passport, but this is not automatically verified.	
Additional information	
Frontex TR 1/2007 (BIOPASS - Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports) This is an earlier system which has been dismantled and will be replaced by a more advanced ABC solution (PARAFES) in CDG and other French airports.	
Content updated	August 2007

Annex D1: IATA SPTIG Ideal Process Flow V. 2.0 - Departures



Annex D2: IATA SPTIG Ideal Process Flow V. 2.0 - Arrivals



Annex E: PNR and API Data Categories

In the House of Lords European Union Committee, 15th Report of Session 2007-08, The Passenger Name Record (PNR) Framework Decision, Report with Evidence, published 11 June 2008 the following categories of PNR data have been defined:

- Data for all adult passengers:
  (1) PNR record locator
  (2) Date of reservation/issue of ticket
  (3) Date(s) of intended travel
  (4) Name(s)
  (5) Address and Contact information (telephone number, e-mail address)
  (6) All forms of payment information, including billing address
  (7) All travel itinerary for specific PNR
  (8) Frequent flyer information
  (9) Travel agency /Travel agent
  (10) Travel status of passenger including confirmations, check-in status, no show or go show information
  (11) Split/Divided PNR information
  (12) General remarks (excluding sensitive information)
  (13) Ticketing field information, including ticket number, date of ticket issuance and one way tickets, Automated Ticket Fare Quote fields
  (14) Seat number and other seat information
  (15) Code share information
  (16) All baggage information
  (17) Number and other names of travellers on PNR
  (18) Any collected API information
  (19) All historical changes to the PNR listed in numbers 1 to 18

- Categories of API data on the obligation of carriers to communicate passenger data:
  (1) Number and type of travel document used
  (2) Nationality
  (3) Full names
  (4) Date of birth
  (5) Border crossing point of entry into the territory of the Member States
  (6) Code of transport
  (7) Departure and arrival time of the transportation
  (8) Total number of passengers carried on that transport
  (9) Initial point of embarkation