



Centrum voor Wiskunde en Informatica

REPORT*RAPPORT*

PNA

Probability, Networks and Algorithms



Probability, Networks and Algorithms

BioVision: Roadmap for Biometrics In Europe to 2010

Astrid Albrecht, Michael Behrens, Tony Mansfield, Will McMeechan,
Marek Rejman-Greene (Editor), Mario Savastano, Philip Statham,
Christiane Schmidt, Ben Schouten, Martin Walsh.

REPORT PNA-E0303 DECEMBER 8, 2003

CWI is the National Research Institute for Mathematics and Computer Science. It is sponsored by the Netherlands Organization for Scientific Research (NWO).

CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics.

CWI's research has a theme-oriented structure and is grouped into four clusters. Listed below are the names of the clusters and in parentheses their acronyms.

Probability, Networks and Algorithms (PNA)

Software Engineering (SEN)

Modelling, Analysis and Simulation (MAS)

Information Systems (INS)

Copyright © 2003, Stichting Centrum voor Wiskunde en Informatica

P.O. Box 94079, 1090 GB Amsterdam (NL)

Kruislaan 413, 1098 SJ Amsterdam (NL)

Telephone +31 20 592 9333

Telefax +31 20 592 4199

ISSN 1386-3711

BioVision: Roadmap for Biometrics In Europe to 2010

ABSTRACT

This document is the first issue of the BIOVISION roadmap for the future of biometrics in Europe through to 2010. It offers a portfolio of techniques, viewpoints and scenarios to support future initiatives by national and European research organisations. A list of 38 prioritised research challenges forms the set of recommendations to the European Commission to support further R&D in these key technologies.

1998 ACM Computing Classification System: H.3.3.[Information Search and Retrieval]: Information Filtering,

H.3.4.[Systems and Software]: Performance Evaluation - Distributed Systems - User Profiles and Alert Services.

Keywords and Phrases: Biometrics, Databases, Data Protection, Identification, Image Recognition, Interfaces, Security

Note: This work was carried out under a EU FP5 project called BioVision, IST-2001-38236. Information Society Technologies.



BIOVISION

Roadmap for Biometrics in Europe to 2010

Project Number	IST-2001-38236
Project Title	BIOVISION Roadmap to Successful Deployments from the User and System Integrator Perspective
Deliverable Type	Document

Deliverable/Issue Number	D2.6 / Issue 1.1
	Issue date 15 October 2003
Title of the Deliverable	Final Report of the Roadmap Task
Work Package contributing to the Deliverable	WP 2
Authors	A. Albrecht (TTT); M. Behrens (UGF); T. Mansfield (NPL); W. McMeechan (Nationwide); M. Rejman-Greene (Editor, BT); M. Savastano (IBB), P. Statham (CESG); C. Schmidt (TTT); B. Schouten (CWI); M. Walsh (Daon).

Abstract:

This document is the first issue of the BIOVISION roadmap for the future of biometrics in Europe through to 2010. It offers a portfolio of techniques, viewpoints and scenarios to support future initiatives by national and European research organisations. A list of 38 prioritised research challenges forms the set of recommendations to the European Commission to support further R&D in these key technologies. Many of the recommendations look forward to the work programme of the European Biometric Forum.

About this document

Any enquiries about this document should be directed to:

Marek Rejman-Greene

Antares 2/6
BT Exact
Adastral Park
Martlesham Heath
Ipswich IP5 3RE
UK

marek.rejman-greene@bt.com

Document identity: Marek Rejman-Greene, *BIOVISION Roadmap Issue 1.1* (2003)

The most recent public version will be available at <http://www.eubiometricforum.com>

This Roadmap was funded by the European Commission under the Fifth Framework Information Society Technologies (IST) programme, project number IST-2001-38236.

Disclaimer

The information in this document is provided on an 'as is' basis, with no guarantee or warranty given or implied that the information is fit for a specific purpose. Users make use of any material at their own risk and liability; and it is strongly recommended that these resources should be used only as guidelines in the formation of an overall strategy. The views expressed are those of the authors and do not necessarily reflect those of the European Commission. All trademarks are acknowledged.

Copyright

This document should not be copied, reproduced or modified in whole or in part without first obtaining the written agreement of the BIOVISION consortium. If granted, the acknowledgement of the authors of the document and all applicable portions of this page should be clearly referenced.

History

1.0	28 August 2003	Version delivered to the Commission
1.1	15 Oct 2003	

Contents

ABOUT THIS DOCUMENT.....	2
CONTENTS	3
GUIDE TO THE ROADMAP.....	5
EXECUTIVE SUMMARY	6
THE BIOVISION CONSORTIUM	9
1. INTRODUCTION.....	10
1.1 INTRODUCTORY OVERVIEW OF BIOMETRIC METHODS AND THEIR APPLICATION	10
1.2 PERSONAL IDENTITY: IMPLICATION OF THE WIDESPREAD ADOPTION OF BIOMETRICS.....	14
1.3 BIOMETRIC METHODS - THE EUROPEAN SCENE.....	19
1.4 THE BIOVISION ROADMAP PROJECT	21
1.5 THE RELATIONSHIP TO OTHER ROADMAP PROJECTS.....	23
2. ROADMAPS AND ROADMAPPING.....	25
2.1 AN APPLICATION- AND USER-ORIENTED ROADMAP FOR EUROPEAN BIOMETRICS.....	25
2.2 ROADMAPPING - FROM CONCEPT TO IMPLEMENTATION.....	26
2.3 SUCCESSFUL ROADMAPS.....	28
2.4 THE ROADMAPPING PROCESS	28
2.5 THE BIOVISION ROADMAP – AN ALTERNATIVE VIEW	32
3. APPLICATIONS	34
3.1 MATCHING THE BIOMETRIC TECHNOLOGY AND THE APPLICATION.....	34
3.2 SPECIFIC APPLICATIONS - THE USE OF SCENARIO MODELLING	36
3.3 SPECIFIC APPLICATIONS: THE CASE OF PHYSICAL ACCESS CONTROL.....	37
3.4 SPECIFIC APPLICATIONS: FINANCIAL APPLICATION OF BIOMETRICS.....	44
3.5 SPECIFIC APPLICATIONS: MONITORING OF CROSS-BORDER TRAVEL.....	54
3.6 SYNERGIES WITH OTHER TECHNOLOGY DEVELOPMENTS.....	64
3.7 SOCIETAL AND TECHNOLOGICAL DRIVERS, INHIBITORS AND WILDCARDS.....	67
3.8 SYSTEM INTEGRATION CONSIDERATIONS.....	72
4. TECHNOLOGIES	82
4.0 ALTERNATIVE AUTHENTICATION TECHNOLOGIES.....	85
4.1 AUTOMATIC FACE RECOGNITION (AFR)	90
4.2 FINGERPRINT RECOGNITION.....	98
4.3 IRIS RECOGNITION.....	106
4.4 RETINAL SCANNING.....	110
4.5 HAND GEOMETRY.....	111
4.6 VEIN PATTERN.....	113
4.7 SPEAKER VERIFICATION.....	114
4.8 DYNAMIC SIGNATURE VERIFICATION/RECOGNITION (DSV/DSR)	117
4.9 KEYSTROKE DYNAMICS	121
4.10 OTHER BIOMETRIC METHODS UNDER DEVELOPMENT	123
4.11 MULTIPLE BIOMETRICS.....	127
4.12 FUTURE DEVELOPMENTS.....	129
5. CRITICAL ISSUES IN THE APPLICATION OF BIOMETRICS	131
5.1 END USER PERCEPTIONS.....	131
5.2 SECURITY.....	135
5.3 SAFETY AND MEDICAL ISSUES	137
5.4 FUTURE DIRECTIONS IN THE UNDERLYING TECHNOLOGIES AND APPLICATIONS.....	138
5.5 LEGAL AND REGULATORY DIMENSIONS.....	139
5.6 STANDARDISATION ACTIVITIES IN BIOMETRICS.....	142

6. THE IMMEDIATE OUTLOOK FOR THE APPLICATION OF BIOMETRICS.....	146
6.1 OVERVIEW.....	146
6.2 BIOMETRICS APPLIED TO IDENTITY AND IDENTITY DOCUMENTS.....	150
6.3 SECURE AIR TRAVEL THROUGH THE USE OF BIOMETRICS.....	157
6.4 E-HEALTH APPLICATIONS: BIOMETRICS AS A SERIES OF POINT SOLUTIONS?.....	162
6.5 USE OF BIOMETRICS BY THE FINANCIAL SECTOR.....	168
6.6 PHYSICAL ACCESS CONTROL AND 'TIME AND ATTENDANCE ' APPLICATIONS.....	171
6.7 CAR PERSONALISATION AND SECURITY.....	172
6.8 APPLICATIONS IN THE CRIMINAL JUSTICE SECTOR.....	172
6.9 ONLINE AUTHENTICATION FOR CONSUMERS AND EMPLOYEES.....	173
7. ADDRESSING THE CRITICAL ISSUES	176
7.1 CROSSING THE 'TECHNOLOGY CHASM'.....	176
7.2 FUTURE APPLICATIONS.....	177
7.3 WHAT ARE THE CRITICAL ISSUES?	178
7.4 THE EUROPEAN BIOMETRIC FORUM.....	180
APPENDIX 1: RESEARCH CHALLENGES	181
A1.1 US INITIATIVES IN DETERMINING A BIOMETRICS RESEARCH AGENDA.....	181
A1.2 THE BIOVISION RESEARCH AGENDA.....	183
APPENDIX 2: CURRENT BIOMETRIC R&D AND INNOVATION IN EUROPE	188
APPENDIX 3: RESEARCH PROJECTS IN BIOMETRICS	194
GLOSSARY: ACRONYMS AND VOCABULARY.....	197
ACRONYMS.....	197
VOCABULARY	198
DIAGRAMMATIC FORM OF A ROADMAP	202

GUIDE TO THE ROADMAP

BIOMETRICS and SYSTEMS USING BIOMETRICS

Introduction to biometrics from a systems perspective	1.1
System integration issues in design and deployment of biometric systems	3.8
Personal Identity - issues and viewpoints	1.2
Specific biometric technologies - now and in the future	4.1 to 4.10
Using more than one biometric	4.11
Alternatives to biometric methods	4.0
The future of biometrics - synergies with other technology developments	3.6.1
Critical issues in the deployment of biometrics (see also CHALLENGES)	7.3
Research issues in biometrics - recommendations for future work	App 1

ROADMAPS

Introduction to Roadmapping techniques	2
Specific features of the BIOVISION Roadmap	2.1
Scenario modelling as a technique for envisioning future developments	3.2
Impact of social, political and technological trends	3.7

APPLICATIONS USING BIOMETRICS

Matching application requirements with the capabilities of biometrics	3.1
Market outlook for biometrics – revenues from specific technologies	6.1
Listing of services that could make use of biometrics	6.1
The key application of Biometrics in 2004: passports with biometrics	6.2
International travel applications (air travel)	6.3
Long term view on identity cards and international travel	3.5
Physical access control - long term view	3.3
Online authentication opportunities	6.9
Applications in the financial sector - near term	6.5
Applications in the financial sector - longer term	3.4
e-Health and biometrics	6.4

CHALLENGES FACING THE ADOPTION OF BIOMETRICS

Adoption cycle of novel technologies	7.1
Issues of acceptability and usability for individual end users	5.1
System security concerns	5.2
Safety and the inference of medical conditions from biometric methods	5.3
The privacy, legal context and regulatory environment	5.5
Standardisation issues in the application of biometric methods	5.6
Design and systems integration considerations	3.8

THE WAY FORWARD

Research Challenges: recommendations for future research	App 1
Recommendations for biometrics use in passports and identity documents	6.2
The European Biometric Forum	7.4

CONTACTS AND FURTHER INFORMATION

References in the text	
The Editor and members of the BIOVISION consortium	Page 9
Reports from other projects using biometrics	App 3
Experts and specialists in European companies and university departments	App 2

TIMETABLE FOR FUTURE EDITIONS OF THE ROADMAP

Comments and suggestions for changes and amendments to Editor by ...	13 Nov 03
Amended version 1.2 available	30 Nov 03
European Roadmap workshop (UK)	23 Feb 04

Executive Summary

By enabling automatic identification – or automated confirmation of the identity of individuals – biometric methods offer a very wide range of opportunities for improving the convenience and security of computer-based systems.

Though there are mature applications in some domains – most notably for physical security and in the use of AFIS in criminal justice systems – the take-up has been slower than anticipated. Certain problems remain to be fully addressed and the market has exhibited significant fragmentation. However since the start of 2003, there has been substantial interest by the European Commission and governments both in the EU and USA - accompanied by a number of formal requests for proposals.

Over the past decade there have been numerous projects through which the biometric community has gained a more mature understanding of the possibilities – and the aspects that still remain to be addressed. In addition, both at the European and Member State level, we see numbers of key suppliers of biometric hardware and software, together with major research groups who are driving forward the technologies.

In preparation for the Sixth Framework of support for R&D in key technologies, the European Commission has asked for the compilation of Roadmaps to identify the critical challenges in key technologies. Biometrics has been identified as one such critical technology, and the BIOVISION consortium offers this Roadmap for consideration by the biometrics community, whether they be suppliers, implementers, researchers, ordinary end users, or other stakeholders such as the data protection commissioners interested in protecting users' privacy.

In contrast with many other technology-focussed roadmaps, the aim was to balance the understanding of developments in the technology with the potential applications that will make use of them. In particular, we were interested in those factors that will determine the success of future deployments, especially those in the European Union. Among these are the addressing of user concerns (whether these be related to privacy or medical implications); the security of devices and systems; legal and regulatory issues; and standardisation. We have reviewed the main biometric technologies from such perspectives. An overview of emerging techniques is qualified by an appreciation of the long process that a newly developed method has to undergo before it stands a chance of commercial acceptance.

The resulting Research Agenda (Appendix 1) with its list of 38 prioritised Research Challenges offers the biometrics community in Europe pointers to system level issues that require continued support at both national and cross-national levels if applications using biometrics are to be successfully deployed in the many areas that we have identified.

The underlying insight that informed our approach was that,

Biometric technologies should be viewed as mechanisms that address one aspect of an application. Whether the use of biometrics enhances or reduces personal privacy, improves or worsens security, makes authentication more or less convenient, will depend on other features of the application. This is no different from many other technologies. It follows, therefore, that discussion of biometric performance, legality or usability should be in the context of a specific application. Moreover, the value of biometric methods - in improving security, convenience, etc - should be judged from the perspective of operators of services using these methods, and from the experience of the end users of such services.

We have considered both government and privately managed applications using biometrics. However, during the 14 months of this study, there have been major initiatives that have transformed the outlook for biometrics in Europe:

- An ISO committee has been established and has already made very significant progress in the development of standards in biometrics. (For many years the lack of standards has been offered as a reason for the low take-up of biometrics.) The BIOVISION team was actively involved in this standards committee, notably ensuring that a further study group was convened to ensure that cross-jurisdictional and societal aspects are taken account of in deployments. In view of the complexity of the issues, we have recommended that the European Commission (or an alternative pan-European group such as the European Biometric Forum) act to disseminate the knowledge on the development of these standards amongst all relevant national bodies in the EU.
- The US has ratified the Enhanced Border Security Act¹ requiring the use of biometrics in passports from late 2004 for those countries that take advantage of the Visa Waiver programme. ICAO has determined the technical requirements for such use of biometrics. In response to the US proposals, a measure of co-ordination amongst European member states has started, although there appear to be no formal plans for a reciprocal requirement for citizens of non-European countries to use such passports on entry into the EU.
- There has also been increasing interest in securing national identity and health insurance cards, with many non-European countries planning to use biometrics. The UK, one of the few member states without an identity card, has undertaken both public consultation and feasibility studies on a card that is backed by a national biometrics database. The acceptance by citizens of these initiatives will depend on how governments respond to issues such as the protection of personal privacy and compromise by poor security designs. (The work of the BIOVISION team in developing a first draft of the Best Practices on privacy and a comprehensive inventory of security issues mark a significant contribution in these directions.) Furthermore, failure to respond adequately to the concerns of users in these deployments could put back public acceptance of commercial implementations. However, sensitively introduced implementations - with first class user interfaces - will encourage the more extensive use of biometrics in everyday life. There is evidence that citizens are willing to accept such use for the common good, provided that adequate safeguards are in place against abuse and failures in the system. However, relatively little is known about those who cannot use these systems, through the lack of a critical body feature (finger or iris), a disability or infirmity, medical conditions such as obsessive-compulsive disorders or even a culturally determined fear. It is clear that the aggressive timescales of the passport initiative may not allow sufficient time for an adequate development of such sensitively designed systems. Citizens and their representatives need to participate in an informed debate on their introduction and use, in order to ensure that such systems serve the people. The BIOVISION consortium has been in the forefront of developing methods of ascertaining which issues are crucial to the acceptance of biometrics by the population at large.

In contrast to these large-scale deployments by national governments, the private sector has not advanced significantly over the past year. Clearly, if identity cards using biometrics are issued, financial organisations and employers will consider ways of making use of them. This would require that sufficient legal, technical and procedural measures are in place to ensure that the user's trust is not abused. The greater danger is if similar cards were introduced without the safeguards that citizens can expect from government identity cards. In a globalised world, there are many states that have no adequate protection for the individual, and consumers could be unaware that their

¹ Enhanced Border Security and Visa Reform Act 2002

biometric (and other personal) data might be extracted in insecurely designed systems. One further concern that has been voiced is that such data might yield information about the user's medical status, and a methodology has been developed in the BIOVISION project to ascertain the possibility of such inference. For these reasons, private organisations may choose to introduce biometrics first in the 'back offices', gaining experience in their use in a controlled environment, before progressing towards application in services for the consumer.

The BIOVISION consortium has examined three specific application areas from both a long (2006-10) and nearer (2003-5) term perspective: the use of biometrics for physical access control (and 'time and attendance'), their application in travel and identity documents, and the potential for their use by financial institutions. Other sectors have been viewed from just one time horizon: near term assessments of the way in which these methods are likely to be applied for e-Health, car travel and on-line authentication. Together these snapshots will enable the reader to note recurrent themes that should apply to the successful deployment of biometrics in other sectors and time horizons.

There have been many research projects in this field that have enabled the participants to gain a better understanding of the algorithms and sensor aspects. The research field has recognised the limitations of single conventional biometric methods and substantial work is underway to use multi-modal and multi-classifier systems, modelling features such as the face in three dimensions and using intelligent agents. However, relatively little effort has been devoted to fundamental work on cross-cutting issues such as design methodologies that take account of the particular aspects of biometric deployments. Future research projects should therefore address this imbalance, so as to ensure that these issues are considered and that the results of the research are communicated to the rest of the biometric community in a clear way.

This Roadmap is one of a set of documents that represent a comprehensive viewpoint on issues in the deployment and use of biometrics in Europe. The principal supporting materials are:

- Best Practices in Privacy in Biometrics (Draft 1.0)
- *Report on end-user perceptions*
- *Technology and application issues for biometric identification systems*
- List of Research Challenges facing European biometrics community (Appendix 1 of this roadmap)
- A database of projects and deployments

The BIOVISION consortium, recognising the need for a body that will bring together the fragmented biometrics community in Europe, launched the **European Biometric Forum** in July 2003, initially headquartered in Dublin. The EBF will work towards the resolution of many of the recommendations of this Roadmap, alongside existing groups such as the Association for Biometrics and with the support of other national and regional bodies. All participants in biometrics-related activities in Europe are encouraged to join the Forum and involve themselves actively in the EBF's initiatives.

Note:

The BIOVISION members are interested in receiving suggestions from the biometric community, whether in the EU or elsewhere, for additions or alterations to the Roadmap. An interim update of the Roadmap will be published in November 2003, taking into account any comments and corrections received by 13 November. A workshop is planned for 23 February 2004 in the UK, after which it is envisaged that a second issue will be distributed.

THE BIOVISION CONSORTIUM

The Consortium consists of the following principal partners:

Theme, organisation and contact	Country
Joint co-ordination, roadmap structure and editing, system integration, standardisation and socio-technical design BT Exact, the research, development and consulting arm of BT Marek Rejman-Greene, marek.rejman-greene@bt.com	UK
Joint co-ordination, legal and regulatory issues Daon, an Irish identity management solution provider Martin Walsh, martin.walsh@daon.com	Ireland
Security CESG, Communications-Electronics Security Group Philip Statham, philip.statham@cesg.gsi.gov.uk	UK
Security and testing NPL, National Physical Laboratory Dr. Tony Mansfield, tony.mansfield@npl.co.uk	UK
Medical and safety dimensions IBB, Institute of Bio-structure and Bio-images - CNR, National Research Council of Italy Mario Savastano, mario.savastano@unina.it	Italy
Technology and applications CWI, Centre for Mathematics and Computer Science Dr. Ben Schouten, bens@cw.nl	Netherlands
Technology and applications, university research University of Applied Sciences, Giessen-Friedberg Professor Michael Behrens, michaelbehrens@compuserve.com	Germany
User perspectives Nationwide Building Society, a major financial institution in the UK Will McMeechan, will.mcmeechan@nationwide.co.uk	UK
User perspectives and legal and regulatory issues TeleTrust, a German association set up to promote information security in an open systems environment, with the main focus on cryptography and biometrics Dr. Christiane Schmidt, csc@softpro.de ; Dr. Astrid Albrecht AAlbrechtLaw@aol.com	Germany

Other members of the consortium include:

- Avanti: Julian Ashbourn (UK)
- Dr Angela Sasse (UK)
- B&L Management Consulting (Germany)

A number of specialist groups are also involved: the Association for Biometrics (www.afb.org.uk) and the Dutch Biometric Forum.

1. Introduction

1.1 Introductory overview of biometric methods and their application

Biometric methods relate to the **authentication** of living individuals in three ways:

- **verification** of identity, confirming that you are who you claim to be; such claims including entry of a user name or presentation of a token (e.g. a smart card) issued to a person;
- **identification**, the system recognising a person by their characteristic being the closest match to a person on a master database of such characteristics;
- **non-identification**², checking that a user has not been previously enrolled into a database.

These methods are conventionally segmented into two main types:

1. Physiological methods that are under no (or very limited) control of the subject. These include the most widely used techniques, such as fingerprint verification, iris recognition and automatic face recognition.
2. Behavioural techniques, that allow a greater degree of freedom to the individual. Such techniques include speaker recognition and dynamic signature verification (DSV),

although it is acknowledged that there is a degree of overlap between these groups that makes it difficult to demarcate an absolute division between these categories.

Even though biometric methods are generally positioned as security mechanisms, their **application in other areas** should not be forgotten. Their use in personalisation or customisation of user interfaces or services directed at a specific individual is one case in point. Biometric methods can also be used to improve internal business processes, for example, as in the initial deployment of signature verification by the UK's Nationwide Building Society. Facial recognition techniques from the biometric industry are also being used by the police service in the UK to sort through the numerous Internet images of the victims of paedophiles obtained during the course of investigations.

The use of fingerprint (AFIS) or facial images in 'scene of crime' and forensic activities is allied to the application of such methods in more conventional services and we shall occasionally make reference to these in this report.

Nevertheless, when considering the use of biometric methods as a means of authenticating an individual, we should be aware of the **alternatives to the use of biometrics**:

1. Authentication by demonstration of knowledge of a secret known only to the individual (e.g. PINs - Personal Identification Numbers, such as the 4-figure PIN used in automatic cash dispensers in some countries, passwords or recognition by the individual of a group of pre-memorised faces from a selection offered at the time of authentication);
2. Identity by possession and use of a unique, unalterable token held by the individual, such as a smart card with a personal identifier securely stored in its chip.
3. Proof by presence at a specific geographical position, such as that offered by caller identification in telephony.

For each biometric method (e.g. speaker verification, facial recognition, etc.), there are a number of **different implementations**. These may use different sensors; each will certainly use different algorithms to process the signals captured by the sensor; and the

² Or 'negative identification'

interface presented to the individuals being authenticated will vary between implementations. In addition, performance will depend to a large extent on the way the biometric is deployed in a specific application or service. Therefore, it makes little sense to compare the performance of biometric methods in general (e.g. fingerprint against facial recognition), as is often done in introductory articles on biometrics. .

A single biometric may not offer the performance or other capabilities that a customer requires. In some cases, this can be supplemented by one of the alternative methods mentioned above, or **multiple biometrics** can be employed, requiring the capture of more than one characteristic either sequentially (e.g. a fingerprint recognition followed by a spoken password) or in parallel. An example of the latter is the imaging of the face and iris at the same time using a dual function camera.

Almost all systems using a biometric require an initial **enrolment** stage, when an individual is registered to the system. In many cases, this enrolment will be supervised by an official who has been trained in the use of the biometric and the way in which it will be utilised in a specific application. This stage may involve confirmation of the identity of the individual through presentation of trustworthy documentation (a passport, identity card or driving licence) and/or through corroboration of identity by a trusted individual. During enrolment, a number of biometric images or samples of data from a biometric reader will be obtained, from which a compressed or simplified dataset - termed the (reference) **template** - is derived. This template, which in commercial implementations ranges in size from 9 bytes to many kilobytes, is designed to extract features from the image or data sample that are most characteristic of individuals, since it will be used as the standard representation of the person's biometric in subsequent operation. Note that the quality of the template is of paramount importance in assuring the optimal performance of the biometric method in subsequent, operational uses. Many systems set a **quality threshold** to enforce a repeat enrolment should the images or processing fail to provide a sufficiently good template. However, a significant proportion of the population may be unable to make use of a biometric at all, and this **failure to enrol rate** is an important limitation on the application of biometric systems. Storage of the template can be either in a central database, on a local terminal or on a token held by the individual. The selection of storage medium will depend on security requirements, costs, user expectations, etc.

In **operation**, the enrolled individual presents their biometric to a sensor, which captures the signal and processes it using an (often) proprietary **algorithm** into a form that allows comparison with the reference template³; this is retrieved from its stored form to make the comparison. Since a person's submission of a biometric to a sensor is subject to variability (e.g. marginally different positioning of a finger on a fingerprint reader, changes in orientation of a face in front of a camera, or suffering a viral infection to affect the performance of a speaker recognition system⁴), it will be rare for a perfect match to be made with the template. One of the key determinants in the successful operation of a biometric enabled system is the setting of the **threshold** for acceptable **matching** of the two signals. Demanding too close a match risks **false rejection** of the enrolled individual, while widening the tolerance allows the possibility of **false acceptance** by someone with a similar template. **Testing** of a prototype system under conditions similar to the proposed deployment is often a prerequisite for a successful application - with tests being a realistic preview of the performance in the field provided that the subject population is representative of the end user group (both in demographics and in motivation) and that sufficient numbers are tested over a sufficiently long period.

Should a person be unable to enrol, or to operate a biometric method during normal operation, provision should be made for an alternative or **fall-back system**. On grounds

³ A few writers use the term 'request template' for the signal processed during the operation of a biometric, which is then compared with the (reference) template.

⁴ Indeed, there are many other causes of short term changes in the individual.

of cost, this may be an automatically operated application, although for reasons of security or convenience, manual fall-back may be the preferred option.

In spite of the discussion so far, it is vital to recognise that biometric technologies should be viewed as mechanisms that address one aspect of an application. Whether the use of biometrics enhances or reduces personal privacy, improves or worsens security, makes authentication more or less convenient, will depend on other features of the application. This is no different from many other technologies. It follows, therefore, that discussion of biometric performance, legality or usability should be in the context of a specific application. Moreover, the value of biometric methods - in improving security, convenience, etc - should be judged from the perspective of operators of services using these methods, and from the experience of the end users of such services.

The classification of **applications** can be considered in a number of ways. AFNOR, the French national standards body, has proposed four classes of service based upon the performance requirements of the technology:

- Class 1 (verification of identity) - against the prior issues of a card or token
- Class 2 (authorisation of privilege) - access to benefits
- Class 3 (proof of uniqueness) - search through a database to ensure that the person has not been previously enrolled, using the non-identification approach
- Class 4 (identity search) - search through a database for a match to data from an unknown person (e.g. criminal AFIS system)

Alternatively, the classification can be viewed from the benefit to the end user or operator - a choice that has been made by the BIOVISION group:

- Authentication of identity
 - For access control (physical or logical)
 - For authentication of a transaction (online or offline)
- Personalisation (physical or logical)
- Authorisation
 - Tracking (identity known or unknown)
 - Tracing (identity known or unknown)

System developers should be aware that **requirements capture** and system definition for biometric-enabled systems are more time-consuming and expensive activities than for most other IT systems. For example, biometric subsystems are often not designed with security in mind, and systems integrators will need to address the **security** requirements of the deployed application in this light. User perceptions (such as any fears and concerns of a significant segment of the user population) need also to be addressed as early as possible in the design process, to ensure that appropriate mechanisms are in place to reassure such users. The concerns may relate to **privacy** or to **safety** issues, which may be addressed in part through **legal and regulatory** measures. Biometric methods are unusual as an IT component in that, in general, they require the motivated co-operation of the individual if they are to work in an optimal way. Any impediment to ease of use - whether technical, social or psychological in nature - will detract from the successful operation of systems using biometrics. On the other hand, use of a biometric can be privacy-enhancing, e.g. by securing access to databases of sensitive material in a more secure and accountable manner.

One particular biometric technology often causing concern is fingerprinting. Some users wish to be assured that it will be difficult for the police authorities to make use of templates stored in other applications, so as to match them with the records in criminal fingerprint databases. The biometrics industry has for many years relied on the statement that the original images cannot be reconstructed from the templates. Although this is correct, it is also possible for many fingerprint biometric systems to offer *some* data to

help in cross-matching to law enforcement databases⁵. For the foreseeable future however, the opportunities for such cross-application transfer of data will be very limited indeed, even though systems could be designed to improve such interoperability.

Designers need also to be aware of the current international efforts in **standardisation** of APIs, protocols for the exchange of images or templates, security etc.

This short overview of the key aspects relating to the successful design, deployment and operation of systems and services using a biometric method highlights many of the issues that are explored in more depth in this roadmap. Even though the first method was developed more than four decades ago, the industry is still in its infancy, both in size and in maturity. There are relatively few centres of expertise in spite of the entry of numerous consultants eager to capitalise on the response to the events of September 11th 2001. For a naïve designer, it can appear temptingly obvious to use an 'off the shelf' solution from the supplier of a biometric sensor, buy in an algorithm from another source, conduct a few in house trials and proceed to deployment in order to meet an urgent requirement from a customer – and at minimal cost. This approach may carry a low risk when the numbers of users are small and the biometric is used in a controlled way, but a failure of a large scale system through inadequate investment could damage the prospects for other deployments. A recent example is the continuing debate following the attempt to use automatic face recognition in the 2001 Super Bowl final without any prior warning to the fans.

This should not detract from the large number of successful deployments, with many smaller scale systems in daily operation throughout the world. Access control to buildings, authentication to computers and electronic networks and the recording of time-and-attendance on the factory floor are the prime examples of their use. A few larger scale systems have also been reported, most notably in the welfare benefits programmes of individual states in the US, predominantly using AFIS-type systems, with others such as Massachusetts making use of facial recognition. Identity systems addressing the needs of governments and social security programmes have also been deployed - in the main in developing countries - and with little published material relating to their performance and cost effectiveness. A very long standing example of a successful system is the distribution of pensions to 1.2 million pensioners and their dependants in South Africa, using fingerprint readers on armoured vans. In operation since 1990, this deployment demonstrates that systems can be built that work with non-optimal subject populations.

Throughout the roadmap, we shall be highlighting the research challenges that need to be addressed, especially in the context of application in the European Union. These will be identified as follows, with a collated list appended at the end of this report.

RC/SD1 RC - SYSTEMS and DESIGN 1: Successful implementation of systems using biometric methods requires an inter-disciplinary design approach. There are few specialist designers able to put together an integrated design that addresses the already documented issues and concerns.

RC/Dep RC - DEPLOYMENTS 1: The impact of a high profile failure in the application of a biometric method could impact on the willingness of other customers to specify such methods, and adverse media comment could increase the resistance to their use by individuals and groups.

⁵ Manfred Bromba, *On the reconstruction of biometric raw data from template data*, <http://manfred.bromba.bei.t-online.de/biometrics/temppriv.htm> (July 2003)

1.2 Personal identity: implication of the widespread adoption of biometrics

1.2.1 Biometrics: a new technology

The introduction of a new technology can have significant unforeseen impacts upon society. Looking back from 2003, the centenary year of the commercialisation of the motor car, it is clear that the impact on social mobility, on global warming and on noise pollution could hardly have been foreseen by those early pioneers. In the 1950's, we note the assertion that the market for computers would be in single or double figures; today, we are still to understand the impact of the PC on society - either through the displacement of millions of clerical jobs or the increased connectivity of peoples in the virtual world of the Internet.

In the eyes of some writers, biometric technologies could turn out to be just as radical in transforming societies. Accordingly, in their view, large scale deployments need to be examined carefully (and even regulated). Even though this may wildly overstate the case, we should consider the impact of the widespread use of these methods in the light of technical developments in complementary fields such as data mining, intelligent CCTV and pervasive computing.

1.2.2 Identity and Authentication

The concept of identity can be approached from a number of standpoints: for example, we can view it from philosophical, psychological, sociological, legal and technical perspectives. It is not our aim to pursue any of these in detail, but it is important to recognise that naïve interpretations of this multi-faceted concept could result in poorly configured systems that do not address the fundamental opportunity or problem. Furthermore, systems could be over-bearing in their complexity or requirements on the capabilities of the individual. Of even more concern are possible unforeseen long term consequences of fixing identities, and the impact of such fixeness if identities are reused beyond the domain of which the individual was aware (resulting from so called 'function creep').

In her review of the literature on roles and identities as applied to new ICT technologies, especially in relation to online activities and Ambient Intelligence, Rebecca Ellis of the University of Essex comments that there is a lack of an agreed definition of identity in this context⁶. Specifically, there is a debate contrasting 'having' an identity, with the expression of that identity through actions that are performed by an individual. In the past, an identity was often thought of in the context of social categories – gender, class, ethnicity, sexuality – to define an authentic self which would differentiate an individual from others in society. Postmodern authors challenge this fixedness, offering a view of identity as 'a multiple, interwoven and hybrid thing, part of a process of reflection on who we are and how we experience the world from our social position'. From such a viewpoint, authentication of identity presents new challenges, and attempts to fix on a single identity for many applications (especially in government-controlled services) can lead to concerns that can be difficult for individuals to articulate confidently, and hence are often reduced to statements about reduction of personal privacy.

However, to start our analysis of identity, we will follow the discussion and definitions offered in a recent analysis of authentication schemes, which identified some of the unintended consequences for individual human rights, especially those relating to

⁶ Ed. Rebecca Ellis, *Roles and Identities – Review and identification of the state of the art*, EURESCOM project PROFIT P1302 (May 2003) http://www.eurescom.de/public/projects/P1300-series/p1302/P1302_portal.asp#P1302%20Deliverable%201

personal privacy⁷. Within this simplified view, identity relates to the individual human being and the ways in which attributes of individuals are used by others in their environment to distinguish one from another. Of course, this view also acknowledges a person has a separate self-identity that may – in certain exceptional cases – be at variance from those attributes perceived and used by others, including government entities that determine the rights and obligations of that individual to the rest of society.

From this perspective, the **Identity** of a person is the set of data about that individual which is associated with that person *in the context of a system* that requires knowledge of the distinctiveness of individuals.

The individual is describable by other people or systems in terms of

- **Identifiers**: pointers to a person; for example, a personal name or an identity card number.
- **Attributes**: describing a property associated with the individual; e.g. height, hair colour or role in an organisation. Some attributes are observable, while others require the individual or other entity to divulge relevant information.

Key concepts in this context⁸ are:

- **Identification** refers to the process of using claimed or observed attributes to infer the identity of the individual.
- **Authentication** is the process of establishing confidence in the truth of a claim.
- An **Authenticator** is evidence that is presented to support the authentication of a claim. For example, a passport could be an authenticator for the particular individual's name – his identifier. Knowledge of a password or the iris pattern in the eye are other types of authenticators for the same identifier.
- **Authorisation** determines what an individual is permitted to do. Often, this is brought together with authentication, as in physical access control using fingerprint biometrics.

The complexity of authentication is evidenced by the following distinguishable processes:

- **identity authentication** establishes that an identifier refers to an identity (not necessarily to an individual) to an understood level of confidence. An email address shared by a family might need to be authenticated, but would not necessarily relate to a single individual. Each member of the family could share the authenticator (e.g. knowledge of the password that is bound to the email address)
- **individual authentication of an identifier** (or 'verification' in the biometric literature) establishes an understandable level of confidence that the identifier refers to a particular individual. The person has first to claim an identifier ('I am John Smith'); then, the system (which could be another person) uses an authenticator (e.g. a passport) to authenticate the individual's claim to the defined confidence level.
- **attribute authentication** establishes that an attribute applies to a particular individual – to an understood level of confidence. In such a process, the attribute is selected first, followed either i) by direct observation of the attribute (if accessible) or ii) by challenging the person to produce an authenticator that supports the claim that the attribute refers to him.

⁷ Stephen Kent and Lynette Millet, Editors for the Committee on Authentication Technologies and Their Privacy Implications, *Who goes there? Authentication through the lens of privacy*, National Academies Press (2003) at <http://www.nap.edu/books/0309088968/html/>

⁸ Note that the vocabulary in use for biometric applications (as noted in the Vocabulary section) differs from this terminology.

Note that in each case, the assurance of correct authentication is limited, whether by technical factors (such as inherent FAR/FRR performance limits of biometric systems or by the resistance to duplication of cards and tokens) or by social norms such as issue of 'breeder' documents such as birth certificates on demand - not just to the data subject.

Stronger authentication, e.g. using biometric methods, can be a component of excellent privacy-protecting systems, providing a higher level of assurance that only correctly authenticated and authorised persons are allowed access to databases of personal information. Secure integration with alarm systems and usable audit trails is required.

Nevertheless, the discussion on the use of more widespread strong authentication centres on apparent trade-offs between the higher security that could be realised and the increased risks to personal privacy that might result. An apparently logically consistent solution to several societal problems (such as identity theft) is for universally recognised single identifiers to be used together with a restricted range of attributes and attribute authenticators whenever an activity or transaction merits strong authentication. Many cultures, especially those that place a higher value on the rights of the individual over those of society, take the view that the risks inherent in such an apparently simple solution outweigh the potential for harm; these cultures place limitations on the power of government or commercial organisations to insist upon the use of such a limited data set. These limitations take the form of constitutional rights and legal protection for personal data. In this way, individuals feel able to express dissent, to take part in legitimate political activities and engage in lawful actions without fear of being tracked (regardless of whether such fears are justified), allowing them to choose to use one of a number of identities - or none at all when this is appropriate.

Of course, many systems suffer from inherent vulnerabilities that could be exploited by criminal elements, or by individuals refusing to accept responsibility by repudiating transactions or refusing to be held accountable for their actions. In some cases, these vulnerabilities could be addressed by stronger authentication. However, in many other situations, such improvements in identification may offer transient benefits (through deterrence) or fail to address the real challenges. The trade-off between personal privacy and improved security is not always obvious, especially when an authentication scheme can be reused in widely differing environments. The debate on the right balance requires an understanding of the issues and the technical capabilities of novel technologies such as biometrics. The BIOVISION Roadmap and the results of associated studies offer a set of resources in this debate⁹.

1.2.3 A world of single identities

The perceived danger is not from a single sector in which biometric methods are applied, but in the interoperation of many identity management systems. A measure of protection against the homogenisation of identity across every aspect of an individual's life is offered by the existence of at least six principal biometric methods, each of which can be implemented in a number of ways.

Notwithstanding such diversity, for these commentators, it is the possibility of defining a single, unique identity for every citizen that causes greatest concern, and the 'function creep' that could propagate its use into every aspect of a person's life. Even though many developed countries have unique (non-biometric) identifiers for their population (even in the USA, there is a Social Security Number), legal limitations in their use across government - and by the private sector - have restricted their benefit. More prosaically, the diversity of IT architectures in use by governments is often the limiting factor in the linkage of data about a person between tax authorities, social security systems, health

⁹ A detailed research agenda for privacy and identity management is a deliverable from the European Commission funded RAPID project. Miriam Lips *et al*, *Roadmap for socio-cultural and economic research in privacy and identity management*, (Deliverable ST 2.3.2, 13 December 2002). <http://www.ra-pid.org/>

records and financial institutions. Clearly, this perpetuates the opportunities for fraud both against government agencies and against other individuals in society. The lack of fixed identity may no longer be defensible for a world of mass travel and e-commerce. Such demands for secure identities may find parallels with the 19th century. As the population of cities grew exponentially, authorities responded by official registrations of births and deaths, insistence on the use of surnames and the development of fingerprint systems to identify criminals.

Yet, a level of inefficiency reassures a part of the population that distrusts the motives of 'big' government and politicians. It may allow greater freedom for dissenting voices while entrepreneurs (whether commercial or social) are left with greater opportunity to experiment, especially at the margins of the legal or socially acceptable. The balance between such conflicting views can only be resolved by debate within each society. The possible application of biometrics adds another dimension to this discussion, requiring a clear appreciation of the operation and limitations of these technologies.

At the start of the 21st century, for many people, theirs is no longer an integrated identity. Their personas at work, in their family life, in their choice of friends, and their use of the Internet may be very different, and may also change as they move through successive stages in their lives. Perceived attempts to fix a single identity may be behind some of the unease that is expressed about biometrics, and which is often expressed in the shorthand of 'fear about loss of privacy'. In the UK, for example, citizens are allowed to change their name without the need to register it formally – provided that there is no attempt to deceive or engage in fraud¹⁰. There are valid reasons for a person wanting to change their identity, and the power of an organisation to stop such a change is open to philosophical enquiry. Discussion about the merits of the introduction of biometrics needs to take account of such views since most biometric-enabled systems require the co-operation of users, and the unwillingness of significant minorities to engage with new services risks their complete failure.

Haralambos and Holborn¹¹ have reviewed key papers in the recent sociological literature on identity. They note a progressive change from a pre-modern view of the lack of individual identity – a human being just one part of God's 'chain of being' – through to the post-modern concepts of fractured identities. Stuart Hall¹², for example, identifies intermediate stages of the Enlightenment view of the indivisible individual, building on the philosophical dualism of Descartes and the later, modernist approach of the 19th century recognising the social framing of identity: a person reflects their concept of themselves through the reactions of their immediate social groups. In a post-modern world, it is no longer possible to determine one's identity in the context of a *single* social group. Numerous factors have affected this change: the growth of a surveillance society, the rapid globalisation of societies and the economy, the impact of the feminist movement and the rise of the 'green' political awareness. Harriet Bradley¹³ refers to the element of choice in the selection of identities and emphasises their dynamic nature. What defines us as individuals is our difference from others, and that difference is an ever-changing response to those around us. This situational, dynamic view of identity needs to be borne in mind as we examine the opportunities offered by biometrics to fix identity in the context of one or more applications. By fixing identity and using biometrics to confirm that single identity in daily transactions, we may be changing society in unpredictable ways.

Action: More fundamental research is needed (in line with the recommendation RC/TTL2 below) to address the issues of multiple identities and personas. In addition, studies

¹⁰ This is not the case for some other EU countries, notably Germany.

¹¹ Michael Haralambos et al, *Sociology: Themes and Perspectives*, Fifth Edition, Collins pp 922-933 (2000)

¹² S Hall and P du Gay, eds, *Questions of Cultural Identity* Sage (1996)

¹³ H Bradley, *Fractured Identities: Changing Patterns of Inequality*, Polity Press (1997)

should be undertaken that examine the impact of simultaneously deploying systems using biometrics.

1.2.4 Other concerns

Among the other concerns that have exercised commentators on biometrics, the most prominent in the context of large-scale application appear to be¹⁴:

1. That the solution employing a biometric does not address the real problem, merely offering a technical fix that placates calls for political or commercial action. Many authentication problems arise from poor registration procedures, or from systems that were designed for other purposes.
Action: Development of requirements capture methodologies similar to those described in Section 3.8.
2. The cost of a secure, usable and robust biometric solution may far outweigh the benefits that it is supposed to offer. Costs may be understated, especially in the areas of enrolment and maintenance. The performance of the systems may be inadequate to ensure the required operational effectiveness.
Action: Collation of experience and lessons learnt on the true costs of systems. Research on economic models of security systems. An approach to cost-benefit analysis of systems using biometrics has been outlined in a BIOVISION paper¹⁵.
3. Dehumanising of individuals by reduction of their identities to numerical entities in a database.
Action: The recommendation below (RC/TTL1) proposes the investigation of alternative ethical frameworks to assess the issues that are inherent in this fear.
4. The individual's rights over their body are overridden by imposed use of its attributes
Action: The recommendation below (RC/TTL1) proposes the investigation of alternative ethical frameworks to assess the issues that are inherent in this fear.
5. Exemptions and exceptions that would exclude some people. In certain cases (e.g. the disabled), this may be inevitable and appropriate mechanisms are required to avoid discrimination. Procedures developed during the design process should attempt to limit the opportunities for misuse of exception cases.
Action: RC/TTL3, RC/TTL9
6. Having deployed the biometric in one system, organisations may find it useful to justify extending its use on grounds of cost, security or political expediency.
Action: Results of the BIOVISION Security Study, RC/Sec4, RC/TTL7, RC/TTL8

RC/TTL1 RC - TRIALS, TESTING, LEGAL, etc 1: There is no clear ethical framework for the development and use of biometrics. To some extent this will be determined by individual societies and cultures. However, currently, the agenda is set by cost-benefit analysis for improved security, without reference to a more fundamental assessment of the advisability of cross-application unique identification of individual citizens and consumers.

¹⁴ A list of 13 concerns that have been voiced about the use of biometrics in identity cards has been tabled in: chair Joe Fontana, *A national identity card for Canada? Report of the standing committee on citizenship and immigration*, <http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06-e.htm> (October 2003)

¹⁵ BIOVISION project report: Michael Behrens and Maik Weber, *Proposal for a Cost-Benefit Analysis* (2003)

RC/TTL2 RC - TRIALS, TESTING, LEGAL, etc 2: Social and socio-psychological research should be encouraged to understand how identities and personas are used at present, and the implication of the use of biometrics on legitimate expression of such multiple identities.

RC/TTL3 RC - TRIALS, TESTING, LEGAL, etc 3: The impact of long term exclusion of those unable to make use of certain biometrics.

RC/Sec4: RC - SYSTEMS AND DESIGN: SECURITY 4: Biometric data for different applications (or held centrally and on-card) may require to be of different types (or held in incompatible formats) in order that centrally held information cannot be misused.

RC/TTL7: RC - TRIALS, TESTING, LEGAL, etc 7: Further development of the Best Practices, based upon experience of similar codes in other fields. One specific application could be in the integration with Privacy Impact Assessments, together with advice to auditors confirming the adherence to such a Code.

RC/TTL8: RC - TRIALS, TESTING, LEGAL, etc 8: Further studies should continue to monitor the progress towards a uniform interpretation of the privacy issues surrounding the use of biometrics in the countries of the EU (including the Newly Accessioning States), and support the activity of the Article 29 Working Party with impartial information about developments in biometrics. Users' experience in the application of biometrics should be collated and interpreted with the aim of either lobbying for a revision in the legal regime or for retention of the *status quo*.

RC/TTL9: RC - TRIALS, TESTING, LEGAL, etc 9: The status of those unable to use the preferred biometric solutions should be recognised, whether these are in the private or in the public sector. Solutions are required that will limit the long term exclusion of such individuals from the opportunities offered by uniform secure authentication.

1.3 Biometric methods - the European scene

As has been hinted previously, there are a large number of biometric methods that have been researched and commercialised. Among the possibilities that are currently exploited commercially (or are close to exploitation) are

- automatic facial recognition, using either visible light or infra-red illumination (or both)
- recognition by fingerprint(s) or surface features extending along the finger
- iris recognition
- recognition by representation of the blood vessel patterns in the retina
- hand geometry
- the pattern of veins on the back of the hand
- speaker verification
- dynamic signature recognition
- keystroke dynamics.

Others, such as gait recognition, are in development. (A detailed analysis of the technologies is presented in section 4.),

This is a market characterised by a large number of suppliers, many of which are small and privately owned. Some supply the sensors, others are specialist software companies developing better recognition algorithms or improved middleware. We believe that there are currently upwards of 200 suppliers of such devices and subsystems and the estimated 220meuro¹⁶ worldwide market is fragmented, especially in Europe.

In spite of this fragmentation, Europe leads in many segments of the international biometrics market. Sagem (France) is considered a world leader in the deployment of large-scale fingerprint systems. Infineon (Germany) and Fingerprint Cards (Sweden) are leaders in fingerprint sensor chip technology and associated security integrated circuits, with the Infineon product commercialised for mass market application in PCs. Precise Biometrics (Sweden) has quickly become recognised as a supplier of consumer fingerprint systems for consumers and PKI applications. Cognitec and ZN Vision (now part of Viisage) are recognised as international leaders in facial recognition technologies. Keyware Technologies (Belgium) was an early leading developer of multiple biometric solutions.

There are well-established organisations. Within the TeleTrusT Working Group 6 “Biometrics” most of the German manufacturers of biometric solutions are represented, such as fingerprint, signature and speaker verification, facial and iris recognition, multimodal solutions, as well as system integrators with a strong experience in the combination of biometrics with smart cards and other tokens. The US government has contracts with UK and German researchers for the exploitation of face, fingerprint and gait recognition technologies; we anticipate that Europe’s future ability to export biometric systems and knowledge will build substantially on the current high status of its industrial academic research base, particularly in the core areas of smart cards, image and pattern recognition.

It is often forgotten that the biometric is only one part of a fully deployed application and experience gained in system integration and deployment needs also to be shared within the European community of interest. European organisations have led the world in many innovative biometrics applications. The European tradition of socio-technical system design affords a perspective that may be absent in many non-European approaches – a possible advantage when European organisations compete for projects world-wide and a perspective which is embraced in this project.

The first biometric-based border crossing system in the world was installed at Schiphol Airport in 1992 (an early fingerprint based deployment), and a new system using iris recognition started operation in December 2001. (Trials in other airports such as Heathrow continue.) Fingerprint and facial recognition systems have been used at nightclubs in the Netherlands. Facial recognition systems linked with CCTV surveillance have been implemented in the London Borough of Newham – with local reduction of crime¹⁷. Application of fingerprint verification with the Spanish social security card started in Andalucia in the early 1990’s. In the Netherlands, the Ministry of Justice is currently deploying a fingerprint secured PKI for systems access authorisation, and industry too is making use of biometrics at the world’s largest port in Rotterdam, where hand geometry is used to secure the entire cargo tracking process. In the UK, the Immigration and Naturalisation department will have saved millions of pounds in 2002 following the deployment of a fingerprint recognition system to screen asylum applicants. Recently, the pan European EURODAC fingerprint system has demonstrated the benefit of co-operation between European countries, whilst respecting the rights of individuals under law.

¹⁶ *The Biometric Industry report, Market and Technology Forecasts to 2003*, Elsevier Advanced Technology (2001). Figure is for Year 2000.

¹⁷ Note that the crime reduction could be due to deterrence.

Clearly, the application landscape is strong in many countries of Europe. However, the future could see many more cost saving and efficiency-enhancing applications with the right mix of expertise, knowledge and consumer awareness. It appears that many suppliers develop their devices and systems without knowledge of the results of current and past research, both from other European Commission sponsored projects in the Fourth and Fifth Frameworks, as well as from universities and national projects in Europe, USA and Asia - and non-academic initiatives such as those sponsored by the Biometric Working Group and those undertaken by the TeleTrusT Working Group 6 "Biometrics" e.g. through its BioTrusT project.

Furthermore the links of researchers in institutions to these suppliers, and between suppliers and system integrators (who will ultimately deploy the biometric method as just one part of a complete project) are poorly developed. This requires the creation of a pan-European organisation that shares knowledge and best practice, which encourages high standards in development and design and that links researchers, developers, end user organisations and other stakeholders across national frontiers. Such a European Biometric Forum will build on the experience of a number of mainly nationally based initiatives such as the UK's Association for Biometrics, Germany's TeleTrusT organisation and the Dutch Biometrics Forum while linking to other organisations such as the US-based Biometric Consortium.

1.4 The BIOVISION Roadmap project

The BIOVISION consortium developed from a workshop on biometrics held in January 2002 and organised by the European Commission¹⁸. The consensus developed at that meeting resulted in the proposal for this project that commenced on 1 June 2002, with a duration of 14 months. The website for the current version of the BIOVISION roadmap and other materials is at <http://www.eubiometricforum.com>

The BIOVISION Consortium undertook this Roadmap with a number of aims in mind. It did not see its primary remit as the preparation of yet another quantitative prediction of the future growth in the biometrics market over the period to 2010. Although such assessments are useful and will be referred to in this roadmap, we believe that the European biometric community needs a set of tools with which to develop alternative scenarios of different types of applications. These should be designed to be robust against changes in the economic and political landscapes, whilst being responsive to wild card events such as those of 11th September 2001. The output is firstly directed to the European Commission, as customers for this study, so as to guide them in supporting areas of research, development and trial deployment that appear to be most critical for the biometrics industry in Europe. However, it is also directed towards individuals and organisations that are considering the application of biometric technologies, to support their understanding and confidence in moving forward with their ideas.

The key elements of this roadmap project are:

1. This document collating the results of the studies and workshops undertaken as part of the contract.
2. A listing of the key research challenges that face the European biometric community and which could be addressed by projects proposed under the Sixth Framework programme.
3. A collation of previous and current research projects in the field of biometrics, with the principal results obtained to date.
4. The results of a series of focussed studies in areas critical to the development of legal, secure and acceptable biometric-enabled applications, using both qualitative and quantitative approaches. The primary areas are:

¹⁸ *Paving the way for the adoption of biometrics*, workshop in Brussels, 15 January 2002, <http://www.cordis.lu/ist/ka2/biometricsworkshop.htm>

- End User Perceptions,
 - Security,
 - Safety and Medical issues,
 - Future directions in the underlying technologies and applications,
 - Legal, regulatory and standards arena.
5. Assessment of the key factors in the commercial take-up of such systems, building upon the work of the BEE project and by the market research of commercial organisations.
 6. Two primary workshops where the results of such studies were brought together.
 7. The development of a community of interest amongst all players involved in the successful deployment of biometric-enabled applications - the European Biometrics Forum.

To this end, the consortium had been selected to represent as many of the stakeholder groups, either directly - through participation as one of the nine principal contractors, or indirectly through either subcontracting or affiliation with the main organisations.

CESG, an agency of the UK government, co-ordinates the **Biometric Working Group** with the specific aim of fostering activities directed at successful use by government and working closely together with other national certification bodies as the BSI in Germany. As the premier agency responsible for electronic security in the UK, it leads on the security aspects of implementing biometric enabled solutions.

The German **TeleTrusT** consortium was the second major player -in particular, its working Group 6 “Biometrics”, which has been addressing the opportunities in several sectors in an interdisciplinary way¹⁹. The BioTrusT project group is specifically interested in developments in the financial sector, with representatives of industrial and academic entities, test institutes and certification bodies, consumer agencies and data protection commissioners.

Major end user organisations were represented by **BT Exact Technologies** - the research and development arm of British Telecommunications, and **Nationwide Building Society** – a leading UK financial institution.

The supplier focus was provided by **Daon**: an SME (small to medium enterprise) developing biometric systems.

The international perspective, together with an independent view on applications, was provided by **Avanti**, who additionally represent the IBIA (International Biometrics Industry Association) within the BWG.

B&L Management Consulting have undertaken studies on the future of biometrics in German-speaking countries in Europe.

The academic community had representation from **CWI**, Amsterdam, **University College London**, the **University of Applied Sciences Giessen-Friedberg** in collaboration with the Fraunhofer Institute, and the **National Research Council of Italy**.

Furthermore, the members of the consortium were positioned to involve the other major players in Europe through their links to the UK’s long-established **Association for Biometrics**, the **Dutch Biometric Forum**, the newly-formed **Italian Biometrics Forum** and the other participants in the TeleTrusT association, which involves most of the key players in Germany. Many of the members also participate in the activities of the US-based Biometrics Consortium, which brings together government, academia and industry worldwide.

¹⁹ Project summaries of work undertaken in 1999-2002 are available at www.biotrust.de

The partners in this project have been informed through a number of other avenues, which has enabled the consortium to have access to the latest thinking and activities in the field throughout the period of this study. Examples of this wider involvement of the biometrics community include:

- Networks of personal contacts of the individual members of the project
- Participation of four of the partners in the ISO SC37 standards subcommittee on biometrics
- Involvement in external projects, such as B&L's management of the electronic identity project for the European Commission and external review of other projects by the members of the consortium
- In-depth discussions with all stakeholders in the field, from officials in the data protection commissions of member states of the EU, to specialist suppliers – both industry leaders and emerging SMEs, through to potential end users, both for large and small scale deployments.
- Responses to presentations made at conferences and meetings of key groups such as the Association for Biometrics.
- Attendance at key industry conferences such as Biometrics 2002 in London; CardTech/SecurTech in New Orleans in April 2002 and in Orlando in May 2003²⁰; and the 4th International conference on Audio- and Video- Based Person Authentication (AVBPA) in Guildford (UK) in June 2003²¹
- Invitation of outside representatives to scenario modelling workshops such as those held in Amsterdam
- The holding of a well-attended 3-day open workshop in Rome in January 2003
- Presentations to country groups in Madrid and Paris and to the participants at the Sixth Framework information day in March 2003
- Information gained from leading specialist newsletters such as Biometrics Technology Today²² and the Biometrics in Human Services User Group²³ and from online forums such as the Biometrics Consortium listserv.
- Input from consultants' reports on various aspects of the industry

Taken together, the results should provide a validated view of numerous stakeholders on the current direction of biometric programmes in Europe and the prospects for the future through to 2010.

1.5 The relationship to other Roadmap projects

This Roadmap is part of a portfolio of 25 projects sponsored by the European Commission as a precursor to the next major programme of European research in the application of information and communication technologies: the Sixth Framework. Of these roadmaps, the following relate to the security and 'trust and confidence' themes²⁴. Their findings were integrated into the final roadmap insofar as the final versions were available at publication time, with the outputs of the BIOVISION project discussed with the project participants in these studies:

- AMSD: Accompanying Measure on System Dependability www.am-sd.org
- RAPID: Roadmap for Advanced Research in Privacy and Identity Management, www.ra-pid.org
- ACIP: Analysis and Assessment for Critical Infrastructure Protection, www.eu-acip.de
- PAMPAS: Pioneering Advanced Mobile Privacy and Security, www.pampas.eu.org

²⁰ <http://www.ctst.com/>

²¹ <http://avbpa2003.ee.surrey.ac.uk/>

²² <http://www.compseconline.com/publications/prodbio.htm>

²³ <http://www.dss.state.ct.us/digital/news33/bhsug33.htm>

²⁴ <http://www.cordis.lu/ist/ka2/rmapsecurity.html>

- RESET: Roadmaps for European Research in Smartcard Technologies, www.ercim.org/reset
 - STORK: Strategic Roadmap for Cryptology, www.stork.eu.org
- 

2. Roadmaps and Roadmapping

2.1 An application- and user-oriented roadmap for European biometrics

An initial aim of this Roadmap was to determine the best opportunities for the application of biometrics in key sectors of the European economy over the period to 2010 and to advise the European Commission and other bodies on how best to foster these. As such, it was firmly grounded in the application-pull end of the spectrum of possible roadmaps, rather than starting from a consideration of the possibilities that novel technologies can offer, and from these possibilities deriving application scenarios (see section 2.2 for a discussion on the taxonomies of roadmaps).

We believe that many of the over-optimistic projections of the uptake of innovative technologies - such as biometrics - have resulted from a fascination with the technology itself rather than in what benefits the technology can deliver for customers and end-users in the context of a specific application or service. Such technology-focussed approaches have also neglected to take into consideration the potential risks and disadvantages of using biometrics, and the claims of alternative solutions, which may offer similar functions or performance, albeit without some of the exciting user-facing hardware.

However, this does not mean that we should adopt a conservative view on the potential of new technologies. We have attempted to balance the projection of existing trends in the adoption and use of systems employing biometric devices, with a scenario modelling method to explore some of the options beyond the near term (2003-5). These longer term visions (2006 onwards) will make use of the results of research currently underway in universities and commercial R&D laboratories.

As the project progressed, it became clear that the BIOVISION project should not necessarily aim to determine the 'best' applications, but to identify those areas where the current scarce resources in the EU could be deployed to the most effective effect. In any case, the use of the qualifier - 'best' - would depend on the perspective of the stakeholder in a particular application and is therefore inappropriate when we aim to bring together all the players in a fragmented European marketplace. Examples of where such different perspectives can offer the biometrics community valuable insights are:

- For **device and software suppliers**, 'best' may refer to applications that generate sufficient revenue and publicity to ensure the continued survival of the large number of small companies in this crowded sector (worldwide, over 200 companies offer a biometric solution of some kind).
- For a **customer**, whether it is a government institution (with security also a major concern) or a corporate entity creating a service for niche markets or large populations of consumers, 'best' may be an optimal return on the total investment of which the biometric component may be only a small part. Nevertheless, price-performance considerations in the use of the biometric subsystem will play some part in the overall profitability of the total design.
- For **system integrators**, ease of interfacing to other sub-systems, robust and easily predictable performance, low maintenance costs and availability of multiple sources of standardised components could be the prime considerations.
- While for an **end-user**, the 'best' application may be determined by the convenience of not needing to remember PINs or passwords, or carry more keys or cards, with minimal implications for personal privacy or health and safety.

There are inevitable compromises to be made, as applications are unlikely to meet the aims of each of these stakeholders. Nevertheless, through its diverse membership, the BIOVISION consortium has been able to assess the positioning of each of these groups.

The focus of the Roadmap is on applications in Europe, but in an increasingly globalised world, it would be pointless to take a narrowly defined view that excluded the impact of events, research and experience outside the 300 million population of the EU. Indeed, it is

likely that many of the biometric-enabled deployments in Europe will include devices from the US or the Far East, and these deployments will be realised by multi-national system integrators. In particular the impact of the US decision to require the use of biometrics in passports and visas in the near term has changed the perspective on the application of biometrics since the initial proposal was drafted in February 2002.

Nevertheless there are specific features of the European market that influence the selection of biometric technique and the details of the application. For example, in contrast with the US, Europe has a commitment to government regulation of consumer rights to privacy, fair trading, etc rather than offering the individual a recourse to law as the preferred method of establishing their rights. Europe differs significantly in many other ways that are relevant in this context: there is a commitment to maintenance of the cultural, linguistic and personal diversity, a rich and complex heritage, and the provision of government funded health and welfare benefits for all its citizens. These differences may be reflected - for at least some system designers - in a preference for socio-technical design of systems, where the needs, perceptions and existing working practices of end users are given equal weight with the requirements defined by the customer of a system.

2.2 Roadmapping - from concept to implementation

The use of roadmaps to capture a view on the future of technology-driven developments, for either a single company or at a national or international level, is relatively recent. Early adopters such as Motorola, Philips and major oil multinationals, demonstrated the value of bringing together experts from a number of departments to collate information and knowledge held across an organisation and then display it in a simple visual way to show the linkages between research, development, products and the requirements of applications along a timeline. In the mid-1990's the value of an industry-wide roadmap began to be appreciated, mainly through a successful US initiative for the semiconductor industry. The SIA (**Semiconductor Industry Association**) Roadmap is now a major fixture, being revisited at two-yearly intervals, with work on the next version commencing once the current issue is published. These can be major projects in their own right, with the latest International Technology Roadmap for Semiconductors - ITRS - released in November 2001 being the combined output of the work of 800 specialists worldwide²⁵. This, and allied maps for the electronics industry in the USA, culminated in the creation of a roadmap for the entire sector, under the National Electronics Manufacturing Initiative.

However, the literature on roadmaps, and what makes them successful or not, is relatively sparse, and this overview draws upon some key papers, backed by the experience of individual members of the consortium. Perhaps as a response to this low level of analytical response, two centres of excellence have been formed, Purdue University in Indiana²⁶, and Cambridge University's Institute for Manufacturing in the UK.

In an early initiative in 1997, **EIRMA**, the European Industrial Research Management Association, reviewed the state of the art, as seen from the European perspective, building upon the lessons learnt from years of experience in the consortium.²⁷

Examples of other resources that are available include:

- Cambridge University's Centre for Technology Management technical papers and the T-Plan approach, a fast-track process for Technology Roadmaps²⁸.

²⁵ <http://public.itrs.net>

²⁶ J Duckles and E Coyle, *Purdue's Center for Technology Roadmapping: A Resource for Research and Education in technology Mapping*, (2002)

²⁷ EIRMA, *Technology Roadmapping: Delivering Business Vision* (Paris, 1997)

- A paper on Motorola's recent work in this field²⁹

In 1998, Sandia National Laboratories in the US published a report on *Fundamentals of Technology Roadmapping*³⁰ that summarised the roadmapping process as a three phase endeavour. More recently, Kostoff and Schaller³¹ have reviewed some of the elements of successful roadmap initiatives on behalf of the US Department of the Navy.

This latter paper quotes Robert Galvin, an ex-chairman of Motorola and a keen proponent of the use of roadmaps:

'A roadmap is an extended look at the future of a chosen field of enquiry composed of the collected knowledge and imagination of the brightest drivers of change in that field ... Roadmaps communicate visions, attract resources from business and government, stimulate investigations and monitor progress. They become the inventory of possibilities for a particular field.'

One fundamental point emphasised throughout the literature is the importance of the **process** of generating the Roadmap. For example, EIRMA note that *'the greatest value ... comes from the business processes that have to be put in place to create it, rather than the possession of a TRM itself. Consequently, a TRM is not something that can be purchased from a consultant, or created by an individual. It must be the output of an empowered team activity...'*

Roadmaps can be either prospective - looking to the future - or retrospective, examining the steps that led to a particular successful or not so successful result, from the fundamental research through to the development and the released product or service. Their fundamental orientation may be either technology-pushed or application- (or requirements-) pulled, and the methodology of generation of the roadmap can be based upon the synthesis of knowledge of industry experts or through the computer analysis of documents, research papers, news items, etc. Figure 1 illustrates these options and hybrids of the various possibilities are, of course, possible. In this project we will be using a future oriented, predominantly application-pull approach (60% of importance), using experts and potential customer assessment, validated by an external community of stakeholders.

Figure 1 Options for the Roadmapping process (underlined terms represent the BIOVISION approach)

Time perspective	Push/pull	Approach
<u>Prospective</u>	<u>Technology push (40)</u>	<u>Human experts</u>
Retrospective	<u>Application pull (60)</u>	Computer analysis

²⁸ R Phaal et al, *Technology Roadmapping: Linking technology resources to business objectives*, http://www.mmd.eng.cam.ac.uk/ctm/pubs/TPlan/TRM_white_paper.pdf and R Phaal et al, *T-Plan: the fast start to Technology Roadmapping: Planning your route to success* (University of Cambridge, Institute for Manufacturing, 2001)

²⁹ M Grinnell et al *Case Study: Innovation Roadmapping using Enterprise Automation Software* <http://roadmap.ecn.purdue.edu/CTR/documents/MotorolaCaseStudy.pdf>

³⁰ M L Garcia and Bray, *Fundamentals of Technology Roadmapping*, <http://www.sandia.gov/Roadmap/home.htm> (1998)

³¹ R N Kostoff and R R Schaller, *Science and Technology Roadmaps*, IEEE Transactions on Engineering Management **48**(2) pp 132-143 (May 2001)

2.3 Successful Roadmaps

Based upon their analysis of the literature, Kostoff and Schaller offer a list of critical success factors for high quality roadmaps. They rightly point out that there is no agreed measure by which the quality of roadmaps can be judged. Even if a roadmap's predictions are fulfilled, it could be that these were set too conservatively and end users followed the route of least resistance. On the other hand, the consensus building approach by the SIA has generated a competitive atmosphere of trying to 'beat the roadmap' perhaps to the detriment of a more commercially logical approach.

The **pre-requisites for a successful roadmap**, as suggested by the authors are many and diverse and drawing on their list, the following seem to be relevant to the BIOVISION roadmap:

1. A comprehensive and broad appreciation of the current status of the science and technology base, grounded in an understanding of how the industry got to the present state. Where are we now and how did we get there? This survey of the present situation should encompass all the latest relevant projects, activities or events that may impinge on the objectives of the roadmap.
2. Looking to the future, the experts should develop a comprehensive vision across all the relevant areas that impact on the technology.
3. A commitment by senior decision-makers to the continuation of the process. Customers, and other users of roadmaps, should realise that the value lies to a large extent in the maintenance of the roadmap as the technology develops and assessments are updated.
4. A strong competent team of experts drawn from research, technology and product lines - led by a roadmap manager who scopes the roadmap, structures the working groups and chooses the final outputs from the large number of inputs gathered in the process of developing the roadmap.
5. A clear sense of purpose and ownership, with the roadmap preferably undertaken by those people who will have a stake in the outcomes. The forming question and resulting recommendations should be relevant to the subsequent activities of the customer.
6. Standardisation of approach to the roadmap, if there is a need for an integrated view across a whole industry sector.
7. A process is required to determine the rationale for the selection of nodes in the timeline and the links between nodes.
8. Validation of the roadmap through the involvement of as large a number as possible of the community of practitioners.
9. A clear vision and action plan detailing what needs to be done - or not done - to foster and ensure support for the achievement of the optimum directions identified in the Roadmap.

2.4 The Roadmapping process

The Sandia paper referred to above offers a detailed account of the roadmapping process in a three phased approach and illustrates its application to the previously mentioned SIA roadmap. The phases comprise an initial preparatory stage, the core phase of developing the roadmap and the final stage of follow-up. Although the **Sandia roadmapping process** is predicated on a technology-push roadmap, the BIOVISION project used some of its insights, although it had to modify them in the context of a more complex application-led framework.

2.4.1 Phase 1: Initial Preparation

- Acceptance of the need for the roadmap from a larger constituency than just a single organisation commissioning or undertaking the project. Furthermore, the rationale should be driven by a defined set of needs rather than be solutions-driven. With the

adoption of such a needs-based approach, the scoping and setting of boundaries of the roadmap will be immeasurably improved.

- Assembly of a team with expertise across all aspects of the technologies, led by a group that will benefit from the results
- Assurance that a vision can be developed for the industry, and that there is at least the possibility of genuine collaboration between the major industry stakeholders.

2.4.2 Phase 2: Roadmap development

2.4.2.1 Technology Push Perspective

In the Sandia framework, the development of roadmaps is treated from a strictly 'technology push' perspective, which is at odds with the presumption in BIOVISION:

- The most critical step is the agreement of the team undertaking the roadmap on the **common needs that the project will address**. Eliciting these needs can be facilitated by a scenario modelling process, and the BIOVISION project refined the needs for key application areas over the longer timescale through the use of such a methodology.
- If a **quantitative measure of the final goal** of the technologies can be defined, this will aid in focussing the efforts of the experts involved. For the range of biometric-enabled applications considered in this project, such a quantification was considered to be inapplicable.
- The next consideration is a **listing of the principal areas of technology** that ought to be considered. For BIOVISION, this included all of the biometric methods (e.g. fingerprint, voice, iris recognition), but the team also needed to take account of software processing developments such as advances in image processing, improvements in user interface design, and changes in costs and performance of specialist and general purpose hardware. This was taken into account to some extent during the work on Section 3.6
- Having determined the technology, the work should move towards a consideration of the **technology drivers and the targets** that will determine which technology will address the requirements in the best way and the dates by which these targets can be met. Some of these drivers were identified in the BIOVISION project, but the major uncertainties in development of biometric and parallel technologies over the extended timescale have precluded this type of analysis.
- This is followed through by an **analysis of the alternative technologies** and the timelines for developments in each. For example, will an attractive technology meet the target requirements in a relatively easy way, but require the solution of tough problems along the way? If more than one approach can address the target requirements, when will decisions have to be made as to which option to pursue and which to relegate (or devote less resource to)? Section 4.0 considers such alternatives, most notably of course, the retention of the *status quo* in which PINs and passwords, keys and smart cards will play a role. By virtue of their cost and the familiarity of end users with them, these established options will continue to dominate the marketplace for many years.
- Having identified the alternatives, probably the most difficult aspect of the roadmap is the **recommendation of which technologies to emphasise** in the allocation of scarce resources. Although some approaches may look attractive in the short term, premature investment in these may prejudice the more profitable options, leading to increased whole life costs as systems have to be updated, or resulting in confusion in the marketplace as deployments are put on hold for fear of making the wrong decision. Disruptive technologies need to be taken into account: those that do not appear to meet the intermediate requirements, but will simplify the final system. In

BIOVISION, the consortium noted that the existing group of technologies offered solutions to most of the authentication requirements (perhaps with the exception of tracking and tracing individuals, in which gait recognition may have a role). The likelihood of a novel biometric method making an impact over the study period was considered to be remote. Therefore, any proposals for support of research into novel methods should be supported by a clear analysis of why current approaches are unlikely to meet the requirements set by service operators. Current projections for the biometric market view three technologies as particularly significant: facial recognition, fingerprint systems and iris recognition. There are niche opportunities for speaker verification, hand geometry and dynamic signature verification, perhaps to be used in conjunction with another method in so-called multimodal biometrics.

2.4.2.2 Application Pull Perspective

Biometric methods are often seen as purely a security measure to ensure a higher standard of authentication than can be offered by either 'something you know' or 'something you have'. This may be true for many applications, but often other considerations come into play. Hence, a biometric could be used as:

- security mechanism for more secure authentication of an individual person
- security mechanism to limit a registration for a service to one user at any time
- a visible deterrent to stop abuse or criminal activity
- symbolic value to brand a service as 'high tech'.

Other distinctive benefits include improved usability of a system and cost reduction due to the elimination of manual processes.

In analysing the future of biometric-enabled systems from an application-pull perspective, several steps need to be considered:

- The **application class** within which it falls. In section 3 we shall provide an initial classification of applications that will support the application-oriented elements of the Roadmap.
- For each application class, there will be **exemplar applications** that fall within the class, while other applications are likely to make use of a mix of these fundamental elements. These exemplar applications will form the focus of the more detailed roadmapping in Section 6, using the insights that were gained in the scenario models of Section 3.
- Current and future developments in these exemplar applications were considered. In some cases, the view of a key body may determine whether a biometric will be considered appropriate and which biometric is to be used. For example, for the case of biometrics to be used in passports and other machine-readable documents, the industry body, ICAO determined that - on the basis of its own studies - face recognition would be the universal biometric, with iris and fingerprint based options available to individual countries.
- Further examination of the exemplar application will focus on the **biometric quality requirements (both technical and non-technical)** that a biometric-enabled solution would be required to meet so as to justify the investment in systems that can utilise these novel technologies. Note that the word 'quality' covers a wide range of attributes, amongst which are robustness, security of operation, usability, cost-effectiveness, interoperability, user friendliness. Not surprisingly, many of these are the critical areas in which there are significant unknowns and which were selected as the themes of special studies in this project. Assessing the way in which quality of a biometric solution meets the application requirements of a service was the subject of

a companion study and the resulting analysis is available in a separate document³². Although at present this work is still theoretical, future work is envisaged in testing the validity of this approach.

- Many biometric-enabled solutions to the applications under consideration above will be implemented. However, one of the major uncertainties is the timescale in which these will start and the rate at which they will take over from existing solutions. This part of the roadmap analysis is one of the more problematic areas, as it is dependant on many factors, only some of which are determined by progress in technology (as discussed in the 'technology push' perspective). Other factors which will influence the **speed of adoption and the rate of transition from non-biometric solutions** include:
 - developments in **complementary technologies** and in technologies that reduce the need for a biometric solution, e.g. the mass use of smart cards, or more improbably, the use of implanted radio frequency tags in humans (Note that in some cases these could enhance the value of a biometric element to the solution.) These complementary technologies and developments are considered in Sections 3.6 and 3.7.
 - **changes in the social, economic and political environment** that will either bring forward the adoption of a biometric-enabled solution or delay it. Examples of such changes are:
 - social: divergence of populations in the advanced economies into two identifiable groups: the wealthy, but 'time poor' and those excluded from the ICT-based services with poorly paid jobs and little stake in the new knowledge based economies
 - economic: the increasing proportion of elderly in the population, with greater expectations from health and welfare provision by the state and private enterprise
 - political: the impact of new terrorist threats such as those manifested in the September 11th events.

Section 3.7 reviews some of these predictable developments.

- **The size and potential value of the market** for the new biometric-enabled solutions addressing the exemplar applications, together with an appraisal of the key players who are best placed to take advantage of these opportunities. The reports of market research consultants provides some limited guidance.
- **Residual uncertainties** that have not been captured elsewhere in the process.

2.4.2.3 *Integrating the Two Perspectives into a Single View*

For each of the applications, there could be a number of technology solutions, some of which fit well with the quality requirements as determined from the application perspective - others of which are inappropriate. Conceptually, a two-dimensional matrix would be required to assess the appropriateness of each technology for every application. In this case, the timeline (generally a linear axis in conventional roadmaps) translates to a non-linear form. Although such a solution is attractive from a philosophical standpoint, its generality is obtained at the expense of extreme complexity, thereby losing the main advantage of the roadmap, its diagrammatic simplicity. The BIOVISION project determined that this would be inappropriate, although future editions of the Roadmap may wish to pursue this aim.

³² Michael Behrens and Maik Weber, *Report on technology and application: Issues for biometric identification systems*, (May 2003). Note that similar approaches are being pursued by the Japanese national standards organisation.

2.4.3 The BIOVISION Roadmap

The Roadmap examines a selection of major application areas through the lens of certain key determinants of the likely success of implementation: user acceptance, security, a medical dimension, legal and regulatory issues and standardisation activities. In many cases, this has been achieved through a listing of the critical issues as identified in a workshop including participants outside of the project. The individual studies that relate to the key determinants are often not made explicit, but colour the assessment of the likelihood of the specific scenario.

2.4.4 Phase 3: Follow-through Work

- Exposure of the methodologies, conclusions and recommendations for **review by the community** at large, firstly through an invitation to comment, followed by socialisation of the conclusions through workshops, conference papers, and networking with thought leaders and decision makers in the industry. The BIOVISION project incorporated this into the roadmap development process and will continue it through the open invitation to comment on the Roadmap.
- Recommendations in the form of **Research Challenges** that identify the cross-cutting issues common to applications and technologies.
- **Review**, to ensure that the roadmap takes advantage of the most up-to-date knowledge and incorporates innovations and the impact of changes in the external environment. In the BIOVISION context, this will form one of the aims of the proposed European Biometric Forum, as well being the subject of a review workshop in February 2004.

2.5 The BIOVISION Roadmap – an alternative view

The Roadmap figure (at the end of this document) is a schematic representation of the diagrammatic element of the Roadmap for a specific Government-oriented application. It illustrates a form of the Roadmap concept grounded in the conventional - technology-focussed – approach to roadmapping. Of limited use in the present roadmap report (due to the diversity of applications and underlying technologies, as discussed previously), it nevertheless demonstrates the value of such an approach. In future versions of the BIOVISION Roadmap it may be appropriate to examine specific applications and services with the aim of constructing such diagrammatic forms of the roadmap concept.

This format draws heavily on the Philips approach as documented by Groenvald³³, with BIOVISION extending it to take account of the strong balancing of the application focus in our work. The timeline summary shown in this Roadmap figure illustrates a number of features of the BIOVISION roadmap:

- The timeline, as the x-axis, stretches to the end of 2010, but the application dimension (at the very top of the page) can continue beyond this date to illustrate the onward development of government plans. It may also be appropriate to include activities that have already commenced - in which case, the timeline will have a historical element as well.
- The bold vertical line at the end of 2005 indicates the boundary between two time periods - short term and long term - as discussed previously.

³³ P Groenvald, *op cit* (1997)

- The BIOVISION project timescale is indicated by the activity labelled BVN in the top left of the figure. (The work of envisioning the future of European biometrics should continue beyond the end of the project through the efforts of organisations such as the European Biometric Forum.) In this particular application, the goal is to deploy a biometric-enabled system for a government (or a department within a government) at the start of 2008 - indicated by the inverted black triangle. The task of refining the vision is shown as continuing to the end of 2004.
- The key components, in addition to a clearly defined application, are
 - research,
 - technology development (often by suppliers),
 - the products offered by suppliers,
 - the processes which need to be in place to make use of these products in the application, and
 - drivers and inhibitors that can either advance or delay the introduction date of 2008.

These components are marked as separate layers in the schematic, working from the bottom of the diagrammatic roadmap to the top.

- Activities such as BIOVISION and the national and European funding bodies develop a set of requirements for priorities in research to support the biometric community in meeting the needs of application sectors. The response of consortia and individual organisations is to put forward proposals to meet these requirements and if successful, these will gather the resources to start a research project, for illustrative purposes shown as lasting for a period of 3 years. Note that even if there are tangible outputs at the end of year 1 of this research that can be moved towards commercialisation, the productisation at the end of the lifetime of the research project will only catch a second phase of the deployment of this application, beyond the end of this time horizon. One of the useful outputs of such a Roadmap is that it can clarify the rate-determining steps and highlight opportunities for increased effort to reduce critical timescales.
- Existing technologies that are under development (such as 'Improved Biom 1') can be mapped; in this case, this activity is being carried out by Supplier 1 who is able to capitalise on its research through the introduction of product P2 in 2005. This can be included in pilot trials and (if successful) included in the procurement cycle, meeting the 'required by' date. A competitor, to whom this technology is licensed a year later will probably miss the deadline with its product, R2, but with its commitment to the 'Radical Biom 1' deriving from the research project described above, it is well placed to take advantage when phase 2 of the application is launched in the next decade.
- Other, non-technical, activities can be included - such as the legislation that needs to be in place in order to start the procurement process.
- Finally, the start date of the deployment may change in response to political, economic or social factors. A list of such possibilities should be added as an aid to policy makers.

3. Applications

3.1 Matching the biometric technology and the application

3.1.1 Failure of adoption of biometric technologies

As has been mentioned in an earlier section, there are numerous ways in which biometric methods can be applied. A few have been widely deployed, such as the South African Pensions use of fingerprint verification (1990-date) and the numerous welfare benefit schemes in the USA that have been implemented to reduce the incidence of fraud. There are also many, quite small schemes that continue operating without much publicity, e.g. in access control to sensitive areas in nuclear power plants. Nevertheless, many more were prototyped amidst a high degree of publicity only to be forgotten - perhaps even quietly withdrawn. This roadmap project collated publicly available information about the current status of biometric-enabled applications in order to assess the reasons for this failure of biometric methods to reach the market. (Section 7.1 discusses these reasons in a more general way.)

3.1.2 Generic Application Classes

The BIOVISION analysis of the applications for which biometric methods could be used has derived the top level classification of:

1. Access control
2. Transaction security
3. Tracking and tracing
4. Personalisation

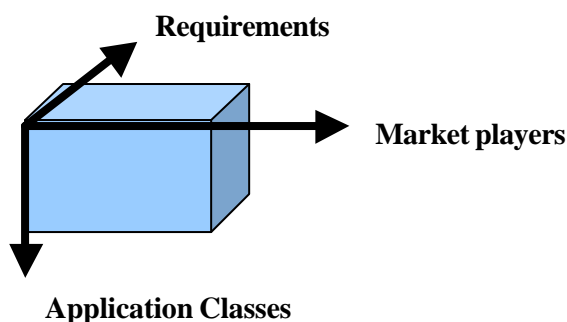
Applications can be viewed as either an exemplar of an application class (e.g. a fingerprint control on a door lock is a clear example of the access control application), or a combination of the elements of one or more of these primary application classes.

3.1.3 The 'Application Pull' Framework

For an application to merit the use of a biometric method, there must be additional features of that technology that will drive its adoption and subsequent diffusion. This can be termed **application pull**, and the extent to which such an application pull is realised in the marketplace is determined by three factors as illustrated in the schema of Figure 2:

- Application class
- Requirements
- Market players

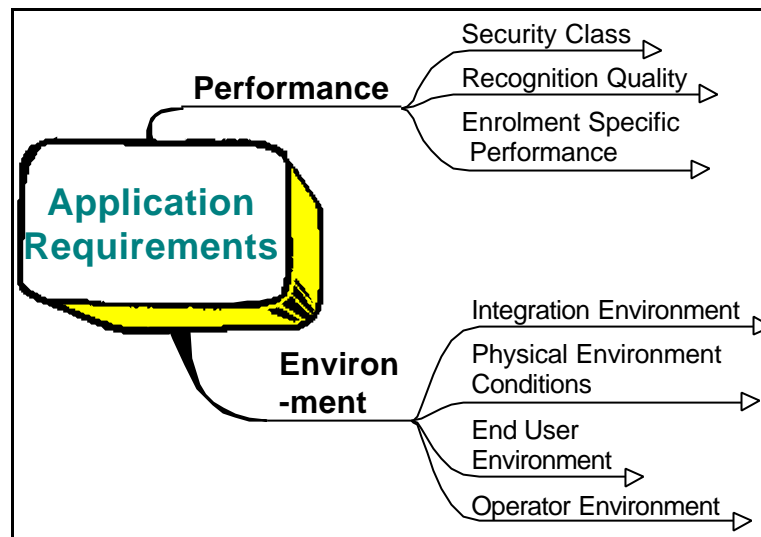
Figure 2: Reference frame for an application pull model



We have described the types of application classes, and a more complete classification of applications in terms of these base classes has been developed during the course of this project.

Each player in the value chain will have different requirements for a specific application. The complete set of requirements, even for a relatively simple deployment, could be quite complex, and work is underway to define such a complete set in more detail³⁴. Figure 3 illustrates some of the dimensions of the set of Technological Requirements.

Figure 3: Requirements for Applications with Biometric Identification from the Operator's viewpoint



The third dimension in the application pull framework is the perspective of the market players. We have identified the following players, although there may well be others, whose identity and role will surface during detailed analysis of exemplar applications:

1. Sensor manufacturer
2. Algorithm and software developer
3. Biometric system integrator
4. System provider
5. End-user

3.1.4 The 'Application-Technology' Compiler

The final analysis tool is the Application-Technology Compiler, that assesses the extent to which a specific technology matches the requirements of an application in all - or only some of the dimensions - of a specification. Figure 4 highlights certain dimensions for which one technology may be the most suitable, such as Technology B in the case of Scalability, where the metric (or 'Intensity') as measured in a standardised manner shows that Technology B does not reach the threshold for adoption in this application. Technology A, however, reaches it in this application. Clearly a set of profiles for each technology and application would be a useful analysis tool with which to understand to what extent current technological implementations fall short of the minimum required to justify deployment of cost-effective, appropriate and user-friendly applications in Europe.

³⁴ A summary of the current status of this methodology is available as a BIOVISION deliverable: Michael Behrens and Maik Weber, *Report on technology and application issues for biometric identification systems* (July 2003)

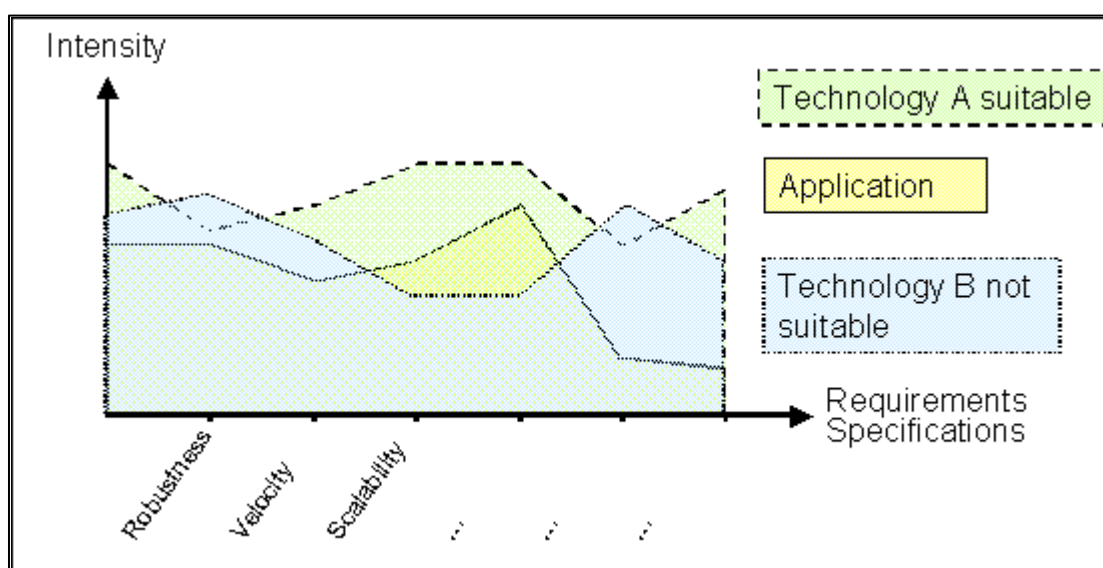


Figure 4: Compiling the 'Intensity' of technologies and applications

3.2 Specific applications - the use of scenario modelling

In order to understand the future opportunities offered by the widespread use of biometric devices, the BIOVISION partners used a mix of techniques, spanning traditional forecasting methods (such as the Delphi) approach and scenario-based modelling techniques aiming to offer alternative views of the future, rather than committing the participants to a single view.

The scenario approach, which is perhaps less familiar to readers will be described in some detail. There are a number of recent books that explore this technique in even more detail.³⁵ This method attempts to integrate the accumulated knowledge of a team as to i) drivers, ii) well-established projections and the iii) the unknowns in a situation set some time into the future. Clearly the more diversity in the group the less constrained will be the range of possible scenarios created, provided that the members are willing to work together constructively.

The scenario experience brings together a group of experts both in the field and related areas over one or two days - under the direction of an impartial moderator/facilitator - with the aim of answering a problematic area relevant to the needs of an organisation. There may also be some outsider 'wise men' and creative people whose aim is to free up the discussion from the predictable directions that have been already well-rehearsed at conferences and in consultants' reports.

An introduction positions the method as neither being crystal ball gazing into the future on the part of a small group, nor a debate between opposing viewpoints in the world as it is today. Its aim is to uncover the real forces that will shape the future of an industry, a company or a country. The resulting output of such a workshop should acknowledge the uncertainties in the forecasts, but the act of working together as a team will have dug deeper into the unconsciously held knowledge of all of the participants.

After the introduction, the process continues in the following way.

³⁵ Kees van der Heijden et al, *The Sixth Sense - Accelerating Organisational Learning with Scenarios*, John Wiley & Sons (2002)

1. The question is clarified in as much detail as is appropriate to the circumstances, by agreeing the key issue, so that the participants are able to test its relevance to the scenarios that are developed subsequently.
2. The next stage identifies the key driving forces at work that will shape the future, in the areas of social dynamics, the economic context, political developments and technology changes. Some of these forces in these four sectors will be easy to forecast: they are predetermined (e.g. the age and gender distribution of those who are already born), whereas some are subject to a great deal of uncertainty. The scenario building process should aim to isolate the major areas of uncertainty that relate to the key question, and understand the relationships between the driving forces that will impact on the key question. This may be carried out through an exercise that asks each participant to individually identify and write down the key forces. These are then collated on a board, and organised into common themes.
3. The matrix of uncertainties. This phase aims to collect the major uncertainties into at most two related groups, each of which are plotted along two axes at right angles with high-low measures in each dimension.
4. Four stories are developed in the four quadrants of the matrix, corresponding to HIGH-HIGH, HIGH-LOW, LOW-HIGH, LOW-LOW, but recognising that none will really come to pass. Indeed the real future will be some mix of all four worlds. Note that the stories should not be selected as particularly extreme cases of 'good' and 'bad' worlds (hence the need for an experienced facilitator to avoid such extremes). Each story or scenario is named to identify them in future discussions.
5. Two or four of these stories are expanded in syndicate groups whose leaders report back in plenary session. Discussion continues to refine the scenarios and note similarities and differences. Rapporteurs write out the scenarios for future more detailed assessment.
6. Over subsequent meetings, the implications of the scenarios for the interested organisations are explored.

3.3 Specific applications: the case of physical access control

This scenario modelling exercise was the first undertaken in this roadmap project, with the participants being drawn exclusively from the BIOVISION partners and contractors. The independent facilitator (as in the subsequent workshops) was Dr. Michael Lyons of BT Exact Technologies who has many years of experience heading the BT Business Modelling group. The introductory sessions explained the process of scenario modelling, giving examples of how it has been used in a high technology context.

The forming question, aimed to assess the drivers and inhibitors for the widespread adoption of biometric methods for access control into campuses, buildings and rooms, was circulated in advance of the meeting:

How will biometrics be used for physical access control by large organisations in Europe in 2010?

3.3.1 The scenario process

The exercise commenced with participants individually listing their views on the main drivers and factors that would impact the widespread deployment of biometrics in this application by 2010. Each driver was written on a separate 'Post-It' note and placed randomly on the whiteboard. At the end of the 30 minute session, these notes were organised into themes, led by the facilitator, but with the co-operation of the participants.

The next stage consisted of placing these themes on a two-dimensional grid with axes of uncertainty and importance, so as to identify the most important and uncertain issues. Three areas emerged: *User Reaction*, *Physical Threat* and *Legislation*. After a discussion, the *Physical Threat* was taken out of consideration, and a 2x2 matrix of the other two themes yielded a set of four world scenarios, of which two were selected for investigation by two teams selected randomly by the facilitator. The aim was to create a story line for each of the scenarios together with a realistic description of how the world would have evolved towards this situation.

3.3.2 Outputs from the exercise: Issues (drivers and other key factors)

The following were the contributions by the participants as written on 'Post-It' notelets, organised by the themes into which they were finally placed by a joint decision-making process of the participants:

Miscellaneous (did not fit into other categories)

- Developments in beauty surgery
- Failure by 'driving countries' to listen and cajole the 'hesitant countries'

Economic

- Global recession
- Further economic recession

Office Security

- Dishonesty of security personnel
- Increase in subcontracting of cleaners, etc
- Easy to get someone's entry card and engage in industrial espionage
- Increasing variability of the workforce
- Multiple occupancy offices - so need to stop unauthorised people moving into your space
- Part of a 'fun' environment for creative organisations
- Increase in the use of smart cards in other applications
- Strengthening of alternative technologies
- Can't afford security staff for a small (e.g. 2 person) office for a company with many small offices
- Trend towards staff working from home - large organisations don't own buildings

Cost

- Security guards cost money and they will cost increasingly more as additional govt regulations come into force
- Cost saving (re: security staff)
- Cost of security personnel
- Cost of tokens and consistency of supply
- Intensive use to reduce costs
- Costs
- Cost saving
- Increased availability of cheap and robust biometrics
- Proprietary systems and willingness to standardise systems and products
- Standardisation (twice)

Legislation

- Privacy policy increasingly requiring 'self protection'
- Legislation requiring company to know who is in building at any time

- Legal requirements in workplace - 'hot desking' means you don't know who is in the building
- Biometrics are mandated
- External Legislation and related developments
- Conformity with data protection issues and directive
- Legislation - positive and negative
- Big Brother fear
- Trend to more legal 'framework' and self-regulation (US approach also in Europe)
- Increasing fear of no longer being able to control personal data
- Integration with existing systems and support
- Lack of respect for privacy and data protection rights
- Assign actions to individuals (accountability)
- Reliable responsibility for electronic transactions
- Privacy organisations successful in getting biometrics banned
- Internal audit requirements
- Need for reliable legal transactions in electronic transactions
- Not feeling disadvantaged and oppressed in comparison with colleagues not having biometric access (psychology)
- Discrimination
- Requirements of people to be anonymous in a networked /linked world

Technology

- How will we trust computers in 2010?
- The effectiveness of biometric being undermined by another technological advance
- Access control a by-product of time and attendance system
- Dispute (cause and resolution)
- Failure of other mechanisms like PIN/Passwords in relevant transactions with new technologies like electronic signatures
- How will the key and PIN/password market react?
- No 100% decision with biometrics³⁶
- Scalability
- PINs and tokens repeatedly compromised
- Maybe we have 'better' solutions for access control
- High turnaround systems will be required
- Touchless sensors will be preferred
- Technical improvements like robustness and scalability
- Throughput
- Performance (Rejection)
- Security

Physical Threats

- The security used to store the tokens being compromised
- Bigger inequality between 'haves' and 'have not's'
- Major security breach/leak, Incidents of transgression against the organisation
- Increase in direct activism - fear of activists getting hold of cards and disrupting your work or gaining access to your information
- Increasing fear of terrorism
- Another terrorist attack
- Physical threats

Health and Safety

- Health concerns around technology

³⁶ In contrast with the assurance that a password matches the reference one.

- Health and safety
- The technology must be totally safe for users
- Governments will be first - global companies will follow
- Enormous power of technologists
- It will be used to stop people from a blacklist

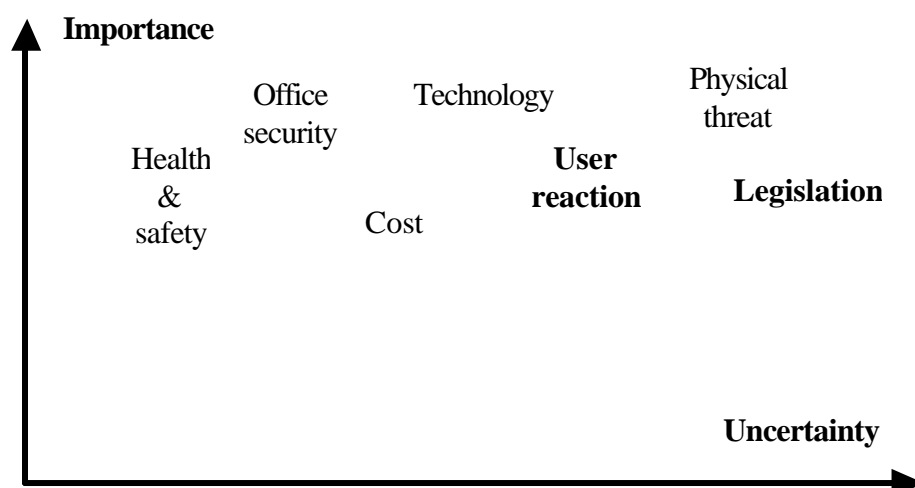
User Reaction

- Geographical environment (changes, etc)
- More strict environmental regime in order to protect own country/public buildings
- Incentive to users (The users must gain something using a biometric system)
- External PR consideration in reaction to social trends)
- Willingness of people to use their body in order to authenticate themselves
- Consumer fears, Media: lack of support
- Perceived benefits - not necessarily qualified - but understood from the political perspective
- People more likely to embrace biometrics if they have experience from work
- Is it a must? or a can? -> what if people deny?
- The ability to use the access control biometric in other areas outside of the business
- No one will discuss it anymore
- The trade unions will not be an obstacle to the biometric process - agreement with the trade unions
- The user's associations should approve the technology - agreement with user's associations.

3.3.3 Output: Themes displayed on axes of Importance v Uncertainty

These themes were then positioned on the following two-dimensional graph to identify those two themes that were both very important and highly uncertain. This process resulted in vigorous debate, although the participants recognised that relative positions of the themes was of significance, rather than their positioning in absolute terms on the figure.

Figure 5: Importance/Uncertainty Plot for Physical Access Control

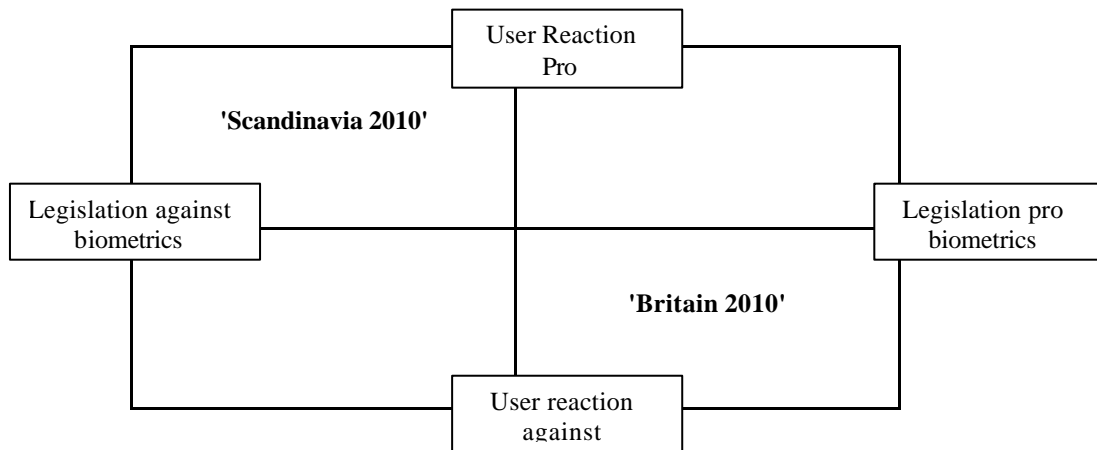


The two themes that were selected were *User Reaction* and *Legislation*. A discussion ensued on the naming of the four scenarios. In view of the limited time, only two scenarios were named and the group split into two syndicates to develop the scenarios in more details.

3.3.4 Output: 2x2 Matrix for Case of Physical Access Control

The naming of the quadrants was as follows:

Figure 6: 2x2 Matrix for Physical Access Control



3.3.5 Output scenario: 'Scandinavia 2010'

Origin of scenario name: Scandinavian countries are seen to be more advanced and receptive to novel systems (e.g. Finland with its high penetration of mobile phones), but seem to be quite proactive to support the rights of the individual.

Scenario Offices in the new age of biometrics are characterised by workers in them feeling safe and secure. PC security is no longer a problem with the use of semi-continuous, user-friendly authentication. Partly this comes about through the tough regulation that requires strict controls on security and use of biometrics, and allowing the introduction of biometrics only with the vote of an overwhelming majority of workers at the place of work. The fully audited use of any biometric data is controlled by clearly defined security countermeasures and processes that are laid down as the result of European standards, that - for example - enforce separation of data relating to biometric authentication from any other data in use by the company. New entrants to the company are introduced to the technology through a 'fun' game that makes the enrolment process simple and easy to understand.

Much of the template data is stored on a smart card that also doubles up as an electronic cash card. In case of loss of this card, there is a backup process that uses encrypted data of the part of the template held in a database, supported by a positive authentication by two of the colleagues of the person whose card has been lost.

Two biometric systems work in harmony to gain the best of identification (iris scanning for entry to the offices and access to e-cash services and ensuring positive assent to a an electronic transaction) and semi-continuous verification of identity whilst on line in the ambient intelligent terminals that support the work of the office (face recognition). Wireless LANs mean that the camera-equipped terminals can work anywhere (except where blocked out for personal or security reasons). When a transaction is required, the terminal is brought close to an iris portal and an interchange between this and the terminal results in a date- and time-stamped authentication that is wrapped into the digitally signed message.

How did we get here? During the early application of biometrics to the workplace in the USA there were no safeguards. In a number of headline-making cases, the FBI managed to use the minutiae data in the company's databases to look for matches to a small number of fingerprint records in their files. Although such a computationally intensive process

would only have been possible for specific cases, the fear was that faster computers and specialised processors would make this a more feasible option in the future. In a South East Asian country that had used a common biometric application for government and commercial applications, the governing party had made use of the system (not the biometric itself) to target dissidents and this had caused a furore in Europe.

Moreover, hopes for Biometric Privacy-Enhancing Technologies that would preserve anonymity - whilst ensuring strong authentication - never took off, with the result that stronger legal sanctions were the only way to protect the individual's rights. Of course, the privacy and civil rights lobby were able to write in very strict controls, as there was no unified biometrics voice in Europe that could speak up for the industry as a whole.

What had not helped was the general increase in fear of technology when studies had shown that there was a small, but measurable effect, of cellphone radiation on the health of individuals. This discovery had led to questions about the long term effects of infra-red light sources used in certain biometric systems – even at the ‘safe’ low levels.

3.3.6 Output scenario: Britain 2010'

Background: The governments have been keen to make use of biometric security systems and have provided legislation to support their use.

The general population is against the use of biometrics.

Scenario The governments have made the use of biometrics for personal citizen ID mandatory; this was done without full consultation and general consent. On the back of this legislation public and private bodies introduced biometric systems to expedite their own interests. As a consequence there is a proliferation of biometric systems to the extent that citizens view them as overbearing.

How did we get here? There is a growing lobby of public opinion that opposes what they see as an overly prescriptive regime in favour of the use of biometric systems. This has come about as a consequence of several well reported incidents including:

- The loss and theft of biometric tokens from poorly and unsecured systems.
- The rising incidence of identity theft that, due to the level of confidence placed on biometric evidence, resulted in the victims being unable to prove their innocence.
- Major security breaches perpetrated from the acquisition of false IDs from biometric systems. Incidents of this nature have led to a large public lack of trust and certainty with regard to biometrics.
- There is also public disquiet surrounding several aspects of the use of biometric systems which have led to a perceived loss of personal individual freedom:
- The inability to remain anonymous in many situations.
- The inability to carry out normal practices, e.g. a wife uses her husband's ATM card.
- The mood of disenfranchisement by citizens leading to a feeling that they are regarded as identity numbers rather than individuals.
- The possibility that there are health threats surrounding the use of some biometrics which have never been satisfactorily examined.
- The proliferation of trade amongst commercial organisations of biometric data.

- The use, by government agencies, of privately held biometric data to carry out surveillance on citizens.
- The use, by commercial organisations, of biometric data to carry out intrusive marketing campaigns.
- The marginalisation of people due to blacklisting, failure to be able to enrol in systems due to racial/ ethnic/ethical grounds as well as the inability to enrol or use certain systems.

The public are irritated by the costs of setting up and maintaining these systems which have been passed on to them by the Government and commercial organisations. There is a growing groundswell of opinion that calls for the tighter regulation and licensing of biometric systems; lobby groups form to pressurise the governments into formulating and enforcing data protection and privacy regulations for the use of biometrics. Commercial pressure groups press governments to maintain the status quo pointing out that any changes would lead to huge implementation costs.

The Governments are happy with the current situation as they can use biometric data without hindrance. Also, they fear that any change that were made would lead to a proliferation of changes that would add greatly to their legislative overheads. They advocate the self-regulation of the commercial sector with schemes of best practice and code of conduct. They refuse to include biometrics in any specific health and safety legislation under the pretext that no firm evidence of any risk has been proven.

3.3.7 Discussion

Security

Current levels of performance are generally adequate for likely applications in this area

Spoofing is a key security issue that can be countered with effective liveness testing. Supervised operation may be effective in some circumstances but it is not always effective where artifacts might be inconspicuous (e.g. fake laminar fingerprint stuck on top of normal fingerprint), and it may not be feasible for out-of hours use (e.g. access by cleaning staff).

Privacy is not a major issue in self-contained applications. The user population is likely to be limited in size (e.g. employees) and cooperative.

Failure to enrol may be a problem, particularly with larger scale applications. The system may become dysfunctional and rely too heavily on fallback measures.

Different trust levels of user population (e.g. regular staff, cleaning staff, third party users) may be a problem; however this is not specific to biometric access control systems.

Larger, multi-function applications may present additional problems e.g.

- Integrated biometric system used for access control and payment for canteen food or other services. Privacy of data that may be used by third party service providers
- Compartmentalised systems with disparate security requirements and implementation. If the highest level of security requirements are not applied uniformly, compromises at the low level points in the system may be used to launch attacks on high level parts.

3.4 Specific applications: financial application of biometrics

This application was one of two examined during a workshop on large scale system opportunities in biometrics. The forming question was:

What will be the use of biometric methods in large scale financial applications in 2010?

This section should be read in conjunction with Section 6.5 that summarises the near term outlook for the use of biometrics in this sector.

3.4.2 Outputs from the exercise: Issues (drivers and other key factors)

Inhibitors for Financial Applications in 2010

User Issues.

Acceptance:

- Media objections
- Rumours
- Bad press
- Low user trust
- Trade Union objections
- Biometric may drive customers away
- Politics of single persons
- Biometrics may put customers off.

Usability:

- Difficult to use
- Banks close down branches
- How do you enrol such a system at home? In a bank with fewer branches?
- User rejection of transactions.
- Genetic engineering. Cloning of live eyes, fingers.
- Population structure e.g. is unfamiliar with technology.
- How to manage users who are unable to enrol
- Lack of awareness. Education.
- Use is made compulsory.

Security:

- How do we create different levels of security?
- High profile case: headline that a dog transfers owner's money to RSPCA.
- Kidnapping for finance theft/fraud.
- Process in beauty surgery.
- Theft harvesting of biometric data. (Spoofing, etc.)
- Ageing population fraud by hospital nursing home staff.
- Terrorist attack.
- User impersonation.
- Low levels of fraud make biometrics unnecessary

Legal:

- Identity fraud harder to revoke
- Details sold to other service providers
- Legislation on privacy (inhibitor) e.g. US or UK legislation prohibits use of face recognition.
- Data leakage to government agencies

- Misuse by service providers.
- Privacy concerns.
- Legal issues (data protection)
- Legal issues.
- User's biometric put on black list.
- Legislation may make secure authentication superfluous.
- Biometric data used for other application. ('function creep')
- Lack of recognition by regulators (world bank/FSA/IMF)
- Who bears risk if thing go wrong?

Cost issues

End user:

- Unemployment
- Risk of loss/theft of money.
- Too expensive.
- High bank charges.
- High cost, expensive devices
- Technology scepticism rejection (computers replaced by humans)

Organisation:

- High development costs
- Instances of fraud
- Major hack results in massive losses. (Barings!)
- Cost for infrastructure.
- Large investment required.
- Unknown benefit.
- Operation cost higher than benefit.
- Owner of networks. Costs for transaction process.
- Structure of financial institutions e.g. infrastructure fails.
- Expensive devices.

Technology issues

Standards:

- Can it be made available everywhere?
- Lack of inter-operability

Applications:

- Can it be made proportional? Anonymous biometric virtual PIN.
- Non-acceptance of technology e.g. iris-recognition. Considered intrusive/invasive or difficult to use.
- Surveillance of transactions.
- Security through bureaucracy.
- Perceived lack of security (not obvious).

Integration:

- Low number of platforms.
- Different systems from different providers.
- Wireless home networks (if not properly secured)
- Interoperability, one system for all.
- Vendors of competitive security technology.
- Lack of penetration of Internet to communities.

- Other alternative technologies.
- Standards not agreed results in biometrics not being used across national boundaries

Performance:

- No channel available.
- Security weakness.
- Reliance on single channel (technology)
- Slow transactions, lack of bandwidth.
- Bad FRR, Bad FAR
- Failed support scenarios.
- Consequence of failure of ID.
- Repudiation of transactions.
- Uncertainty about system performance.
- Technology doesn't work well.
- Breach of security data dumped on Internet.

Drivers for use of biometric methods in financial applications in 2010

User Issues

Security:

- High profile fraud cases involving identity theft.
- Safeguard users transactions.

Acceptance:

- Large scale theft/break-in with on a system not using biometrics.
- Trust.
- High user trust
- Enthusiastic press.
- A service is only provided if a biometric is in place/agreed by user (e.g. home banking needs a biometric at home)
- How industry (vendors) and media communicates the story about biometric systems.
- Other financial institutions have it.
- Good marketing of a service (available if you accept a biometric)
- Social change: the delivery mechanism into the home e.g. home-banking needs verification of user.
- Bodyline scanning: made-to-measure clothes.
- Giving incentives for using biometrics.
- The confidence in buying on line will grow.
- Offering the 'option' of using a biometric

Legal:

Legislation (driver) e.g. US legislation requires use of biometrics.

Usability:

- Ease of use.
- Will stimulate biometrics because of convenience.
- Easy to use.
- User convenience.
- Make service more comfortable.
- Environmentally friendly.
- Number of pins in 2010.
- People will get used at using biometrics.

- Ageing population growth in PC/Internet usage. Home banking bad memory login to PClogon to bank account.
- No need to travel.
- Inconvenience linked to value of transaction.
- Banking at a touch.
- Reduce process times of e.g. bills.
- Ease of access/transactions.

Cost Issues

End user:

- Will it make transactions more expensive?
- 'Pay' on a personal level. Person to person or only business to consumer.
- Save time.

Organisation:

- Increase service penetration.
- Money laundering.
- Close branches save.
- Cost reduction.
- Cash flow of financial list.
- Return of investment.
- Internet fraud will grow.
- Cost of hardware + processing power
- Current transaction fraud is very high.
- Cheap devices.
- Reduce fraud.
- Low cost.
- Reduce employers.
- Declining number of bank branches. Need for phone/PC banking. Digital signatures or equivalent for transactions.
- Sensors and processor become less expensive.

Technology issues

Standards:

- Interoperability. Global availability of biometric-systems.

Applications:

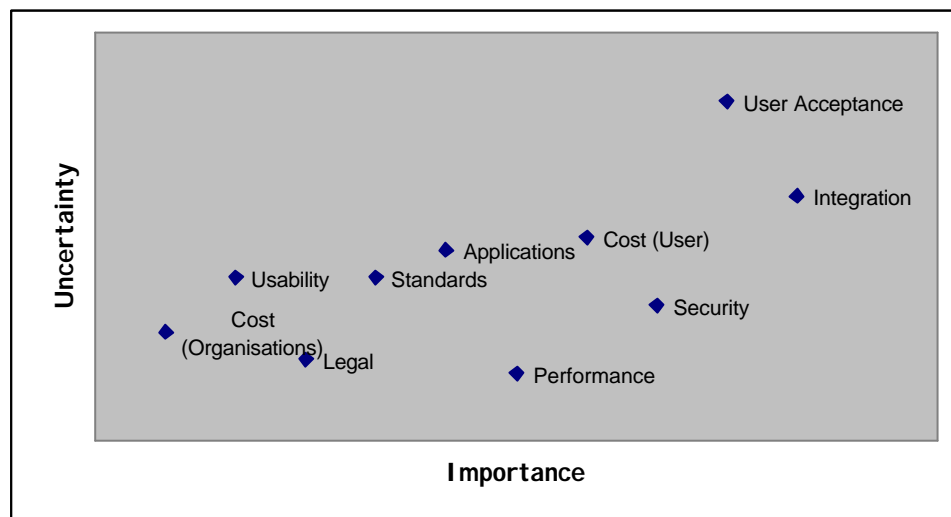
- Video-assisted shopping & browsing.
- Widen range of online transactions.
- Financial institutions want to offer their services on line.
- Technology friendly people.
- Quality of services which need authorisation.
- Need to secure phones/terminals.
- Mobility and teleworking.
- The right biometric for the right purpose (e.g. face-recognition at a distance)
- Ability to produce new innovative services.
- Key applications for biometrics.

Integration:

- Smartcards. Industry/vendors.
- PKI.

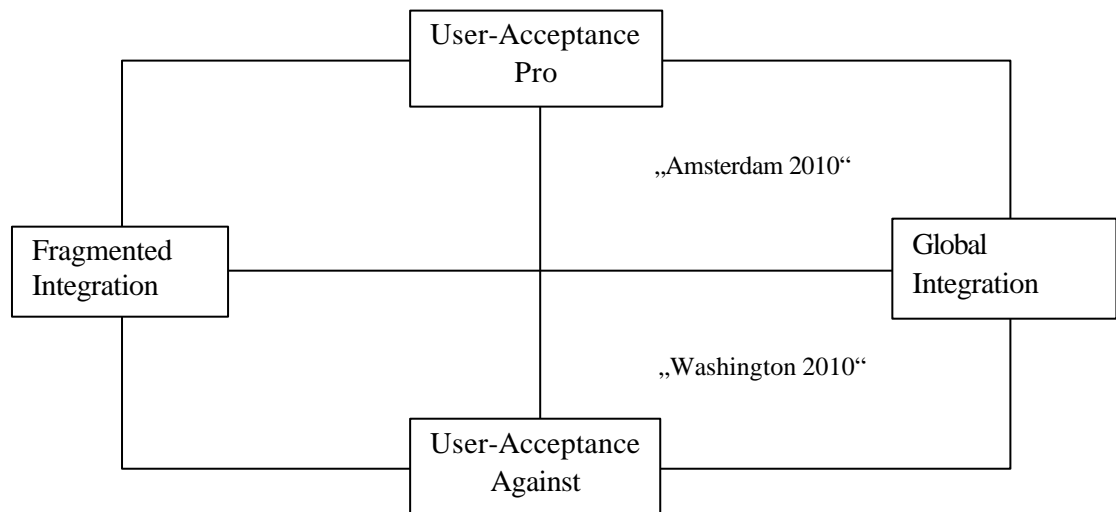
Performance:

- High number of supported platforms.
- Fast.
- Mobility.
- Fallback position or technologies.
- Automatic process without manual intervention.
- Good long term stability of the biometric world.
- Development of multi-modal biometric systems. Progress of life-recognition.
- Trust from valid tests of biometrics
- Good FRR. Good FAR, FTE = 0
- False acceptance of technology. (e.g. London Borough of Newham + people count more cameras even if evidence of success is not proven)

3.4.3 Output: Themes displayed on axes of Importance v Uncertainty*Figure 7: Importance v Uncertainty Plot for Financial Application of Biometrics*

Output: 2x2 Matrix for Case of Financial Applications of Biometrics

Figure 8: 2x2 Matrix for Financial Application of Biometrics



3.4.5 'Amsterdam 2010' Scenario

In order to develop a scenario for 2010, in which the use of biometric systems is highly accepted and biometric systems are globally integrated and standardized, two main questions have to be addressed:

1. How may different visions under these conditions be illustrated in a way that adequately demonstrates that these conditions have been met?
2. How did we get there?

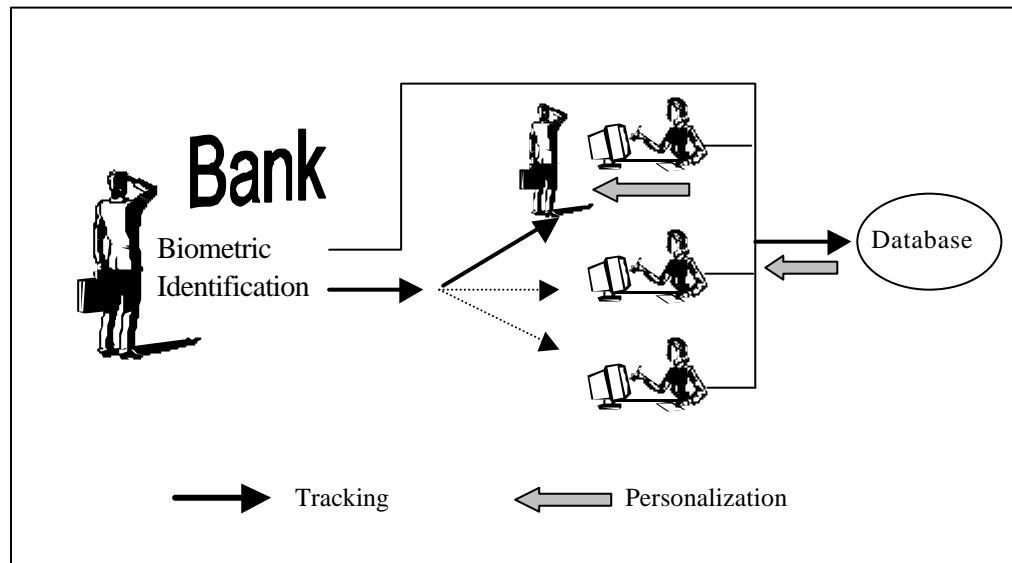
Establishing the visions

1. Customer Recognition

The first vision relates to the application fields “Tracking & Tracing” and “Personalisation” (See Section 3.1.2) using biometric identification systems. An individual enters a branch of a Financial Institute (Bank) where he has an account. The biometric surveillance system identifies him and tracks him on his way to a teller. The bank’s personalisation system will make all of the customer’s CRM information available to the teller. In this scenario the customer has a large sum of money (10,000€) which he wishes to invest. He has previously been interviewed, by a specialist investment adviser at the Bank. At the time of the interview no suitable opportunities were available. However, the bank has just announced a *High Return, Low Risk, Long Term, Investment Bond* that ideally suits this customer’s requirements. The teller is informed of this, on his information screen, and is able to alert the customer to this fact. The customer is given the details of the Bond by the teller, decides that it is a sound proposition and the investment is made, there and then. The goal of this vision is to illustrate how the ability to discretely identify and track an individual can be used to offer a personalised and convenient service.

Figure 9 illustrates this vision:

Figure 9: Using biometrics for customer recognition

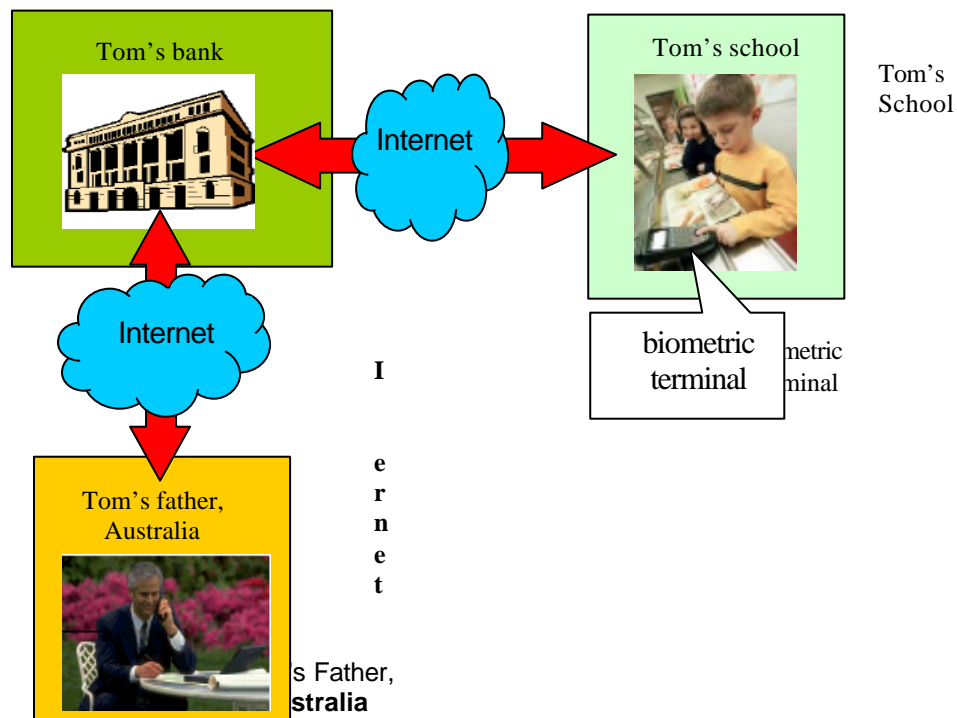


2. Shared bank account

The second vision relates to the application fields “Validation & Verification” for “Privacy Enhancement” using biometric security systems.

Tom is an 8-year-old schoolboy, living in Europe. In order to make the process of purchasing school lunches faster and cash-free his school has installed a biometric verification system, which uses fingerprint technology. When Tom selects his lunch and goes to the POS (Point of Sale), he inserts his *Smart Purse* and verifies the payment by placing a finger on the fingerprint reader, the cost of the lunch being deducted from the balance in his Purse. On one occasion Tom goes through this process but on this day there are insufficient funds in the Purse to meet the cost of the purchase. The POS system immediately contacts the bank, which administers his Purse. The Bank's system is aware that Tom's account is administered by his father and sends an urgent message to him, by means of a mobile communication device, suggesting a transfer transaction and requesting authorisation to carry out the transaction. Tom's father is in Australia on a business trip. He receives the message on the device, and acknowledges his agreement to the transfer using speaker verification. The Bank credits Tom's purse with the agreed amount and the lunch purchase is completed. Figure 10 illustrates the vision.

Figure 10: Using biometrics for a shared bank account

**How did we get there?**

To achieve the visions of 'Financial Applications in 2010' characterized by a high user acceptance of biometric systems and a global technology integration, the participants of the Amsterdam 2010 Scenario determined the following milestones:

- Legislation
- Education
- Global Co-operation
- Technological Advancement

The actions that would need to be achieved in order to meet these milestones are:

Legislation

- Regulations on Finance
- Strong legislation on the secure use of biometrics
- Effective European Data Protection Act

Education

- The European Biometric Forum co-ordinating media dissemination
- Sponsored socio-economic research
- Sponsoring of large scale biometric system pilots

Global Co-operation

- Championing International Standards
- Drafting International Legislation

Technological Advancement

- Promoting Interoperability
- Sponsoring and Promoting Technical Research
- Developing links between research and industry

3.4.6 Washington 2010' Scenario**Scenario description***Step 1*

High availability. A major application (for example, biometrics on ID or 'entitlement' cards, introduced by one or more EU governments in response to mounting pressure to deal with the growing problem of illegal immigrants) has created a standard (*de facto* or proscribed) for the implementation of one or multiple biometrics, and created an integrated market. This has led to a supply of low-cost readers and software together with an appropriate infrastructure.

Step 2:

Credit card issuers and/or banks use this opportunity to agree to use the same biometric(s) on credit and cash cards. All customers receiving new cards are requested to register one or more biometric for those new cards, and existing cardholders are encouraged to swap theirs as soon as possible. Persistent 'refuseniks' are issued an old-style card, but

- customers are told that cash dispensers that do not require biometric identification will be gradually reduced, and
- credit card transactions over the certain amount are not authorised or insured unless biometric identification is used.

Legislation lags behind introduction of the application (e.g. responsibilities for safekeeping of biometric identifiers have not been defined).

The process of registration and safekeeping creates additional bureaucracy with the financial institutions, which inconveniences customers and increases the cost of running the system.

*Step 3:***Bad experience and a lack of perceived benefit results in low user acceptance**

Bad experience: Several of the following occur and become public:

1. Misuse of biometric ID data by government officials or employees of financial institutions.
2. Cases of fraud involving identity theft by employees of financial institution or third party. (Made worse if prosecution fails because the legal system lags behind.)
3. A poor implementation or incompetence in registration/data safekeeping creates confusion.
4. Usability problems (with reader, or delay in any part of authentication) leads to queues at cash dispensers and sales terminals.

Lack of perceived benefit: Several of the following occur and become public

1. Banks close local branches and reduce counter staff; banks and credit card centres replace staff in call centres with automatic phone transaction systems and/or self-service Internet services.

2. Trade unions object to job losses in financial sector, which they blame on increasing automation.
3. Customer perception of low quality of service, due to lack of “human touch”.
4. Customers see no financial benefit from introduction, maybe even increasing cost because of increasing bureaucracy.

Complete list of drivers

High availability:

- Coherent standards
- Low infrastructure costs
- Coordinated responsible approach by EU and governments.
- Big application need will mainstream biometrics
- *De facto* standards through market dominance (Microsoft, DVD, CD, GSM)
- Mainstream products build in biometrics.
- Products are good and useful.
- Acceptance of biometrics by powerful players e.g. smartcard companies and vendors.

Low user acceptance:

- Hostility from customers who feel it is just another technology inflicted on them.
- Media reports say technology does not work.
- Reported cases of identity theft.
- Insufficient time for implementation, testing, refinement and properly managed deployment.
- Technology cannot be improved beyond certain level, e.g. FAR or FRR remains too high.
- Just enough customers are annoyed often enough to conclude “it’s not worth it.”
- Customers feel “personally” rejected by technology.
- Fundamental failure of technology in action leads to crisis shortly after introduction – similar to London Ambulance case.
- Manufacturers and/or vendors fail to listen to user problems and concerns.
- Cost too high.
- Removal of options for customer – threatened or actual penalties for non-use.
- Benefits not clear.
- Build-up of resentment.
- Function creep.
- Data shared between institutions.
- Lack of protection and/or recourse for customers.
- Lack of certainty – technology backlash.

3.4.7 Contributions from the specific perspectives:

Security

False rejection is likely to be a major issue here. Banks and other financial institutions cannot afford to alienate customers. This may result in threshold adjustment that compromises security. However, in financial applications, authentication is likely to be 1:1 verification of identity and the biometric may well be supplemented by other means (e.g. possession of a card), which may mean that the security required by the biometric component is not over-demanding.

Repudiation and legal acceptability of biometric authentication is an issue in cases of dispute.

The perceived risk levels of financial transactions may be quite different from the supplier's viewpoint than for the user. What is an insignificant sum for the bank or supplier may be far from insignificant for the user. Thus the user and supplier view of

necessary security might differ, and the supplier may be forced to implement more rigorous and costly security measures than he would otherwise wish.

Large scale centralised databases of user biometric data may be vulnerable points for directed attacks and will need to be protected. The consequences of disclosure may be more serious than for conventional personal data (which is not directly used for authentication).

Biometric authentication used within the finance company may help to reduce insider fraud through the existence of an audit trail that has stronger binding to responsible staff. In itself, this may have a deterrent effect on insider fraud.

Spoofing is probably not a major issue for the majority of "high street" applications because of the small sums involved, and the limited attacker opportunity and expertise.

Users may be concerned over function creep and the undisclosed use that their biometric data may be put to. Binding of user data (templates) to application and user consent may help in addressing these concerns.

Use of unproven biometric technology in large-scale public applications is a high risk strategy, particularly if it is replacing - rather than augmenting - the existing (well known) security measures.

3.5 Specific applications: monitoring of cross-border travel

This scenario was the second of two examined during a workshop on large scale system opportunities in biometrics. The forming question was:

How will biometrics be used by governments to monitor cross-border travel in 2010?

3.5.1 Introduction

Consideration of this application has been accelerated following the events of 11th September 2001. In particular the US congress has passed the Enhanced Border Security and Visa Reform Act which will mandate the use of a biometric for entry visas into the US, as well as requiring countries whose citizens take advantage of the visa waiver programme to incorporate this type of authentication mechanism. To support these initiatives, a number of activities are underway both in the US as well as in Europe. NIST, the National Institute of Standards and Technology, in the US reported on the technological feasibility of various biometric technologies. Also, in the US, the General Accounting Office has prepared a comprehensive assessment of the technological and economic aspects of the use of biometrics for cross-border security.³⁷ Note that this addresses a very specific set of requirements, and in this scenario workshop, the BIOVISION consortium chose to look more widely than is envisaged in the proposals from the US, and without the constraint of current proposals by European governments. We will return to examine the near term outlook in more detail in sections 6.2 and 6.3.

In Europe, at least four countries are looking specifically at the challenges of including biometrics in national identity documents: UK, Germany, Italy and the Netherlands. In the UK, a proposal by the Home Office was the subject of a public consultation to develop an entitlement card for Citizen-to-Government transactions.³⁸ One option envisages the creation of a national biometric database, which would be the point of reference for all applications for passports, driving licenses and entitlement cards.

³⁷ United States General Accounting Office, *Technology Assessment; Using Biometrics for Border Security*, GAO-03-174 at <http://www.gao.gov/new.items/d03174.pdf>

³⁸ Entitlement Cards Unit <http://www.homeoffice.gov.uk/dob/ecu.htm>

Opportunities for the implementation of biometrics in European travel documents were discussed in a recent conference in The Hague³⁹. The European Commission has also commissioned a study on the current status and future prospects for identity cards⁴⁰.

3.5.2 Outputs from the exercise: Issues (drivers and other key factors)

Security compromise

- National travel documents become easier to forge through excellent digital printing.
- Security of database.
- To reduce fraudulent applications.
- Data might be safe with own government but with others?
- Different sorts of people; different security levels needed.
- Passports can be forged.
- Different security levels in more or less developed countries.
- Compromised biometric in another country.
- An enrolment process within a particular country is flawed.
- National newspapers/media/civil liberty groups demonstrate how easy it is to fool the chosen system
- No system secure enough for European requirements

Failure of Biometrics to work properly; feasibility of doing it at all.

- Breakthrough in face recognition technology means face + digitised photo is unique.
- Available alternatives (double operation) for people who can't supply biometric data.
- Concerns with reliability of solutions.
- Concern with robustness of solutions.
- Use more than one biometric technique.
- Positive trials.
- Biometrically enabling all border crossings not possible.
- Avoid discrimination for people who fail to enrol
- No discrimination.
- ICAO preferred biometric - face recognition - is not up to the task.
- Maturity in functionality and performance of biometrics.
- How would the system cope with power failure or denial of service attack?
- Stability of biometric features (age, illness) has to be researched.
- Biometrics don't work well for young children or babies.
- Failure to enrol.
- Uncertainty about the quality of biometric systems

Interoperability.

- Are there possible gaps with biometric systems?
- Economic disputes between EU + US stop the development of harmonised passports.
- Has to work world-wide.
- Interoperability of standards.
- Inhibitor. Need for interoperability between countries.
- Interoperability.
- Passport must not be forgotten.
- Too many biometric templates needed.... different IDs for different countries.

³⁹ European Conference for Issuing Authorities of Travel Documents, The Hague, 20-21 June 2002

⁴⁰ B&L Management Consulting, *Study on the Deployment and Interoperability of Electronic and Biometric Authentication and Identification* (report to the European Commission, 2003)

- Lack of standards.
- Data formats have to be interchangeable.
- Standardisation.

Efficiency at ports of entry (operators)

- Save time.
- Border control takes at least 20 sec. without waiting.
- Border crossing is more easy and fast.
- Passports have validity times of 10 years (and more).
- Biometric renewal required more frequently than current passport renewal.
- Back-up systems and add human check in case of false reject
- Need to change airport, seaport procedures so biometric check is not side-stepped.
- Big numbers of users.
- Speed up flow of travellers.
- To help speed passenger traffic through airports.
- Time needed to enrol large population.
- Fast transit through congested airports.
- Processing biometrics will slow down current border crossing checks especially in vehicles.
- Entry efficiency at airport/other ports.

Benefits and efficiency for travellers.

- Not mandatory.
- Opt-in or opt-out system.
- Objectors can use same fall-back as 'goats'.
- Gratification for user.
- Lack of necessity to bring paper document.
- Service to passengers.

Fear of abuse. Trust.

- Who owns the data?
- Impression of higher security.
- Trust in Governmental trails.
- Extremely strict privacy regulations and strong civil liberties groups.
- Use of Biometric data to deny entrance/border crossing.
- Guaranteed level of trust in biometrics.
- Respect of human rights and privacy.
- Fear of function creep.
- Biometrics can't be forced upon the people - need to convince them.
- Public acceptance.
- Who has access to my biometric record?
- Where my biometric record will be stored.
- Lack of information.

Biometrics as a country prestige project.

- National prestige being one of the 'first' to introduce biometrics.
- To try and stay one step ahead of fraudsters.
- To create a user acceptable need upon which to build an unacceptable ID card.
- To be seen to be moving with the times by adopting hi-tech solutions.

Government: terrorism threat reduction.

- Strong need for security e.g. to counter terrorism.
- Crime registry control.

- Improve security by detecting criminals.
- Find and identify terrorists, gangsters
- Government fear of terrorists (internal/external)
- Re-use
- Mixed use for governmental and private purposes possible e.g. banning certain individuals
- To reduce multi-applications.
- Implementation of other biometric national ID.
- Combines well with smart card passports.
- Mobile phone becomes the cash/credit card/passport with simple biometric.
- Commercial pressure for fraud reduction and ID theft provision forces government. to act.

Governments' requirements

- No borders; extension of Schengen agreement to all of the developed world. No need for passports.
- Government rules border control.
- Prevent misuse of ID-cards by combining them with biometrics.
- Improve tracking of travellers.
- Secure national border.
- Traditional border control seen as not secure enough. Need for alternatives.
- No *look-a-like* risk with valid ID.

Cost

- Lack of investment by US ports and entry locations to obtain sufficient numbers of adequate readers.
- Technology over-sold. Who pays for damage/penalty?
- Low cost or High Tech approach.
- Decreasing costs in technology but high costs in operational fields.
- It's too expensive to have biometrics at each border control station.
- Costs.
- Too costly. Compared to benefit of reduced fraud.
- Cost-intensive. Personnel-intensive.
- Cost of issuing and maintaining biometric identities?

Alternatives non-biometric.

- Efficient database search of citizens means no need for biometric. No more secrets from government.
- Implanted sensor technology becomes feasible cheaply and quickly.

Legislation.

- Enabling legislation.
- French data protection law stops EU wide cross-border scheme.

Increasing travel.

- Virtual tourism takes over from real tourism as multimedia becomes very cheap.
- Increase in 'green' vote stops growth in tourism and therefore no need for airports of fast track.
- Very high increase in travel between countries as tourism from non-EU, non-US countries takes off.
- Increased cross border traffic.
- Increase in price of oil reduces level of international air travel.

Other countries starting similar schemes.

- To comply with US visa waiver requirements.
- Visa waiver mandates specific US based solutions.
- Border control all over the world. Other technologies used.

Taxation opportunity

- Increase in numbers of retired people.
- Travelling, increase in medical costs – countries want to reduce these costs.
- Tax on tourism becomes a big new form of revenue government.
- A new way to make more money.

Governments seek better immigration controls.

- Political dimensions.
- Need to control asylum seeker flow by knowing who is in the country at any time.
- Helps immigration control, and national agencies dealing with refugees

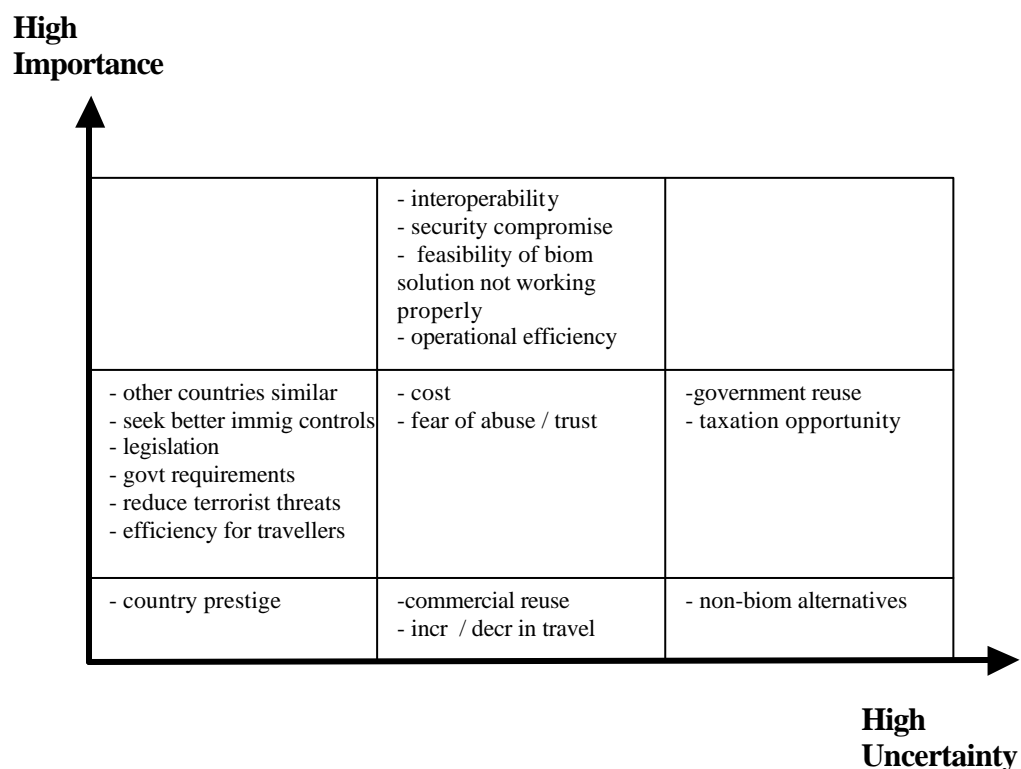
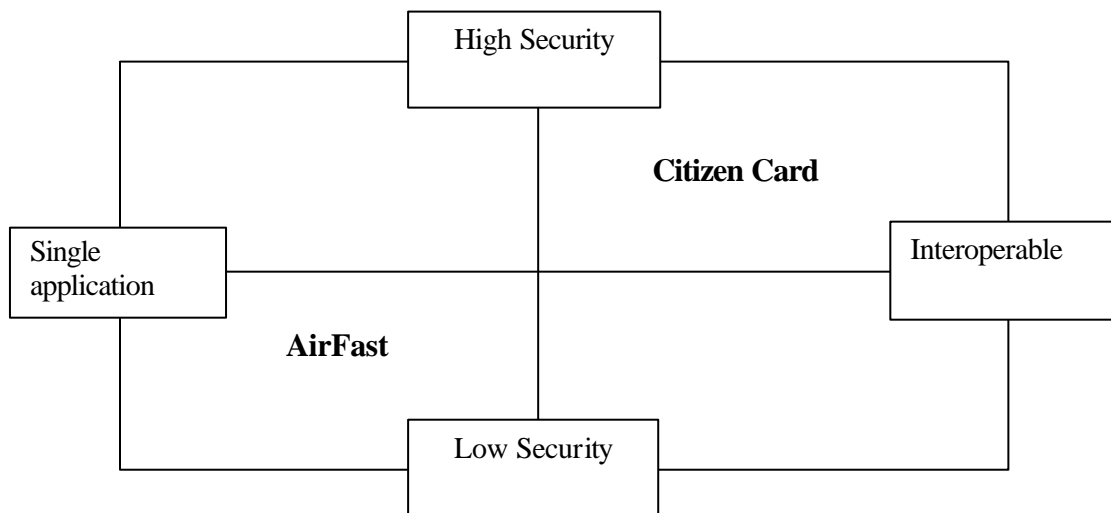
3.5.3 Output: Themes displayed on axes of Importance v Uncertainty*Figure 11: Importance v Uncertainty Plot for Cross-Border Travel Monitoring***3.5.4 Output: 2x2 Matrix for Case of cross-border travel monitoring**

Figure 12: 2x2 Matrix for Cross-border travel monitoring



3.5.5 'Citizen card' Scenario

Mario Rossi is a specialist roofer living in Milan, sometimes working on contract to a major manufacturer of roofing materials. The most popular innovation this season has been the introduction of Verazzo - a new line of terracotta tiles only made by the one Italian supplier. Mario is engaged by this supplier to re-roof a group of houses in Stockholm: four jobs which should take him about a month. He will be taking with him his three man team: Paulo, Giuseppe and Mario.

The Internet way of working is commonplace in 2010, so the use of digital signatures to sign off jobs once they are complete is normal practice. At the same time, Mario can countersign for the team, while simultaneously the tax authorities are automatically notified back in Italy and the guarantee period is started. Biometric validation of the digital signature on a citizen card is now used in preference to the use of PIN numbers. Although there is a choice offered throughout Europe as to which biometric is used, face and voice recognition is preferred by many as many labourers find the use of fingerprints problematic. For this multi-modal system they insert the citizen card into a mobile phone that has camera capabilities.

During his time in Sweden, Paulo develops a toothache, and goes to the local dentist who is able to check Paulo's health record on his citizen card, when both people authenticate correctly to the citizen card using their biometric measures. That's lucky, as Paulo had forgotten that once he had an allergic reaction to the anaesthetic that the dentist was considering using. Checking the validity of his health insurance with Paulo's insurer in Milan is also no trouble for the dentist, but in both instances the amount of information that he is able to read is very strictly controlled in accordance with a Code of Practice to which many entities in the health sector in Europe subscribe.

On the following weekend, Giuseppe goes around the local bars on his own. Unfortunately he gets into a fight after drinking too much alcohol, and the police are called. His citizen card shows the police that he has had problems with excessive drinking in the recent past, back in Italy, and recognising the social offence that overindulgence in alcohol has become in Scandinavia, they offer him the choice of a week in prison in Sweden or to undergo an equivalent period of community service on his return to Italy. Following an agreement between the two countries, entries in criminal databases of the respective states (when not related to major offences such as terrorism) can be checked and added to, provided that the unambiguous consent of a properly verified identity is obtained. In this case, Giuseppe has to make the fingerprint verification system work, albeit with difficulty (a special terminal using ultrasonic fingerprint detection is used to

obtain sub-surface fingerprints). This is checked at the central Italian database using a challenge-response protocol that does not allow the Swedish authorities access to either template or image. Once this method of verification has been used, it cannot be reused until the activity that caused the need for verification is discharged. In this way, the system is prevented from 'function creep'. Giuseppe elects to serve his sentence in Italy..

The next week's job is proving more complex than they had planned, and they need the services of a local builder for a less specialist task. A non-EU national is found at the nearby employment agency and his resident's citizen card shows that he has permission to work for no more than 80 hours a month, that he is a member of the trade association and has a number of signed recommendations by past customers in the optional section of the Swedish card. He is taken on, does an excellent job, and Mario is happy to add his own reference to those already on the card, digitally signed using just his voice pattern, as that level of security is deemed to be sufficient by the trade association.

On the last weekend of their stay, after the work has been completed, the group of artisans decide to take a short break in St Petersburg in Russia. Unhappily, Marco has had his passport stolen by a pickpocket while at the dock, and he only realises that he is missing this document with its visa for Russia while on the ferry. The Russians do not subscribe to the international biometric citizen card convention, so they would normally not allow Marco to land with his friends. Mario remembers that there is an Italian consul in St Petersburg who can issue a 'one off' passport and visa through the use of a multiple fingerprint enabled portable reader that checks higher security level information on the citizen card ... at a price! Marco phones him at the consulate, and arranges to meet the official at the dockside to arrange the issue of a temporary passport with a digitised photograph.

When the four return to Milan, they reflect that it was worth signing up for the full public-private version of the citizen card, rather than applying only for the basic identity card. Even though there was always going to be some doubt in their mind about trust in governments not accessing and reusing all that additional data, it was on occasions such as these that it was useful to have a highly secure store of credentials with different protection mechanisms and varying levels of biometric authentication. This system had not been introduced overnight, but had grown over a period of time, allowing citizens to understand step by step what was involved in these innovations.

How did we get there?

Again, as in the previous example of a large scale biometric deployment, certain prerequisites are needed for such systems to work:

- Legislation
- Education
- Cross-European Co-operation and standardisation
- Technological Advances

Legislation

Identity cards have in the most part been the preserve of governments, and these guard their rights over issue, design and use, especially from use by other governments. The scenario envisages sharing of the use of the memory on a smart card, which by 2010 could allow the storage of many megabytes of data in securely partitioned areas.

Education

Clearly there are many different facilities associated with the card, either stored on the card or referenced through it to a central database. At least three types of biometric will be used, but this multiplicity of authentication methods must be managed by the user in a secure manner. Hence, we believe that one of the costs of introducing such a complex card will be the marketing of its capabilities through an ongoing marketing campaign.

Users will need to be reassured as to the methods employed to minimise the opportunities for function creep, otherwise there will be a significant minority that will refuse to engage with such systems.

Cross-European Co-operation and Standardisation

The particular applications described and their uses across borders will require standardisation and agreements. Interoperability of templates and assessment of the strength of security offered by less strong biometric methods such as speaker verification will need to be realised.

Technological Advances

Much of the technology required to realise this scenario is already in existence, with some of the cryptographic interchanges and security of biometric operation still to be resolved.

3.5.6 'AirFast' Scenario

It is 2010 and biometric authentication systems are routinely used at many airports.

The users

Mr & Mrs Brown arrive at the airport with their children Sam (7) and Rachel (10) on a package holiday to Crete, their first foreign holiday since their children were born. None of them have biometrics in their passports: the adults' passports were issued in 2003, while the children are too young to have stable biometrics. At check-in their face images are automatically recorded.

As they pass to 'airside', a camera checks their face images (against those who have checked in, but not yet passed through to departures). Mrs Brown is stopped as she was looking down at the kids, but is recognised when she glances up, so does not have to use the re-present her passport and boarding card (the back-up system) to the security officer. They are all checked again as they board the plane, to confirm that the same people are boarding as those who checked in.

Herr Schwartz is travelling on business back to Zurich. Again, he has no biometric on his passport, and his face image is used as a biometric to pass through security. While in the business class lounge he is offered biometrics enrolment. His fingerprints are enrolled on a remote enrolment unit, and a 2D barcode encoding the template, passport number, and other enrolment details is stamped in his passport. On his next visit to the UK he will be able to use the automated express lanes to pass through check-in, and passport control.

Mrs White has one of the new biometric passports. She is able to check in using an automated unit, which checks her fingerprint matches the details encoded on her passport. On her return she will use the automated express lane at passport control. She prefers this option to the previous inspections by immigration officials, as it is completely free from racial bias. Previously, she had been stopped and questioned almost every time at passport control.

Technology

The system uses face and fingerprint recognition. (Some countries/airports use iris recognition instead of fingerprint recognition).

Users are tracked through the airport using face recognition operating in one-to-few identification mode. The system keeps track of where travellers should be, thereby reducing the number of stored face templates that need to be checked. Where users fail checks, fingerprint can be used as a backup, as the biometric is stored on the new range of passports. Face enrolments use the face image at check in comparing it with that stored on the passport.

Fingerprint recognition uses the two (usually) index fingers. Fingerprint templates are stored on a smart chip (or 2D-barcode as an interim measure) on the passport, but to save having to read the passport at all the check-points in the airport, the templates are copied in the airport security system, and are deleted once the passenger is airborne.

How did we get there?

In the first half of the decade, airport congestion within airports was a serious problem. The terrorist threat post 11th September 2001 and the additional security checks had exacerbated the problem. Easing the problem by building new terminals was not an option at some of the busiest airports due to local opposition and environmentalist protests. To help speed up security checks and transition of people through the airport, airlines, airports and government agreed to the implementation of biometric checks of passports. Moreover, the US requirement for biometrics on passports or visas brought forward these plans.

Fortunately in 2001-2002 trials had commenced to test the feasibility of such systems, such as those at Schiphol and Heathrow. These initial small trials had been successful and larger trials commenced in 2003. Also in 2002 standardisation in the field of biometrics commenced with a new standards committee for biometrics, which immediately started to address the issues of interoperability.

During 2003, consideration was given to a national biometric ID scheme within some European countries. However it was realised that such a complex system could not be brought into operation by 2007, and would take many years to enrol the population (and would meet with opposition of privacy groups), while the congestion at airports needed to be addressed much more urgently. Instead a simpler scheme was proposed, where biometrics would be incorporated into passports from 2004 (for one-to-one verification only, and one-to-few identification). In the interim (until 2017), travellers' biometrics could be recorded in existing passports as a 2D barcode. Such enrolments could be made at international airports, where in addition to a special office at the airport, passport agency staff had a mobile enrolment unit, whereby they could enrol passengers in the business class lounges.

A variety of trials and user consultations took place during 2004 and 2005 to determine which system the public found easiest to use, and to determine the optimum procedures. As a result, these procedures vary between airports.

In 2004 biometrics started to be recorded in passports. Applicants had to request such passports, and the main use of biometrics was for travel to countries such as the USA requiring biometric visas or passports.

In 2006 the *live and well* features for fingerprint sensors improved immensely, when research projects combining a variety of ideas for liveness tests were completed, and the results rapidly commercialised by the main fingerprint system suppliers. This addressed the main outstanding security issue delaying implementation.

From 2006 all new passports were issued with biometrics⁴¹.

In the first years of operation, the system underwent several biometric security audits, with security improvements having to be made, many of these addressed by improvements in the biometric products themselves.

3.5.7 Contributions from the specific perspectives:

⁴¹ Note that events have overtaken this forecast. As discussed in Sections 6.2 and 6.3, passports with biometric images stored on contactless ICs are due to be introduced from late 2004.

Security

Enrolment integrity is crucial in this application. There will be a need to establish trust relationships between the enrolment services operated in many different countries.

Performance is also a very critical factor. Systems will require fairly good performance in verification mode (where no particular problem is envisaged), but also in negative identification mode against huge populations. This is currently an unproven factor and is questionable with current technology. Potential solutions include: (radical) improvements in biometric technology, or the use of multi-mode biometrics.

There are likely to be large numbers of strongly motivated individuals who are seeking to force system errors so that their true identity (or *alter ego*) is not revealed.

For this scenario, the security of the central database is critical. There is high threat of an insider attack and/or a denial of service attack. The central database is a vulnerable point.

Difficult environments at borders (e.g. at a land border where scanning of individuals is done with them still in their cars) may cause lowering of thresholds to prevent high reject rates and hence poor detection of illegal immigrants.

There will be a need to integrate cross-border solutions and share data internationally. This has many implications for privacy and security, since much of the time the data will be out of the control of a single nation.

Data may be used by multiple parties, e.g. immigration authorities, airline companies, police services. Again, there are many privacy and security issues.

Citizen card scenario

This revisits many of the same issues as for border control. There will be some simplification because the card is limited to a national boundary. However, because of the (intentionally) broader scope of use of the card, security and privacy issues related to multiple functions predominate. Separation of functionality and limitation of functionality in individual cases presents a security challenge. For example a citizen may be enabled for a subset of card functions only.

Issues include:

Should the user authentication be a separate function for each enabled service?

Security requirements for different services may vary.

How to prevent user data leakage between different services?

Standardisation aspects

ISO/IEC JTC1 SC37 is developing the standards for interoperable biometric systems. ICAO has determined that for machine-readable travel documents, the universal biometric will be facial recognition with optional use of fingerprint or iris recognition. Certainly, a measure of interoperability is possible, and by 2010, the use of travel documents with a base level of interoperability should be unquestioned.

Preview of near term developments

In Section 6.2 and 6.3 we will return to consider how moves to create the infrastructure for greater control on travellers (especially those moving by airplane) will make use of biometrics. The security and privacy concerns have been recognised and considerable work is under way to standardise on key aspects of identity cards and other types of

machine-readable documents, together with the interchange formats for exchange of biometric data.

3.6 Synergies with other technology developments

We have discussed future scenarios that make assumptions of the direction in which biometric technologies and applications will develop in the period to 2010. However, there will be advances in other technical systems, and possibly even the emergence of new technologies. It is not possible to predict the extent to which these will be commercialised, and as a precursor to a more comprehensive overview of the societal, commercial and technological future, we offer the following scenarios that were developed at an open BIOVISION workshop in Rome in January 2003.

Prior to the exercise, the participants were invited to consider some of the headline forecasts from the future of other technologies, e.g. ambient intelligence, wearable computers in custom-designed clothing, more natural IT interfaces, better interfaces with knowledge, true multimedia 3G-4G mobility, ... We could anticipate that the performance of biometric systems would have improved by 2010 and that these would have become more secure. Legal concerns could have been resolved, but perhaps new concerns would take their place? The opportunities for better privacy protection, the degree to which governments would become more or less authoritarian, and the extent of the digital divide were all uncertain and would need to be considered in each group's scenario. Examples of how biometrics could work with advances in other technologies were:

- Integration of face, gesture and emotion recognition to provide a more comprehensive package of authentication and profiling
- Intelligent scene analysis could have advanced significantly with cross view handover and interpretation. Small 2cm size processor cubes containing various sensors and miniature CMOS cameras, together with short range networking and small solar cells become available at low cost.

Further discussion of technological developments and political and social trends is postponed to Section 3.7.

3.6.1 Scenarios for technology synergies

3.6.1.1 Scenario 1: 'Italian Mother'

The customer for the 'Italian Mother' service in 2010 has the reassurance that his health and welfare monitoring systems are working on his behalf 24 hours a day. Biometric methods are no longer authentication tools. They are embedded seamlessly into other systems that give a user the feeling of greater personal security and health. Wherever he is, his monitoring systems are personalised and secured by the use of a biometric – whether a conventional one that is available in 2003, or by supplementing this with biometric information from, for example, sensors that measure the quality of a person's sleep. So, authentication is combined with monitoring and tracking of an individual's activities.

Buildings are becoming more intelligent, so that everything from a coffee machine to a shower has sensors that can respond to your preferences as derived from optimisation of your daily routine and assessment of your current needs.

At work, your concentration and productivity is monitored (for your own benefit to help you improve performance), with periodic changes of your environment (temperature, breeze, colour, music) to stimulate or relax you, as and when required. Access to buildings is no longer just a matter of determining whether to allow you inside or not, but more importantly to offer guidance to help you with your visit, whether it is to a hospital,

a public building or an office. Speech recognition in cars responds to the individual driver, so that when he hires a rental car, a downloaded package enables all the settings to be reconfigured to suit his needs and preferences.

This support functionality is distributed between hardware that a person carries on them in the form of a personal trusted device (see scenario 2), and networked support systems with ubiquitous sensors and locally networked knowledge. Much is under the control of the customer, with clear interfaces that enable him to know (and intuit) its status at any time. Although it is possible that the data could be accumulated and used to track him, there are considerable penalties attached to attempting to defeat the complex, interlocking security measures that are in place to defeat attempts to access such data.

Contribution from the specific perspectives

End user perspectives

Clearly this is a commercial offering that will only be successfully marketed if all the components fit together to provide an easy-to-use and valuable service. Ubiquitous computing plays a key role, but so does the effectiveness of the system training and integration between the personal device and networked components. Two groups of people could be attracted to this type of service: the growing number of retired, yet physically able, individuals, who continue to lead an active life, but have concerns about potential health problems. The second group consists of younger people with a high pressure career and involvement in diverse activities outside of work.

The interviews held with current early users of biometrics shows that convenience may outweigh concerns with privacy, provided that the benefits are clear to end users. Such a pervasive system may not appeal to other groups in the population. Amongst these are those people who are not convinced about the security measures and the protection against data aggregation. Personalisation of services and customisation can be carried out insensitively with the aim of using this kind of systems for direct marketing of other services. Also, we can foresee the temptation to obtain an early payback through less investment in the design of user-friendly systems, which could impact on lower take-up rates.

Security

In this application, the issues are mostly privacy rather than security. The main threat is to the user rather than to the application. However stalkers could find out information about users that would pose a physical threat to the user - which is a security issue. If any such system were to be implemented, enrolment would be a key issue.

There would probably need to be an external check on credentials before enrolment was permitted (e.g. does this person have a criminal conviction?).

The user would need to be firmly in control of the functionality. Where external services (i.e. services that are not under the direct control of the user) are involved, the security needs to protect the user from unsolicited services.

There are likely to be conflicts between the provision of personalized services (which implies identification) and the user's right or wish to remain anonymous. These may ultimately be insoluble, and the user may be forced to make a choice between acceptance of the service or retention of his anonymity

3.6.1.2. Scenario 2: Personal Identity Agent

By 2010, a small electronic device has been developed that is biometrically activated by its owner (this could be using voice, finger or face), or perhaps one that only works in proximity of its owner, his identity to be confirmed by some as yet undefined biometric that does not require active behaviour or specific action by the owner but is passively

activated or deactivated. This PIA stores personal and professional information about the owner in a series of profiles defined for various social and professional events/situations. The device is owner configurable to broadcast identify information based on the given event or situation and will retrieve identities based again on user configurable criteria. The device authenticates the identities it receives with the cooperating PIA. (An initial background check and identify confirmation would be required to initially activate the PIA).

Organisers of events can require participants to submit to biometrically verified background checks so that their PIA can be activated for that given event. Possible uses of such a system could include businesses networking, locating individuals at large public or private venues, social networking to identify potential dates or partners (readers can use their imagination here). PIAs could also be used for physical and logical access as well as ID confirmation for border crossing, travel, obtaining licenses, etc. All such possibilities would be highly dependent on the development of secure wireless transmission.

3.6.1.3 Scenario 3: Service Wonderland

- **Technology Synergies:**
 1. Ubiquitous connectivity: connectivity is cheap – all sort of devices everywhere are connected and have an IP address.
 2. Smart cameras: smart cameras become ubiquitous, and replace sensors in most biometric applications, offering contact-free sensing of fingerprint, hand geometry, face.
- **Functionality:** networked devices equipped with smart cameras can recognise persons and retrieve information such as entitlements, profiles, preferences, past behaviour.
- **Scenarios.**
 - **Ubiquitous access.** People can access their own information anywhere, from a personal device (next -generation mobile) or publicly available networked devices.
 - **Intelligent shopping 1.** Shopper enters mall and uses device to specify what she is looking for. System signposts shops that have items and prices. User identifies herself, and goes to shops she is interested in. When she enters shop, rails with specified items in her size move towards her. The shop is aware what she is looking for, and may offer matching items and discounts for purchases. When trying on items, shopper can activate videoconference with significant other/personal stylist/mother/friends to get feedback and help with selection. She can also check whether anyone on the guest list for a particular event has bought a dress similar to the one in which she is interested .
 - **Intelligent shopping 2:** On the way to a birthday party, friends can stop off at book, music or wine store. On providing a biometric ID, they can access the birthday girl's home database, which contains a list of all her book/music/wine items (all items are automatically scanned and registered when they are brought into the house). They can identify her preferences, and whether specific items have already been bought for her already.
 - **Ad-hoc Services:** Carpooling and taxi booking. People transmit where they want to go together with their identity, with the system checking their claim of identity (to ensure personal security) and optimises matches between carpoolers and taxis and customers by current location and destination.
- **Issues**
 - **Personal vs. ubiquitous devices** – what information and functionality do people want on a personal device, what will they use public access points for.
 - **Convenience vs. control/privacy** – safeguarding privacy and retaining control, whilst at the same time maximising benefits and convenience, will require much involvement and work for individual.
 - **Trusted third-party** - required to verify participants in ad-hoc services.

3.7 Societal and technological drivers, inhibitors and wildcards

Although technologies may be mature and the applications appear to be ready for mass deployment, a biometric technology may never be implemented, or at least its start delayed, by other, non-technical, considerations. Examples of these inhibitors are adverse comment in the mass media and interference of unrelated political events. Alternatively, system development and deployment may be accelerated by unpredicted events such as 11th September 2001. Such wildcard events are of course impossible to predict and even to assess the consequent impact on take-up of particular technologies, whether in the timescale over which the impact occurs or the extent to which they hasten or impede their use⁴².

In this section, we list a number of technological developments together with political and economic drivers that are forecast to impact on the lives of people in Europe over the next decade.

3.7.1 Visions of future, non-biometric, technology developments

For many years, BT Exact has been refining and updating a 'Technology Calendar', that brings together inputs from a number of sources⁴³. The timeline below selects some of the possible developments from this resource as an aid to envisioning possible futures. As in the case of scenarios, for the purposes of this Roadmap it is best to view these not as precise predictions, but as indicators of the ways in which technology could impact upon the lives of citizens. Whether these innovations become part of their everyday life depends to a large extent on economic and social factors that are very difficult to predict. Note that the timeline was published just after the 9/11 events, and before the full impact of the 'dotcom' crash became evident. Some of the predictions for 2003 have been included to indicate those developments that were considered to be imminent at that time.

Demographics		
2010	25% of the UK workforce are teleworking at least 2 days a week 40% of paid workforce will be women (worldwide) World population of over 65's increases by 1 million a month	
Business		
2003	Air mouse and air typing	
2004	Displays with image quality comparable to paper	
2005	Paperless working is the norm internally in most UK businesses 3-dimensional fax Polymer screen advertising billboards Talking head technology used in public terminals Voice synthesis quality up to human standard Full voice interaction with machine Totally managed world logistics systems 1 billion Internet users 1 billion Bluetooth devices worldwide TV Internet users overtakes computer-based users	
2006	Software trained rather than written	
2007	Lifestyle brands predominate Portable translation device for simple conversation	
2008	Universal monitoring of all business transactions 'Expert system' software competes with lawyers, doctors and other professionals	GWU
2010	95% of people in advanced nations are computer literate	

⁴² John Petersen, *Wild cards in our future; preparing for the improbable*, The Futurist pp43-47 (July-August 1997)

⁴³ Ian Pearson and Ian Neild, *Technology Timeline*
<http://www.btexact.com/docimages/42270/42270.pdf> (Issue 1, 21 November 2001). Other dates from timelines prepared by

GWU: George Washington University Forecast (Newsweek, 18-23 September 2002)

	Virtual companies and co-operatives dominate the business world Inter-business financial transactions are all electronic Solar reflector satellites bringing sunlight to major Northern cities Computers used for creativity enhancement	
--	---	--

Manufacturing and Computer Hardware		
2003	Use of molecular computing	
2004	Smart paint available (contains ICs) Tactile sensors comparable to human	
2005	New engineered organisms used to produce chemicals Odour and flavour sensors comparable to human Semiconductor devices based on 0.01 micron technology Solid state replacement for CD Fire-fighting robots that can find and rescue people Fractal shape-changing robots	
2006	Activators make any household object First artificial electronic life	
2007	Optical neuro-computers Totally automated factories	
2008	Anthropomorphic robots used for factory jobs	
2010	Green manufacturing and renewable energy blossom Self monitoring infrastructures using smart materials and sensors Homes made in prefabricated modules Radio transceivers in all Intel's silicon ICs Molecular sized switches Self organising adaptive Ics Quantum dot memory using 20nm dots: 50 Mbytes in a full stop DNA storage device 1 Terabit memory chip Optical Card storage- replaces CD, VHS, audiotape, magnetic disc	GWU

Government		
2005	Half of all UK government services are delivered electronically Global electronic currency in use	GWU agrees
2007	People reduce tax liability by being paid partially in information products	
2008	All UK government services delivered electronically E-mail used to communicate with most social security claimants Replacement of people leads to anti-technology culture Widespread online voting in the UK	
2010	Effective prediction of most natural disasters National UK decisions influenced by electronic referenda Universal ID card in the UK	

Defence and warfare		
2005	Soldiers fire weapons remotely Crime and terrorism mostly computer based	
2007	Remote override capability on planes	
2010	Insect-like robots used in warfare Most fighters and bombers flown remotely Most weapons attack systems rather than injure people Attacks based on facilitating natural disasters	

Education		
2004	AI teachers in school	
2005	Widespread use of virtual reality for education and recreation	
2007	Network-based learning causes polarisation in classes – streaming is essential Global classes used for multicultural immersion	
2010	Superstar teachers use telepresence to lecture to dispersed classes Personalised degrees are awarded based upon performance and understanding of individual lectures Translation software replaces foreign language teachers	GWU

Health and medical		
2003	Smart pills with chip dispensing drugs Kitchen food tester that identifies the presence of food poisoning bacteria ICs on food packaging tell when food is at its best Various forms of electronic addiction	
2004	Telepresence used extensively in rural clinics Retinal implants linked to external video cameras Instant electronic diagnosis of illnesses	
2005	All patients tagged in hospitals	

	Designer babies Synthetic retinal implants for simple vision Electronic prescriptions reduce fraud and improve speed Electronic patient records become valuable data mines Brief human suspended animation Frequent use of multiple identities causes personality disorders	
2008	Neural networks used for patient appointment management Hospitals use virtual queuing systems Expert systems used extensively in GP surgeries Holistic healthcare gains widespread acceptance	GWU
2010	Online surgeries dominate first line medical care Direct electronic pleasure production Use of human's own tissues to grow replacement organs Operations videoed and stored as part of the multimedia medical record Lifestyle monitoring and insurance linked to medical records Genetic screening widely used Devices roaming within blood vessels under own power Make-up by numbers Active contact lens Video tatoos	

Home Life		
2003	Electronic paintings	
2004	People cyberspace wardrobe Cash badges	
2005	Clothes collect and store solar power Video tiles, Fibre optic plants in gardens, Video photo frames Jewellery that changes shape and colour Emotion badges Polymer video screens built into clothes Personal shopping tablets; shopping lists automatically complied by supermarkets Living area use of virtual reality scenes	
2007	AI systems to understand text and drawing (e.g. patient information) Domestic appliances with personality and talking head interface Emotional objects, switches, etc around the home Electronic cash migrates from the Internet onto the high street as paper and coins largely replaced by electronic cash Kaleidoscope clothes using materials with embedded pigment micro-capsules	
2008	Personalised response from household gadgets Electronic newspapers and magazine tablets Majority of people use PDAs Digital bathroom mirror 10% of UK shopping is electronic Cars with automatic steering Position monitor ICs built into cars	GWU
2010	AI houses that react to occupants Voice interface for home appliances Mood sensitive light bulbs Electronic wallpaper Anti-noise technology built into homes Washing machine aware of contents and selects cycle ICs in packaging of food control its cooking 90% of telephone calls are tetherless All new cars fitted with basic cellular communications with automatic distress systems Urban car co-pilot	

Leisure		
2003	Cyberspace make-up	
2004	Action man toys engage in war games over networks Toys with network based intelligence Garden audio systems	
2005	Toy soldiers with video camera eyes enrich play Voice control of many household gadgets Personalised adverts on TV and radio Video walls - single screens 2m across Most portables powered by fuel cells Conferencing technology for remote socialising in public places Cameras built into glasses recording what we see Theatres gain extra revenue by allowing internet attendance Smart tickets for navigation through airports Assisted lane keeping systems in trucks and buses	

2006	Emotionally responsive toys and robots	
2007	People have virtual friends, but don't know which ones	
2008	Virtual Reality overlays on the real world Automated real life highlight channels on digital TV	
2010	'smelly telly' using ICs with small reservoirs of chemicals 25% of TV celebrities are synthetic Separate volume controls for different people in a room Social software organising functions Loneliness in aged population greatly reduced by networked communities Robotic dolls and pets account for 10% of domestic telecom traffic	
Security and law		
2003	Devices registered in homes and will not work if stolen	
2004	Security Barbie used for locating lost children	
2005	Behaviour alarms based on human mistake mechanisms Cheap miniature cameras cause social backlash Video surveillance built into telephone boxes Neighbourhood intranets	
2008	Net chat sites insist on proof of identity Robotic security and fire guards Law: logic checkers highlighting contradictory evidence	
2010	Neighbourhood video surveillance networks, but surveillance of neighbours becomes a problem Household access by facial recognition Extensive use of electronics to monitor police behaviour Criminal tagging augmented with video and audio sensors Computer advice to jurors on probability issues	

Table: Example Timeline of Future Technologies (November 2001, contributed by BT Exact)

The impact of two major events at the start of the 21st century, the terrorist attacks on the USA and the stock market crash in telecommunications and new media, have altered some of the perspectives. The increased investment in advanced military capabilities and security technologies should accelerate the application of biometrics, but paradoxically, it appears to have put back the take-off point as governments seek to assure stable standards and interoperability and corporate customers await the improved performance that government will force through, while the large volumes of product for the government should reduce the price for subsequent applications. Perhaps this observation reflects the increasing maturity of the biometrics market. Reflecting upon the adoption of new technologies, many forecasters echo Paul Saffo who comments that 'all fundamentally new technologies overpromise in the short term, but overdeliver in the long term'.

A selection of more recent reports on future trends, that have taken this new world into account, offer the following observations⁴⁴:

Political, social and commercial trends

1. The increase in size of the European Union making it the only possible counterweight to a single military and commercial superpower, but in ways that offer a different perspective on world governance.
2. Reduction in the scope of the welfare state, as the cost spirals out of control with increasing pressures on government to keep taxation low; zero inflation reduces opportunities for 'hidden' taxation increases.
3. Coins and paper money increasingly become relegated to small-scale transactions.
4. Increase in whole-life education, from increased investments in pre-school children to tailored short programmes for adults.
5. Continuing conflicts in the less-developed world, and increase in tension in Taiwan and Korea.

⁴⁴ Newsweek Issue on *The World in 2012* (16-23 September 2002); Business Week, *25 Ideas for a Changing World*, (19-26 August 2002); MIT Technology Review, *The State of Innovation*, **105**(2) 55-63 (June 2002); Eamonn Kelly, Peter Leyden and the members of the Global Business Network, *What's next?*, John Wiley (2002)

6. The 'wild card' of a major disruption to the continuing economic well-being of the developed world through a terrorist attack using a dirty nuclear bomb or readily available chemical or biological agents, or a determined attack on an unsecured part of a critical national infrastructure. (The impact on national and regional economies of i) relatively confined anthrax dispersal and ii) the SARS outbreaks demonstrates the fear that these would cause).
7. Tensions as wealthy regions in otherwise mismanaged nations demand greater autonomy.
8. Transport hubs (railway stations and airports) become the magnet for shopping and entertainment zones; multi-purpose environments are developed with successful cities needing to offer facilities that appeal to the wealthy knowledge worker.
9. Increase in retirement age by 5 years by 2010. As the percentage of retired increases relentlessly new opportunities arise to address this market, in preference to the youth orientation of 1960-2000. (Two-thirds of all retired people that have ever lived are alive today, many of whom are relatively wealthy. With the post war baby boomers moving past their 50th birthday, significant opportunities for specialised healthcare will emerge.) Alternatively, a massive labour shortage may require increase in immigration of young people into the developed world.
10. Male insecurity increases as more women take on traditionally male roles in the service sector and managerial jobs, while traditionally blue collar (male-dominated) jobs continue to disappear.
11. Continued dispersal of jobs to countries with the cheapest 'all in' rates, and its progression to more high added value activities (data processing, software development and call centre operations).
12. Move away from technology utopianism and belief in wealth for its own sake (manifested in anti-globalisation protests, downshifting from stressful jobs, new ideas of holistic management, apocalyptic literatures and fundamentalist beliefs); although the future-orientation of the US will continue to drive innovation after a hiatus over the next few years.
13. Corporate mismanagement that surfaced in the early years of the 21st century increases the drive for transparency, accountability and responsibility for sustainability.
14. The quality of data and information becomes key as its volume and accessibility increases. Increased need for better information and metrics for investors in enterprises, especially in measuring intangible assets.
15. Copying of, and competition to, successful new products follows ever more quickly.
16. Changes in marketing to more entertaining, crisper, interactive messages that will appeal to an audience that is losing trust in organisations, technologists and traditional institutions.
17. Development of new products and services will increasingly depend on bringing together creative people from diverse backgrounds. Social entrepreneurship may work in hand with conventional corporations and governments to uncover new demands in the marketplace.
18. There is an untapped market for simple-to-use products for the less-developed world.

Technology trends

1. Growth of grid computing networks, networking devices of diverse types and functionality; pervasive, ubiquitous and 'disappearing' computing; more adaptive, self-healing and dependable networks that respond to surges in demand or loss of connectivity; the associated opportunities for massive crime and terrorism if their security is compromised.
2. Extensive use of RFID technologies for article control in manufacturing and wholesale and retail merchandising.
3. Pharmaceutical products, diets and bodies tailored to the individual using gene manipulation, and marketed to increasingly knowledgeable patients. There will be an emphasis on minimised side effects and reduction in the costs of in-hospital care.
4. Industrial biotechnology may take the role of the engine of technology-driven growth that IT played in 1985-2000.
5. Weapons based in space

6. Nanotechnology possibilities: the computer in the fibres of a shirt, microscale sensors, and implications for novel approaches to health.
7. New services that will make use of the potential of the over-investment in core telecommunications networks, both fixed and mobile.
8. Ambient intelligence or pervasive computing will deliver smart systems embedded in everyday objects.
9. The toy market is about to be transformed with products using AI, wireless communications, multimedia and virtual reality. Spin-offs will benefit other sectors.
10. A new perspective on the impact that probability, uncertainty and unpredictability have on systems making use of advanced technologies. A recognition that technologies are not 100% reliable or guaranteed to work in an intuitively simple way: precision warfare, network security systems and encryption, forensic analysis, biometrics, computer modelling of weather, national identity cards, safety tests on cars, digital archives, ...). MIT professor of aeronautics, John Hansman says - speaking of advances in transportation IT (but extendable to other areas of IT), 'as the complexity and information flow in these systems increase, the human will become - or in some cases has already become - the limiting factor in the design and operation of the system'. Lessons from complexity theory, such as the emergence of unpredicted effects from interacting non-linear systems, may start impacting on system design.

Impact upon the take-up of biometric technologies

The reality of these trends will determine whether services using biometrics will be needed or commercially viable at a particular point in time – or even be acceptable to users. For example, recently a debate has begun on the wisdom of development of nanotechnologies. For some commentators, the fear is that uncontrolled release of systems could result in unpredictable and catastrophic consequences for the human race. Increased physical security in laboratories and manufacturing facilities may be required, with clear accountability based on undisputed logging and audit. A biometric system linked directly into operation of individual pieces of fabrication equipment would be preferable to access control systems on doors and entrances. Work on such security mechanisms could begin now, if the legal requirements for operation of equipment requiring a defined expertise level were upgraded to mandating the use of 'state-of-the-art' technologies.

3.8 System integration considerations

The studies accompanying this Roadmap clearly confirm that integrating a biometric into services or products is not a simple substitution of a device and software for a key, a card or a password. In this section we examine some of the design considerations, especially for medium and large scale deployments.

User-centred design - a requirement for successful biometric deployments

For example, the limited experience of successful large scale deployments is that the principles of user-centred design need to be at the heart of the design process. This is not just confined to biometric-enabled applications. In recent years, there has been a growing acknowledgement of the need to understand the potential end user's needs and the context in which they will be asked to operate a system⁴⁵. There will also be processes that involve other colleagues and customers; a social perspective is also required. The realisation of this dimension to the design process has encouraged research into different methodologies and evaluation of these methodologies in real world situations. Initially, the focus has been on usability, defined in ISO standards as 'the extent to which a product

⁴⁵ For example, Hugh Beyer and Karen Hotzblatt, *Contextual design: defining customer-centred systems*, Morgan Kaufmann (1998)

can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use⁴⁶. However, the ambit of User-Centred Design (UCD) is more far-reaching. Jokela⁴⁷ comments that four activities underpin the definition used in these standards:

- Understanding and specifying the context of use, in terms of the user, the environment and the tasks
- Defining the user and organisational requirements for successful application, thereby setting the guidelines for the design
- Building in the knowledge of human-machine interaction principles into the design
- Evaluating the performance in the context of the task

The extent of user involvement can vary from system designers observing the 'status quo' and inferring better ways of integrating new functionalities, through to a fully participatory approach in which end users take an active role. Methodologies that can support the aims of UCD include modelling of the roles and responsibilities of actors or stakeholders using Soft Systems techniques⁴⁸, semantic analysis of the actions and behaviours of the principals in transactions⁴⁹ and the use of scenarios in the development of a product or service that has abstract tasks or where the unfamiliarity with technology presents a barrier to understanding⁵⁰. Kujala has reviewed the benefits and costs of UCD, noting the limited amount of research that has followed though the application of such principles. He acknowledges the additional resources and possible delay in the delivery of the system, but argues that on balance there are positive benefits to be gained⁵¹.

For many years, the Scandinavian approach to participatory design of Computer and IT systems resulted in a number of apparently successfully applied methodologies. Of recent years, this school of design has perhaps lost its direction, with Eevi Beck locating the fault with trends such as the growth of consumerism and the strength of large corporate entities⁵². However, as technology grows ever more complex, there may be a move back to simplification of interfaces as embedded, ubiquitous computing renders many IT functions virtually invisible⁵³. For biometric-enabled systems, this could be both a promise (of transparent authentication) and a threat (privacy-threatening systems that track users without their knowledge). Design of such embedded systems will require careful attention to these concerns and opportunities.

Further discussion of the results of the BIOVISION project work on user-centred design is postponed to Section 5.1.

Comprehensive design frameworks for systems using biometrics

Participatory design is just one element of a more comprehensive and radical approach to the design of biometric-enabled systems. From anecdotal evidence of the reasons for the lack of full deployments following many trials using a biometric, it appears that a more

⁴⁶ ISO 9241-11 (1998) and ISO 13407 (1999)

⁴⁷ Timo Jokela, *Assessment of User-Centred Design Processes as a basis for improvement action*, (Oulu University, 2001)

⁴⁸ P. Checkland and J Scholes, *Soft Systems Methodology in Action*, Wiley (1990)

⁴⁹ G Dhillon and J Backhouse, *Structures of Responsibility and Security of Information Systems*, European Journal of Information Systems 5 2-9 (1996)

⁵⁰ S Bodker, *Scenarios in User-Centred Design - setting the stage for reflection and action*, 32nd Hawaii International Conference on System Sciences (1999)

⁵¹ S Kujala, *User involvement: a review of the benefits and challenges*, Behaviour and Information technology, 22(1) 1-16 (2003)

⁵² E. Beck, On participatory design in Scandinavian computing research, Univ. of Oslo, Dept. of Informatics Research report 294, ISBN 82-7368-244-7, ISSN 0806-3036 (August 2001)
<http://folk.uio.no/eevi/research/pub-papers/rrepBeck2001.doublepages.pdf>

⁵³ Peter Tolmie *et al*, *Unremarkable Computing*, Proc of CHI 2002
<http://www.xrce.xerox.com/Publications/Attachments/2001-104/Unremarkable-computing.doc>

comprehensive design framework is needed. There are a number of resources that will help the prospective designer and operator, but further research is required to integrate these methods and to validate them in major deployments:

- General guidance is available on product selection and implementation, e.g. for certain applications involving identification and authentication for use by governments⁵⁴;
- Papers on general design methodologies⁵⁵;
- Development of BANTAM: a system modelling language⁵⁶;
- Isolated instances of compilation of lessons learnt across a number of pilot deployments⁵⁷;
- Integration of fallback methods⁵⁸.

Work on two **requirements capture** methodologies has already started. In Section 3.1 we introduced the Application-Technology Compiler and the BIOVISION method of comparing the requirements of a system to the capabilities of various biometric solutions.

A complementary approach, which we shall discuss at length in this section, was initially focussed on specifying the requirements for operational *testing* of a biometric in the context of a real world service⁵⁹. As applied to requirements capture, it may make no assumptions about a specific biometric method; indeed, the analysis might determine that an alternative, non-biometric approach, would be more suitable or cost-effective. Once the operational requirements of the system are defined, the BIOVISION Application-Technology Compiler can be used to match the capabilities of biometric solutions to the system requirements.

Four levels of system description are defined in B-SAD* and the service analysed in sufficient detail to move to discussion with suppliers or integrators.

At Level 0, a number of classes of a service are defined. For a biometric system to be acknowledged as one belonging to Class 0a, it must satisfy a number of conditions, chief among which are:

1. Identification or recognition of a human individual
2. Use of a biometric feature of the individual in order to determine or verify identity
3. Operation in a near real time manner
4. Requirement for automated processing and storage of biometric data for identification and/or verification

By relaxing these four requirements in turn, we identify other services that do not fulfil all of these conditions, but which should be considered when designing 'biometric' systems. It may be that a service does not require a full biometric implementation, perhaps to protect end users' privacy in a technical manner:

⁵⁴ UK Biometrics Working Group, *Use of Biometrics for Identification and Authentication: Advice on Product Selection*, <http://www.cesg.gov.uk/site/ast/biometrics/media/Biometrics%20Advice.pdf> (Issue 2.0, 22 March 2002)

⁵⁵ Marek Rejman-Greene, *A Framework for the Development of Biometric Systems*, Biometric Technology Today (January 2003)

⁵⁶ Julain Ashbourn, *BANTAM User Guide*, Springer (2002)

⁵⁷ Department of Defense, *Case Studies* <http://www.defenselink.mil/c3i/biometrics/case.htm>

⁵⁸ Dialogues Spotlight Research Team, *Apology strategies, security data, insult rate and completion procedures*,

http://spotlight.ccir.ed.ac.uk/public_documents/technology_reports/No.5%20Verification.pdf

⁵⁹ This discussion is a development of a paper by Craig Arndt of Mitretek Systems, *Biometric Standard Application Description (B-SAD) methodology* submitted to ISO/IEC JTC 1 SC37 SG5 (23 July 2003). B-SAD* is a variant of this methodology that is being developed for requirements capture.

- Class 0b services (failing to meet condition 1) may relate to non-human entities – animal identification; or relate to human beings but without the primary need to identify them, for example, by clustering of facial images that relate to individuals – as in the ChildBase applications cited in Section 6.8.
- Class 0c services provide automatic identification where no human feature is required (such as knowledge of a PIN or password together with a token).
- Class 0d services remove the requirement for quasi real time operation (condition 3). Examples are manual identification of fingerprints by specialised staff and analysis of DNA under current laboratory conditions.

At this stage, the operator may determine a number of options, one or more of which may involve the use of a biometric.

At Level I, the classification consists of four classes of operation each considered in a number of different contexts:

- Class 1 (one-to-one verification of identity)
- Class 2 (one-to-many positive identification)
- Class 3 (negative identification, confirming that a person is not in a specific group or database)
- Class 4 (one-to-few matching, where the individual is either a part - or not - of a small group of possible matches)

Note that this classification does not match with the AFNOR classification of applications introduced in Section 1.1.

The context dependency for each class is in two parts:

- with or without the presentation of a token
- the user being cooperative, un-cooperative or unaware (surveillance mode)

Level II specification addresses the system's operational characteristics. Documentation is required for each of five groups of operational characteristics:

- *Operational environment*: temperature, lighting, vibration, contamination, noise
- *Operational mode of the system*: role of the human in the decision loop, attended or unattended operation
- *End user population*: Size of user population and size of the database, Distribution and diversity of the population, location of the population, special characteristics of the population, operation or processing in different countries, social and psychological disposition towards biometric systems
- *Exception handling*: procedures in the case of alarms being set off, procedures for those who experience difficulty in enrolment, procedures for false rejection, procedures for disabled individuals, procedures for VIP individuals.
- *System interfaces*: links to external workflows, processes, systems and databases - whether these are legacy, currently under development or envisaged in the future)- with specific reference to systems that are permitted to receive either the results of biometric processing or biometric features or templates, links to external hardware and support systems including those to audit and logging schemes.

At this level, a full understanding of the user and their relationship with the task and application needs to be defined. This B-SAD* approach has to be supplemented with the results of the BIOVISION project results on user perceptions summarised in Section 5.1.

Level III specification defines the system requirements for the service:

- *Performance*. For a verification service, this can be quoted in measures such as FAR, FRR, time to match, time to search a database, etc., and specified to pre-determined confidence levels; tradeoffs can be explored between various combinations of the measures; different performance requirements can be set for initial operation (to

allow for familiarisation and training by enrolment officials and end users unfamiliar with systems), and - where appropriate - for operation where users are habituated; further levels may need to be determined for alarm or warning of problems with the system, and additional levels at which operations are terminated and the system is withdrawn from service;

- Required *rate of deployment* of the system to meet commercial or political objectives;
- *Standards compliance*, to include desired or undesirable interoperability with other systems in the country or worldwide;
- *Systems security specification*;
- *Secure upgrading of systems*, and handover state at specified points in the future (e.g. at the end of an agreed period of outsourced operation, or after non-compliance with other performance measures)
- *Compliance with privacy and other legal codes*, and with any stated preferences or commitments to anonymous or privacy-enhancing operation;
- *User interface requirements* (to include education and marketing);
- *Other technical application requirements* (to include reliability, maintainability, durability, etc)

It is our belief that rigorous definition of the specification at the outset - even before engaging with individual suppliers - would enable the service operator to clarify the business requirements of the system. This requirements specification model is still under development; it is possible to envisage further segregation of the analysis into aspects and bands of operation that must be met, as compared with those which would be useful if provided at a low enough cost.

Note that this approach does not prejudice the use of a specific biometric technology - or even the selection of a biometric approach. However, it does require that the operator considers the 'real' aims of the project and sets targets that are achievable; for example, some banks have been known to set performance requirements of zero false rejections in proposed biometric deployments.

Having captured the requirements, operators can challenge system integrators to offer solutions that will address the totality of the list. Their responses will often indicate inconsistent or contradictory elements, and more likely point to the need for detailed piloting and trials to ascertain whether proposed solutions are workable. The extent of these trials - and who bears the costs - need to be resolved at an early stage in the negotiations. At this point, revisiting the B-SAD* requirements analysis in the light of proposals from system integrators should highlight those aspects which have had to be compromised in achieving a practical solution. A tool that can support this process is the Application-Technology Compiler described in Section 3.1.4, which assesses the extent to which specific biometric technology matches the requirements of an application in all - or some - of the critical measures.

In reality, it is unlikely that operators will take such a cleanly logical approach. Even before the completion of an outline specification, they will have been influenced by publicity about the capabilities of systems already using biometrics. Some operators will be afraid of being seen as outdated in their thinking if they fail to make use of the most modern technologies. The benefit of an agreed methodology (such as B-SAD*) is that independent monitoring of the process of system procurement is possible, allowing citizens to engage in meaningful dialogue with governments and end user organisations to effectively represent the interests of their communities.

Once the system requirements have been agreed, and the feasibility studies, work breakdown structures, etc have been completed, the development of robust designs needs to be undertaken in a way that reflects the requirements in an accurate way. This is hardly a trivial exercise for most medium- and large-scale deployments for systems using biometric methods. Even in less complex systems, maintaining the consistency

throughout the design process is difficult⁶⁰. This is an area where applied research could provide useful processes for European systems integrators. It is also an unfortunate reality that during the design and development of these systems, 'requirements creep' will take place. Operators will either realise that the system description was incomplete, or political imperatives make the introduction of new features a mandatory requirement for the system. Recognising that appropriate measures are required to address these realities should reduce the impact of such changes on the cost and performance of the delivered system.

Although these issues have been addressed in deployments, there is little publicly available analysis. As part of the remit of the European Biometric Forum to reduce fragmentation in the European market, the EBF should consider advocating research into best practices in the design of biometric-enabled systems. Ethnographic studies of deployments, supported by the lessons learnt from other large-scale system developments would improve the likelihood of future successful system deployment and the sharing of knowledge for the benefit of operators who are unfamiliar with biometrics and the challenges these methods pose to the design community.

Specific design challenges

One research challenge that has not been addressed to date is consideration of **fallback methods**, when a user is either unable to enrol, or if enrolled correctly, fails to be recognised within the maximum number of attempts. The need for a secure alternatives to a biometric methods is acknowledged, but little published material is available to indicate how this should be approached. One exception is a study by the University of Edinburgh on strategies for failure of speaker verification systems that reported, in addition, on user attitudes to failure of systems⁶¹.

Other facets of system design that should be considered from the outset include **security** and the response to user concerns about privacy and abuse of the system in general. Three fundamental principles of secure design of systems are i) commencement of the design of the security of the system as early on in the process as possible (the later that this is postponed, the more expensive and unsatisfactory solution will result); ii) frequent revisiting of the security design in response to changes in the design of the overall system; iii) assessment of the security policy and security implementation by a third party. It may not be economic to undertake a full security evaluation in accordance with the Common Criteria, but an independent detailed review should be a part of any deployment.

In order to take account of the **privacy** implications of a proposed biometric-enabled deployment, a Privacy Impact Assessment should be carried out at an early stage (Sections 5.1 and 5.5 provide background material - from the viewpoint of end users and the legal context, respectively.) Such a PIA will document the possible privacy-related issues, take account of the views of the stakeholders (or their representatives), ensure that the legal requirements are met (together with any codes of conduct or privacy principles to which the organisation is a party) and develop a strategy of addressing each of these in turn. As for the development of a secure system design, the solutions may need to be revisited if the system itself undergoes significant changes during its development. However, there is a vocal constituency that believes that the rights of end users need to be protected in a more proactive manner. They will assert that the complexities of an installation using a biometric may be beyond the understanding of even conventional system analysts, and the hazards involved in using the technology, may require the maximum of openness and transparency during all stages of the development together with additional security mechanisms and procedures to protect the interests of all

⁶⁰ James Kirby, *Rewriting requirements for design*, Proc IASTED International Conference on Software Engineering and Applications (SEA) 2002, Cambridge, Mass, USA.

⁶¹ Dialogues Spotlight Research Team, *Apology strategies, security data, insult rate and completion procedures*,

http://spotlight.ccir.ed.ac.uk/public_documents/technology_reports/No.5%20Verification.pdf

concerned. A willingness to understand this perspective and engage in a discourse at an early stage will help mitigate any subsequent adverse publicity. The results of applied research into the underlying differences of approach would help the prospective operator in negotiating with such parties. For example, Whitworth and de Moor have explored the concept of 'legitimacy'⁶² and there is a growing literature on trust and 'fairness' that may support this aim.

The BIOVISION Privacy Best Practices document⁶³ offers guidelines for designers on compliance with European legal requirements. There are other resources available that provide good design rules. One example is provided in the recent National Research Council report on authentication.⁶⁴ Although written from a US perspective, many of these rules echo the legal constraints in the European data protection. Taken together, such resources offer checklists that the system integrator should consider in any design, and an example of which is shown below.

Minimising Risks	
R1	Authenticate only when needed and only for well-defined purposes, details of which should be openly available wherever possible;
R2	Anonymise personal data wherever possible;
R3	Minimise the scope of data collected to that which is necessary, and remove securely any intermediate data that is not required (e.g. original images from the biometric sensor);
R4	Minimise the opportunities for inference of physical or psychological characteristics (or medical conditions) unrelated to the authentication process;
R5	Biometric data should be stored with the minimum of other personal data;
R6	Consider the options of decentralised data storage and user control over their personal data;
R7	Minimise the time for which the data is retained;
Security considerations	
S1	Secure the biometric data during collection, storage, transmission, use and destruction; this includes the results of operations on the biometric data;
S2	Identify who will have access to the collected data;
S3	Ensure that only specified types of access to, and use of, such data are permitted;
S4	Ensure secure audit of the use of the system, protecting against unauthorised modification and destruction of such audit records;
Consideration for the user	
U1	Involve the person who is to be authenticated in the process;
U2	Minimise the intrusiveness of the authentication process;
U3	Minimise the intimacy of the data that is collected;
U4	Failure of the system should not place the subject at a disadvantage;
Policy Management	

⁶² B. Whitworth and A de Moor, *Legitimate by design: towards trusted socio-technical systems*, Behaviour and Information Technology, **22** (1) 31-51 (2003)

⁶³ Astrid Albrecht, *Privacy Best Practices in deployment of biometric systems*, Issue 1 (2003), available at the <http://www.eubiometricforum.com> website.

⁶⁴ Stephen Kent and Lynette Millet, Editors for the Committee on Authentication Technologies and Their Privacy Implications, *Who goes there? Authentication through the lens of privacy*, National Academies Press (2003) at <http://www.nap.edu/books/0309088968/html/> Recommendation 3.2

- P1 Clearly articulate the policies under which the system will operate, and wherever possible allow subjects to view these policies in close proximity of time and place of operation;
- P2 Any changes in these policies should be communicated to the subjects in an effective manner;
- P3 Third party audit of compliance to such policies should be considered;
- P4 Failure to operate to these policies should result in appropriate redress to the subjects of the authentication process and penalties to the operators of the system;

Errors and exceptions

- E1 Wherever possible, offer an alternative – non-discriminatory – system, for those people who are unable to use the system or have valid objections to its use, informing them of risks and benefits of not participating in the biometric system;
- E2 Provide methods for the subjects of the authentication to check and correct the data about them that is used for authentication, and - if appropriate - to remove themselves from the system;
- E3 A secure process for the withdrawal of the biometric system should be developed.

Middleware

For all but the smallest deployments, good **middleware** will be a prerequisite for robust designs. In outline, it is the 'glue' between the biometric and the application. Although there is some debate as to what the integrator should expect from the supplier of middleware, some elements that are often included are:

- Facilitation of a heterogeneous authentication environment with different biometric methods, legacy systems, using passwords, smart cards, etc;
- Storage and application of reference templates as and when required;
- Securing of the system components;
- Logging and analysis of performance.

A number of suppliers have been in the market for some time. Among these are SAFLINK and BioNetrix in the USA and Daon and ISL (Informer Systems Ltd) in Europe. With much biometric hardware being designed in accordance with BioAPI standards, there is increasing differentiation between suppliers in the architectural designs they work to, whether basing their designs to work optimally with existing operating systems and business process models or by developing their own design. Although a small market at present, the middleware sector is forecast to expand rapidly as soon as interest in biometrics in medium scale deployments (500-50,000 users) starts to take off.

Scalability issues

Many suppliers can be trusted to implement small scale designs using biometric technologies. However, as the size of the deployment increases, it becomes proportionally more complex to satisfy the more diverse requirements of such systems. Scalability is often a matter of experience, and there are no clear rules to help clients in determining whether their requirements can be addressed using small scale design methodologies. Capacity and resource utilisation may appear to be straightforward, but bring unexpected problems as the complexity of interactions with other systems become clearer. Scalability needs to be considered in all aspects of the system design: in the hardware - both biometric and support and in the middleware, in data extraction, the algorithms, databases and business processes. A comprehensive guide to scalability issues in the design of

larger biometric systems remains to be written, but some of the key aspects will certainly include⁶⁵:

- A more comprehensive analysis of the *error rates* than is usually pursued at the level of the device and its dependent software (see Section 4). Failure to accept a user's biometric sample, for example, could depend upon database management errors as well as changes in the immediate environment or variations in the user's positioning or behaviour. As the size of the subject population increases, unexpected features of the biometric method being used will begin to surface in increasing numbers. For a small deployment, the security policy could tolerate a change of operating threshold, since the officer can make a local judgement in the context of the service. The key to this aspect of the deployment is extensive testing at the technology, scenario and operational levels; simulation and modelling of systems; development of validated reference systems, as well as staged deployments across different cultural groups.
- *Architecture*. As the system size increases, it touches an increasing number of other systems, some of which may anticipate simple 'yes/no' answers from an authentication scheme. Individuals not familiar with the particular features of biometric systems can take decisions at fault centres and help desks that can lead to system close-down or degradation. Mission critical or 'fail-to-safety' systems could be compromised. Unless a biometric-enabled system is isolated from other business processes, further complexities can be anticipated as multiple feature interactions emerge during pilot testing. The operation of fallback systems will change the context of operation of the business processes.
- *Requirements creep during the design and development*. Not all of the requirements can be captured unequivocally at the start of the programme. The failure or cost overrun of many headline systems both for governments and large multinationals can be traced to the addition of additional functionality during an extended development period. Clear management responsibilities and a single champion for the programme, who remains in post from the project inception through to its handover, may reduce the impact of such changes. This champion should clarify the priorities of all major stakeholders, and assess the evolution of their strategic goals over the period of the development and deployment, possibly using the roadmapping techniques described in Section 2. Acceptance criteria for the final system will have to be developed anew for each application, since there is little prior experience in this area.
- *Security*. Protection profiles are available for small and mid-range systems, whereas large scale public systems will probably require specialised security designs. For example, AFIS systems for the law enforcement community operate in closed communities, whereas civil AFIS systems are likely to have a much higher interconnectedness with other systems. If the biometric is to be used in any legal proceedings arising from attempted fraud or other criminal activity, then both the system design and the underlying technologies will need to be accredited in an appropriate manner. The evidential value relating to biometric methods is still a matter for debate⁶⁶, and the numbers of experts is relatively low (except for fingerprint identification).
- *Patents and licensing*. Numerous patents have been granted over the past four decades for authentication schemes. Large scale systems will, in particular, be likely targets for legal action.
- *Limited expertise of personnel in both the core technologies and in design methodologies* to ensure robust, secure and acceptable systems. There are relatively

⁶⁵ Julian Ashbourn, *Applications Scalability*, <http://homepage.ntlworld.com/avanti/scalability.htm>

⁶⁶ Michael Bromby, *At face value?*, NLJ Expert Witness Supplement page 302-3 (February 28, 2003)

few specialists who understand biometric methods and their application to specific systems, and no certification scheme for those who claim to have such experience.

- *Support, maintenance and business continuity.* With little experience of large scale systems, assessment of operational risk is likely to be an issue. If too pessimistic a view is taken, the costs of providing for alternatives will become a significant item in the budget for the system. If the risks are not fully appreciated, costs during operation of systems could escalate.
- *Enrolment and registration of end users.* There may be a pre-existing database of users (such as an HR database of employees), although it may not be dimensioned for the additional data required from a biometric system. Furthermore, since biometric authentication is likely to be viewed as a more trustworthy method by the organisation - and any partner organisations relying on such authentication both at the initial deployment of the system and in the future - the security policy should insist on an appropriately secure confirmation of the identity of the user at enrolment.
- *Operational management.* Future upgrades are inevitable (for example, as further security vulnerabilities are encountered), and the system should be capable of accepting upgrades in the sensor, algorithms, etc. in a cost-effective manner. Some contracts operate for a fixed term on an outsourced basis, and the operator of the service for which biometric methods offer the authentication should plan for handover at the end of the contractual period.

RC/SD1 RC - SYSTEMS and DESIGN 1: Successful implementation of systems using biometric methods requires an inter-disciplinary design approach. There are few specialist designers able to put together an integrated design that addresses the already documented issues and concerns.

4. Technologies

There are numerous methods that make use of an individual's individual physical characteristics or behavioural traits. This section will summarise the main aspects of each of the principal technologies, identify the main commercially available systems, overview the research effort in each area and provide a view onto the future of the approach. The methods that will be analysed are:

1. automatic facial recognition, using either visible light or infra-red illumination (or a combination of both)
2. recognition by fingerprint or surface features extending along the finger
3. iris recognition
4. recognition by means of the blood vessel patterns in the retina
5. hand geometry
6. the pattern of veins on the back of the hand
7. speaker verification
8. dynamic signature recognition
9. keystroke dynamics.
10. other potential biometric methods (including gait recognition, lip movement analysis, ear shape biometrics, odour recognition, quasi-real time DNA analysis)
11. multiple biometrics - combinations of one of the above with another biometric or another form of authentication

An initial discussion positions alternatives to the use of biometrics. Often there are alternative ways in which a solution can be developed. In some deployments, a decision to select a biometric has been made on the grounds of its innovative features appealing to the system specifier, its high visibility or because of well-targeted marketing by companies with a vested interest in selling their products. There is also a suspicion that in some jurisdictions, the requirement for a biometric solution or even a specific technology has been written into legislation following lobbying by suppliers, without a corresponding examination of alternative approaches.

In this section of the Roadmap, the aim has been to summarise key aspects of the current status and future prospects of each technology using a common framework:

- Introduction

This overview summarises the most significant features of the technology and the way in which it is being applied.

- Survey of principal technical approaches to the practical realisation of the biometric

A technology can be implemented in several distinct ways. For example, in the most common situation, there will often be

- a) a number of different *sensor* options (e.g. all-optical, capacitive silicon and electro-optic plastic sensors are available for fingerprint biometrics) and
- b) the *algorithms* used to define a template and the matching process can vary widely (again for fingerprint approaches, the system designer has a choice of working with the image as a whole or with the key points on an image - the 'minutiae').

The best way in which the authentication decision is displayed can also be dependent upon the application and capabilities of a specific way in which the technology is implemented. For facial recognition, some systems will preferentially deliver a percentage probability of match between template and the image captured during operation; whereas others will offer a sequence of the top matched images for final decision by a human in an attended operation.

- Principal commercially available systems

A selection of those suppliers of system level solutions has been compiled. Users of the Roadmap should note that the market is fast changing, and that lists such as these can become rapidly outdated. Many companies are privately owned (especially some of the more innovative ones) and sales figures for these are unavailable.

- High profile deployments

This section points out the more interesting deployments of a technology. These may not necessarily be the most extensive, or the newest; the aim is to highlight systems that demonstrate the opportunities offered by biometric technologies.

- Testing and factors limiting the performance of the specific technology

At the heart of the decision on which technology to use (or whose approach is best, or indeed, whether to use a biometric at all), is the question: how will it perform when it is operational in the context of the application that is under consideration? It would be courting commercial disaster if the decision were made solely on the basis of projections of performance grounded in a mathematical model offered by a supplier. Ideally, there will be a reference implementation of the same version of the biometric hardware and software operating in exactly the same application. It will have been working for more than two years with substantial numbers of end users - whose demographic profile is very similar to that in the proposed implementation (in respect of gender balance, age distribution, educational background, attitude to novel technologies, cultural orientation, political environment, etc.) and in which the physical environment is very similar. Performance measurements will have been logged throughout the deployment and the result of attitude surveys will also be available. Rarely, if ever, will all a reference site meet these conditions.

Instead, the feasibility study for a proposed implementation will need to plan for a programme of testing throughout the design and deployment of the system. Not only does this represent a significant additional cost, it also requires a considerable degree of expertise in the design of such tests. It may be that a consortium of prospective operators working with a number of suppliers can share the costs, although this will be at the expense of some degree of direct matching to the specifics of the implementation by individual operators.

Many years of experience in the conduct of such tests has been distilled in an internationally accepted document that is the basis for work on an ISO standard on the testing and reporting of biometric devices⁶⁷.

Three types of evaluation of the performance of systems should be distinguished, each of which gives different types of information to stakeholders in the decision on implementation of a system:

- technology evaluation, generally comparing the algorithms used by different suppliers;
- scenario evaluation tests at the system level, with a specific sensor, a selected algorithm, and a user experience that mimics the simulated 'real world' environment;
- operational evaluation aims to 'determine the performance of a complete biometric system in a specific application environment with a specific target population'

In general, a number of performance metrics will result, the principal ones being the rates or probabilities associated with

⁶⁷ Tony Mansfield, *Best Practices in Testing and Reporting Performance of Biometric Devices* (Version 2.01, August 2002)

- *failure to enrol* individuals and to generate a (reference) template, either because they are missing the relevant bodily part or function, or are unable to make the system work to the acceptable quality level;
- *failure to acquire* an image or signal of a sufficient quality;
- *false rejection (Type I error)* of the correctly presented user that should have been a match to an enrolled template, but failed due to - for example - changes in appearance or action of the individual;
- *false acceptance (Type II error)* of an impostor who is falsely matched against a wrongfully claimed identity. Note that there are different types of false acceptance tests. Most automated systems of testing will test all of the presented images against all templates and look for accidental matches and these are the results presented in the following sections. 'Live' tests of varying levels of severity will pit the human adversary against the machine with different degrees of knowledge about the operation of the system and biometric characteristics of the target subjects.

Understanding the *presentation of test results* requires an appreciation of the way in which biometric systems work. Most biometric systems offer an adjustable function, called the threshold setting, which allows system designers to alter the balance between false acceptance and false rejection.

- The results of tests can be shown as two graphs, with the proportion of both types of failure being plotted as the threshold setting is changed. At one value of this setting - the *Equal Error Rate (EER)* - the proportion of false accepts is the same as that of false rejects. Although of no significance in itself (as security and usability requirements for a system will determine the specific rates), the EER is sometimes used as a figure of merit.
- An alternative way of presenting the results is to derive a single graph of the rate of 'false negatives' against that of 'false positives': the 'Receiver Operating Characteristic' (ROC). A related form is the Detection Error Trade-Off (DET) curve: a replotting of the ROC on a dual logarithmic scale to enable better comparison between similar-performing systems.
- In some tests (termed 'closed set'), impostors are assumed not to exist and all users are assumed to be enrolled in the system. In this case, another reporting metric is to report the probability that an individual appears as the first match in a list of possible matches. By extension, *Rank n* performance reports the probability that the correct individual appears in the top *n* of possible matches.

Many of the performance measures obtained in independent tests fall short of the claims of suppliers of biometric systems - often by a considerable margin⁶⁸. Additionally, in the absence of standardised methods of ascertaining the error rates in real world applications, performance in laboratory settings are often the only available measures, and these may focus on the algorithm, rather than assessing a complete subsystem. However, it appears that some biometric systems are being deployed with threshold settings set at insecure levels in order to maintain service levels. A greater level of transparency is required in order to encourage research and development aimed at improving the performance of such systems. A part of this work would determine whether there are fundamental limits to the accuracy with which biometric methods (and specific ways in which a biometric method may be implemented by a supplier) can characterise an individual.

RC/C1 RC - COMPONENTS 1: R&D effort is required to improve the operational performance of existing biometric systems. In some cases, the error rates are substantially below what is required for the applications for which they are sold, and 'quantum' improvements in their performance may be required.

⁶⁸ A comprehensive list of evaluations is collated in a BIOVISION report: Tony Mansfield, *Biometric Performance Evaluations* (25 January 2002) in Michael Behrens *et al*, *Discussion paper on actual testing programs and recommendations: Annex 2* (July 2003)

RC/C2 RC - COMPONENTS 2: There is little understanding of the fundamental limits to the performance that could be attained using a specific biometric

- Specific user issues in the implementation of this technology in solutions

Some of the technologies have been associated with possible concerns that are specific to the method (e.g. methods that use supplementary light sources to illuminate the face or facial features).

- The legal and regulatory dimension

Although the use of all biometric methods appears to fall within EU laws on personal data protection, in some countries there are other laws and regulations that restrict the use of certain technologies. In particular, facial recognition and fingerprint systems have specific restriction on their use in certain countries. There is a cultural and historical background that underpins the differences between member states, especially in the consideration of privacy and personal data. Some Data Protection Commissioners respond by placing limits on the tracking of people or access by law enforcement to biometric identifiers.

- Standardisation activities

Although there is considerable activity related to biometrics in general in the ISO standardisation subcommittee 37, a number of the technologies are the subject of specific proposals for standardisation of the image transfer.

- Key research initiatives

This section reviews a selection of the more ambitious research projects that will impact on future use of the technology.

- Outlook on the future of this technology

4.0 Alternative authentication technologies

Conventionally, discussion on methods for the authentication of individuals centre on one of the following types of credential (Section 1.1):

- Authentication by demonstration of knowledge known only to the individual ('what you know')
- Authentication by possession of a unique, unalterable token ('what you have')
- Authentication by a physical property or action that is unique to the individual ('what you are or do')

Our experience is that such uniqueness, unalterability, etc. is not a practical option for applications that have to be operated by people with limited time, memory and attention - using systems that have to be justified by demanding business cases. Of course, two (or all three) of these approaches can be used serially or in parallel to improve the level of security. For example, a speaker verification system can make use of a password or number sequence that is special to the one individual. The real improvement needs to be assessed carefully, preferably on the basis of testing under real, operational conditions.

There are a few other alternatives that have been described and this summary of the range of options aims to provide a complementary view to the discussion on individual biometric technologies.

4.0.1 Knowledge-based systems

The user-name and password combination is by far the most prevalent method of authenticating persons on computer-based systems. This is an example of a *recall-oriented* knowledge-based authentication scheme, and its persistence in spite of the well-known problems merits more detailed consideration. A number of variants exist, such as 'question-and-answer' approaches. Yet this is not the only form of a KBS authentication scheme. In the 1990's, *recognition-orientation* was suggested as a way of overcoming their deficiencies. Studies showed that people appeared to remember and recognise faces - even those of unfamiliar people - more reliably than other unrelated facts. Similarly, recognition of random images was also proposed in the form of Déjà Vu⁶⁹. This work was commercialised as Passfaces⁷⁰. Research on the usability of such systems demonstrated problems when users were faced with having to use these for more than one application.

Passwords have a long and well-established provenance, at least in the field of physical security. Although not operated automatically, for many centuries these provided a 'friend or foe' identification to sentries at gatehouses, on the presumption that it would be difficult to pass on an unknown phrase to others at a time when there was no form of electronic communication. Frequent change of password was recognised as a key requirement, with lack of trust in the loyalty of guards and in recognition of the possibility of exchange with enemy agents.

The user name/password combination was adopted early on in the computer age, when the rules were appropriate for the typical end user (usually a technically aware professional operating a single, closed user group IT system). Some systems offer a degree of user choice, provided that common dictionary words are not used. The hazards of allowing such choice (e.g. selecting foreign language words) have forced many system administrators to enforce randomness in the selection and use of passwords. Rules for these were codified in a US Department of Defense memo and FIPS standard that calculated the required password length and ageing time to assure a given level of security. Even now, many password systems are designed on the basis of this approach, even though the human memory assumptions that underlie the methodology have been disproved.

PIN numbers have been the technique of choice for applications that make use of number keypads (e.g. in telephony applications and in retail financial services). False accept rates should be 1 in 10,000 for a 4 figure PIN, but allowing user self-selection can result in the use of birth dates, house numbers, etc, many of which can be guessed by knowledgeable adversaries.

A number of 'knowledge-based' alternative techniques have been proposed, although the usability of many remains to be proven:

- 'Question and answer' systems that require answers to a number of questions about user preferences and history⁷¹ that the user is presumed only to know;
- 'Associative passwords' that provide challenge-response interactions to a selection from a large number of previously determined word pairs, e.g. 'black-eye'⁷²;
- A longer passphrase or sentence, preferably one that makes no logical sense

⁶⁹ R. Dhamija and A Perrig, *Déjà vu: A user study using images for authentication*, Proceedings of 9th USENIX security Symposium, pp 45-58 (2000), available at www.usenix.org/publications/library/proceedings/sec2000/full_papers/dhamija/dh

⁷⁰ commercialised by IDArts in 1999

⁷¹ M Zwiiran and W Haga, *Cognitive passwords: the key to easy access control*, Computers and Security 9(8) 723-36 (1990)

⁷² M Zwiiran and W Haga, *A comparison of password techniques for multilevel authentication mechanism*, The Computer Journal 36 (3) pp 227-37

- Visual knowledge-based systems, using either faces which the user has memorised previously or randomly-generated art, such as the inkblot method suggested by researchers at Microsoft Research⁷³.

Problems. A detailed assessment of the use of passwords in 'real life' situations has been undertaken by Angela Sasse and her colleagues at University College London⁷⁴.

- The multiplicity of passwords that many knowledge workers are required to use (in one organisation, an average of 16 per person), with differing change regimes and combinations of minimum/maximum lengths results in considerable confusion amongst end users of such systems.
- The mismatch between password mechanisms and users' capabilities is clearly evidenced from studies of 'real world use'. Forcing randomness in the selection of PINs and passwords is often seen as a challenge by end users to explore the limits of the algorithm designed by the security team.
- Resetting of passwords in a corporate environment occupies a substantial proportion of the IT helpdesk's time.
- Reuse of passwords between applications of differing security levels pose a clear risk of dissemination of this secret. The 'secret knowledge' required as a backup security question in many financial applications - the user's mother's maiden name - can no longer be treated as confidential data.
- PIN numbers are even more of a problem with heavily used numbers being quickly forgotten even after relatively short periods of not being used.
- Many security policies now recognise that users write down passwords, and have resorted to suggesting that this be done in a non-obvious way and then keeping the note in a secure place.
- The importance of passwords and PINs as the key security measure is easily forgotten, and even conscientious users can fall victim to social engineering⁷⁵.

With regard to legal liability, the use of passwords and PINs can also pose legal problems. For example, in Germany, the use of the so-called prima-facie evidence often leads to legal disadvantages to the PIN-user as he is confronted in court by arguing that he has not kept the PIN sufficiently secret as he was supposed to do according to usual contractual conditions imposed by, for example, financial institutions with regard to the use of cash dispensers.⁷⁶

4.0.2 Authentication by possession

A number of methods have been used from physical keys to locks, cards of various types, through to dongles or USB tokens that require their insertion in PCs for data or software to be operated. Some 'calculator' type cards (such as SecurID) have a display that displays a sequence of random numbers, changing in synchronisation with a server. These may be used in conjunction with a PIN to strengthen the authentication. An interesting variant on this is the Quizid electronic token⁷⁷, which replaces the PIN with a five colour button sequence (which has additional support for the memory in terms of positioning of the five

⁷³ Suzanne Ross, *Is it just my imagination?*, <http://research.microsoft.com/displayArticle.aspx?id=417>

⁷⁴ Angela Sasse *et al*, *Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security in Internet and Wireless Security* (Eds. R Temple and J Regnault, Institution of Electrical Engineers pp 243-261 (2002)

⁷⁵ Social engineering refers to methods of obtaining critical information by unauthorised individuals through the use of plausible ruse or excuses. For example, *Office workers give away passwords for a cheap pen!* Information Security Bulletin www.chi-publishing.com/portal/index.php?id=487 (18 April 2003). A comprehensive study of social engineering has been written by Kevin Mitnick, a hacker who explored its practical aspects: Kevin Mitnick, *The art of deception*, John Wiley (2002)

⁷⁶ See for example Astrid Albrecht, *Consumer Acceptance and Legal Frameworks*, pp. 68 ff., in: Lockie, Mark/Deravi, Farzin: *The Biometric Industry Report*, Elsevier Advanced Technology, Oxford December 2000

⁷⁷ www.quizid.com

coloured buttons. The suppliers claim that people's memory for colours is better than for numbers.)

Clearly, the complexity of design and resistance to copying determine the level of security, while they offer little protection against their being lent to another person by someone who does not require their use for that duration. For example, plastic cards have become more sophisticated from the initial use of 300 byte magnetic stripe versions. The information from these could be copied easily using equipment costing a few hundred euros. Next generation systems with more complex types of material in the magnetic strip, and stripes with imprinted watermarks in the magnetic pattern have been introduced to counter such copying. Chip cards with a built-in silicon integrated circuit have proved more robust against such simple forms of copying, while sophisticated encryption co-processing and the use of public encryption techniques have improved some aspects of security. Ultimately, though, users have to be trusted not to part with the token, and to report its loss immediately to the authority that manages any revocation measures.

The RESET roadmap project has overviewed the future challenges and opportunities for the use of smart cards ('chip cards')⁷⁸ It notes the very large number of devices shipped annually (approximately 1.9bn units in 2002, with a doubling to 3.8bn by 2005). By far the largest number is for use in the telecom sector (1.5bn in 2002), followed by 170m units delivered into the financial arena.

Specific comments about the range of applications and the drivers for the use of smart cards in the period up to 2005 include:

- Of the telecom use, a substantial number (over 2/3 of the total produced for this sector) are memory-only devices, with just over 400m being SIM cards. The consortium believes that the potential of m-Commerce has been hampered by a lack of standards and fragmentation in solutions, but that it will continue to be a priority for the new generation of services built upon the advent of 3G mobile systems, expected to start in a major way in Europe in 2004.
- The migration of standards in the financial sector towards EMV for chip based payment, and consequent shift in liability for those not using such cards, by 2005 should ensure the uptake of IC cards for this type of application.
- Up to 200m cards are predicted to be used for personal identification by 2005.

Key challenges that are foreseen in the future are:

- A move towards Java open source platform operating systems that can support multi-tasking;
- Improved communications between card and reader, in terms of data exchange speed and lower power consumption; support for protocols that offer better confidentiality and security; and improved mobile connectivity;
- Faster access to non-volatile memory and enhanced RAM capacity;
- Better design tools and design methodologies;
- Two possible ways of enhancing the functionality: through improved card functionality with key pads, displays, biometric sensors and better network interfaces; or alternatively, through the development of more powerful user terminals such as the PDA, which could be used the trusted device for applications as diverse as access to buildings and ATM cash access;
- Improved security by eliminating the leakage of information through side-channels, better physical security protection techniques (such as tamper-resistant chips), more powerful evaluation tools, and improved cryptology solutions.

Proposals for more complex (and possibly more secure) schemes for authentication by possession have included *parasitic authentication*, whereby a second unit is required as well as a smart card. This unit would be a small, self-powered, disposable device that

⁷⁸ RESET project: Draft Roadmap v 2.0 (28 March 2003) www.ercim.org/reset

would communicate with the smart card⁷⁹, such as an RFID device. Incorporation of such devices into watches, rings, etc would improve the likelihood of their being always available, while mobile phones could serve as a similar carrier.

4.0.3 Authentication by location

For many years, Caller Identification has been the authentication method of choice for the telecommunications operator. This sufficed when customers had one phone, fixed at a single address, with a single individual responsible for all of the transactions made using that phone. As the numbers of mobile telephony terminals grew, such a model was no longer a viable option. Although mobile operators could determine the cell from which a call was made, more precise location information was not possible in the initial releases. The need to locate people in an emergency and the opportunities offered for new services based upon location have revived interest in the possibility of location-based authentication. (Many fraud protection systems have used the impossibility of an individual being at two separate sites separated by a considerable distance to reduce the incidence of cloning fraud, whether of mobile phones or credit cards.) A combination of location-, possession- and knowledge-based authentication could drive novel applications without the need for a biometric infrastructure. The advent of pervasive computing in the second half of the decade could hasten the arrival of such systems.

Note, however, that there are significant privacy concerns in the aggregation of such information. Care with the system design and storage of such data is needed if such location-based technologies are to be accepted by the public at large. The PAMPAS Roadmap offers a number of scenarios, visions and challenges for such systems⁸⁰. Notions of tuneable anonymity, user-centred mechanisms that allow the controlled release of personal information, etc require further research to ensure that solutions are developed that offer benefits to end users and operators, whilst providing security and protection for both.

4.0.4 Authentication by history of use

Human beings are, in the main, creatures of habit; yet in the developed world, they are increasingly offered a multitude of complex options. Most resort to selecting a narrow range from the totality of opportunities, and for 'everyday activities' such as shopping, working, routine leisure pastimes, etc. they repeat a similar pattern, week after week and month after month. For example, once a pattern of use of a complex software program has been established, most users will not deviate from this. Both marketing specialists and fraud detection programs make use of these habits to codify individuals according to behaviour and pattern of use of services. Their use for authentication has not been fully developed. Clearly, the likelihood of false rejection at times of extreme need (emergency, such as illness or accident) or unusual circumstances (for example, when on holiday) limits the use of this method. Nevertheless, in combination with other approaches, history-based authentication could allow for innovative service offerings.

As with location-based authentication, this approach could be seen to be privacy-invasive and appropriate measures will be necessary to protect the individual. The advance of ubiquitous RFID (radio-frequency identification) tags in clothing, jewellery, money, etc. raises the prospect of another form of history-based authentication: the RFID-sensed individual. Potentially, these tags can be made the size of small silicon integrated circuits in a plastic packaging at 10 cents and below in price, with individual identification for each chip. A human person passing by a portal that has been set to collect all forms of RFID data could be identified and re-authenticated at a different time and place, even though they may change some of their clothes and jewellery.

⁷⁹ Tim Ebringer *et al*, *Parasitic Authentication*, IFIP CARDIS 2000, pp 307-25 (2000)

⁸⁰ PAMPAS (Pioneering Advanced Mobile Privacy and Security) *Deliverable D03: Refined Roadmap* (28 February 2003) at www.pampas.eu.org

4.0.5 Authentication by implanted chip

The logical extension of RFID tags is the implantable transponder, already used as an identification device for many household pets and larger farm animals. In April 2002, Applied Digital Solutions was given approval by the US Food and Drug Administration for their VeriChip, a 12mm by 2 mm sized device⁸¹. Insertion of the unit using a hypodermic syringe can be performed as an outpatient or GP surgery procedure, under a local anaesthetic. Although the current applications call for association with other implanted prosthetic devices, the use for certain categories of prisoner could be envisaged. Clearly, all of the privacy and security concerns mentioned in the previous sections apply, as well as the potential for any unexpected medical side effects due to the invasive surgery.

4.1 Automatic face recognition (AFR)

As one of the longer established biometric systems, AFR has been available commercially for many years. The ubiquity of CCTV⁸², especially in the UK, has led to an increase in interest in the application of this technology for surveillance. A major area of research centres on the use of biometric techniques to match images recorded in photographs (such as those in passports and other identity documents) with real time video or photographs captured at a specific place or time. In the future, current research into emotional states and gesture recognition could add another dimension to the use of face recognition as more than a security mechanism.

Although at first sight, AFR appears to be an easy and acceptable method of authenticating individuals, in practice, the performance of many systems is very susceptible to changes in the angle of incident light and in the pose of the subject. The high incidence of twins in the population also acts as a security limitation, at least for some applications, although the developers of infrared imaged recognition systems claim that their method is less susceptible to twin confusion.

4.1.1 Principal methods⁸³

The following ways of operating an AFR system have been documented:

- capture and processing of the facial image by a single digital still or video camera using ambient light
- capture and processing of the image of a face under infrared illumination, or a mix of visible and infrared lighting
- capture and imaging of faces using stereoscopic camera systems

The most commonly used algorithms are based on the following approaches:

1. Spectral image decomposition.
This method seeks to break down the facial image into the sum of many sub-images. (These sub-images can be superimposed to reconstruct the facial image.) Such sub-images can either be *global* - representing parts of the entire face - or *local* - representing only parts of the face (e.g. upper right hand corner, middle, etc). *Principal Component Analysis* is a global representation commercialised by Viisage. *Local Feature Analysis* is a local representation, as commercialised by Identix, another US vendor. It is worth noting that neither method attempts to locate facial landmarks such as the nose, eyebrows, chin, etc; nor does either

⁸¹ Gaia Steden, *I've got you under my skin*, Global ID Magazine 6 pp 54-5 (2002)

⁸² Closed Circuit TeleVision Systems

⁸³ Note that not all methods are listed for this (or other) biometrics

method make use of direct physiological measurements such as the distance between landmarks. Neural networks can be used with either global or local methods to measure the similarity between enrolment and sample images of the face.

2. Elastic bunch graph matching.

The approach used by ZN-Vision represents the face by an elastic graphical overlay, fixing it to the specific pose and expression by adjustment of the key points on a face by an appropriate distortion of an originally rectangular mesh. Each node on the mesh is assigned a particular filter structure that represents local features in the vicinity of the node. Both local and global comparison of node features is made at verification.

3. Combination of spectral analysis and 3-dimensional modelling derived from geographical imaging systems. (This approach has been developed by Imagis Technologies of Canada.)

4.1.2 Principal commercially available systems

Identix (Visionics) (USA)	Commercialisation of research at Rockefeller University	http://www.identix.com
Viisage (USA)	Commercialisation of work by the MIT group	http://www.viisage.com/index.htm
Imagis (Canada)	Company diversified from a satellite image processing company	http://www.imagistechnologies.com
ZN Vision (Germany)	Commercialisation of research at Ruhr-Universitat Bochum and University of Southern California. In the process of acquisition by Viisage.	http://www.zn-ag.com
Cognitec (Germany)	Spin off from Siemens-Nixdorf	www.cognitec-systems.com

Template sizes for commercial systems are quoted in the range from 84 bytes to 1.3kbytes.

4.1.3 High profile deployments of facial recognition systems

Deployments using AFR include:

- London Borough of Newham's fitting of Visionics' algorithms to a network of CCTV cameras across this local council area in London. It has been claimed that the level of street crime was reduced through a deterrent effect, and surveys have shown that the local citizens feel safer for the addition of such a technology⁸⁴.
- A large trial of facial recognition from Cognitec has been underway for some time in Australia. The SmartGate project enrolled over 4000 Qantas crew members travelling through Sydney airport and now checks their identity by comparison of the passport photograph with the image captured by cameras at the immigration desk. Some unfavourable comments were voiced when it appeared that some Japanese

⁸⁴ CCTV: constant cameras track violators, NIJ Journal **249** p. 20 (2003)
www.ncjrs.org/pdffiles1/jr000249d.pdf for a description of the system in operation

businessmen were mistakenly authenticated after exchanging passports. The AU\$1m+ project is designed to be extended to other Australian airports from 2004 onwards, provided that the pilot is completed successfully.

- Announcement of the use of ZN Vision's facial recognition system in securing access for season ticket holders to Hannover Zoo in Germany. The potential deployment size is all of the 60,000 users of such tickets.
- Imagis has sold a system to Scotland's Grampian police authority to compare the identity of arrested individuals against the database of photographs of criminals.
- Imagis has also developed ChildBase, a facial recognition software package for the UK's National Crime Squad that aims to organise the many hundreds of thousands of Internet images of sexually abused children into clusters relating to individual children⁸⁵. Newly acquired images can be compared with others in the database to ascertain whether they are of an existing child or of a new victim. It has demonstrated the capability of grouping together brothers and sisters in the database.

4.1.4 Testing and issues of performance limitation

Tony Mansfield of the National Physical Laboratory lists the following evaluations of facial recognition systems (together with more recent testing)⁸⁶:

AcSys Biometrics		IBG 2001, FRVT 2002
Banque-Tec		FRVT 2000
Cognitec Systems		FRVT 2002
C-VIS		FRVT 2000, FRVT 2002
DCS AG	BioID	BIOIS 2000
Dermalog		BIOIS 2000
Dream Mirh		FRVT 2002
ETrue		FRVT 2000, IBG 1999
Eyematic Interfaces		FRVT 2002
Icinquest		FRVT 2002
Identix (Visionics)	FaceIT	NPL 2000
		FRVT 2000, FRVT 2002
		IBG 1999, IBG 2000
Imagis Technologies		FRVT 2002
Lau Technologies		FRVT 2000
Miros	Truface	ICSA 1998
Viisage		IBG 2001, FRVT 2002
VisionSphere Technologies		FRVT 2002
ZN Face		BIOIS 2000

The test centres undertaking these evaluations are as follows:

BIOIS Study: www.bsi.de/aufgaben/projekte/biometr/biois-e.pdf (May 2000)

FRVT 2000: Facial Recognition Vendor Test 2000 test of algorithms used in AFR with results at: (Feb 2001)

FRVT 2002: Face Recognition Vendor Test 2000, results at <http://www.frvt.org/FRVT2002/documents.htm> (March 2003)

IBG 1999, IBG 2000, IBG 2001 are three sets of scenario tests undertaken by the International Biometric Group, with details available for purchase from this consultancy

NPL (CESG/BWG) Scenario Testing:

<http://www.cesg.gov.uk/technology/biometrics/media/Biometric%20Test%20Report%20pt1.pdf>

⁸⁵ Lisa Kelly, *Police invest in ChildBase system*, Computing (16 July 2003)

⁸⁶ Tony Mansfield, *Report Biometric Performance Evaluations* (25 January 2002)

Best performing systems (technology evaluation: algorithm only)

The key conclusions from the most recent study of the algorithms used in AFR (the 2002 version of the FRVT) are summarised below. In the main test, photographs of more than 37,000 visa applicants were used, equal number of men and women, with a strong bias to subjects aged 18-40, and collected in Mexico by the US consulate). For each individual, at least three photographs were available, taken up to three years apart. All are front-facing (to within 10 degrees), the subjects co-operate with the system and have a neutral expression. As such, the results from this large scale test represent the performance of state-of-the-art algorithms under nearly ideal conditions. A significant proportion of the images were taken at less than 60 days after the initial photograph, and hence, the better performance for short term use such as for immigrant visas can be assessed. Nevertheless, we quote the average results for a range of separations in time.

- **Verification performance:** under reasonably controlled lighting conditions in an indoor environment, the best systems operate at the following levels of accuracy:

FRR is 10% for a FAR of 1%
FRR is 4% for a FAR of 10%

(More correctly, these figures relate to FNMR and FMR, since - amongst other differences - only one recognition attempt is made.)

The dramatic effect of changing lighting conditions is illustrated when tests are undertaken outside of the laboratory environment on the same day that one set of images were obtained indoors: the FRR increased from 4% to 46% for a FAR of 10%

- **Identification performance:** The results are stated for the percentage of faces that are correctly identified as the most likely match. The best system performed as follows:
 - the correct face was located as the top match 85% of the time in a database of 800 subjects;
 - the correct face was located as the top match 73% of the time in a database of 37,000 subjects;
 - the correct face appeared in the top 50 matches 87% of the time in a database of 37,000 subjects.
- **Watch list performance:** For a false alarm rate set at 1%, the best system performed as follows:
 - with a watch list of 25 people, it detected and identified them 77% of the time;
 - with a larger watch list of 3,000 people, this rate dropped to 56%

The data in the FRVT2002 evaluation enabled some other general conclusions to be made. Performance in successfully identifying individuals is not uniform across gender or age; it also deteriorates the longer the interval between an initial enrolment and subsequent recognition. Summarising the extensive data that is available, performance *decreases* by approximately 5% for each of the following;

- for females (males are recognised more easily)
- for every 10 years reduction in age (older people's faces are recognised more easily)
- for every year since the original photograph was taken (rapid ageing of faces)

Performance testing (access control scenario, together with watch list)

A report on the use of facial verification techniques in a scenario setting accompanied by a watch-list application has been published, using Identix (Visionics) equipment: a custom design for the verification scenario and FaceIT Surveillance and Argus for the

watch list application.⁸⁷ Approximately 140 subjects from a USA facility were enrolled on a video system and then re-recorded up to 38 days later, for assessment of the verification performance of the system. A database of 14,000 images from the same facility was collected for the watch list scenario.

Factors influencing the performance of systems:

Factors affecting the performance of systems operating using ambient illumination are⁸⁸:

- Changes in direction of incident light will often result in problems in enrolment or verification
- Some systems are particularly sensitive to the presence of glasses and will give poor verifications when the glasses are removed.
- A complex or confusing background behind the user may cause problems in identifying the position of the face.
- Variation in pose of the user (tilt and rotation angles greater than 20-30 degrees) will often degrade the performance of systems.
- Changes in the application of cosmetics, or colouration of the face can impact on system performance
- Beards, moustaches and change of hairstyle can affect the performance of systems
- Skin tone or colour may affect the algorithms locating the position of the face.
- Medical conditions such as bruising or temporary swelling of parts of the face may cause some system to perform less effectively.
- The facial appearance of young people or very old individuals may change quickly, so that templates may need to be updated at more frequent intervals.

The susceptibility of algorithms to each factor will vary, with extensive testing the only way of ascertaining how well each system performs.

Security evaluations

There have been no formal security evaluations of face recognition systems. In its testing of devices for simple spoofing, the German magazine *c't* showed that simple 'live and well' measures to detect the presentation of a still image were insufficient. In the specific case quoted, the replay of a video clip in which the subject moved from side to side was accepted as a live individual.⁸⁹

TNO in the Netherlands have undertaken research into the detection of 'look-alikes', a key concern for passport issuing authorities. 3 commercial systems were trialed using 129 subjects over a period of 6 weeks. In general, the results were not encouraging; indeed, some of the lower quality photographs performed better than higher quality ones, possibly due to a wider range of expressions being captured in the latter case⁹⁰.

4.1.5 User concerns

Integration of AFR systems into surveillance systems is a contentious issue. Its trial at the Super Bowl 2001 in a covert manner caused significant embarrassment⁹¹ that was not

⁸⁷ Mike Bone and Duane Blackburn, *Face Recognition at a Chokepoint: Scenario Evaluation Results* (14 November 2002)

⁸⁸ Tony Mansfield, *Best Practices in Testing and Reporting Performance of Biometric Devices* (Version 2.01, August 2002).

⁸⁹ Lisa Thalheim et al, *Body Check: Biometric Access Protection Devices and their Programs put to the Test*, <http://www.heise.de/ct/english/02/11/114/>

⁹⁰ Koos van Woerden, *biometrics in travel documents: suitability of face recognition for look-alike detection*, European Conference for Issuing Authorities of Travel Documents, The Hague (20-21 June 2002)

⁹¹ *ACLU Calls For Public Hearings on Tampa's "Snooper Bowl" Video Surveillance* <http://www.aclufl.org/snooperbowl2-01.html>

helped by its subsequent use in a couple of Florida cities. More recent criticism has centred on the limited performance in trials of AFR for watch-lists at US airports, even though the results were in line with the conclusions of the FRVT trials mentioned above. Expectations of much better performance had been raised and there is a need for an open discussion of this type of application.

The deployment of an AFR in the London Borough of Newham was, in contrast, handled with sensitivity, with prominent notices displayed in the neighbourhood and continued dialogue with the local community. It should be noted, however, that even in this case, many citizens were unclear about the role of the police authorities and the capabilities of the technology.

Thermal images may offer additional information about the subject. For example, Pavlidis *et al* at Honeywell showed that when subjects were startled, there was an instantaneous redistribution of blood flows away from the cheeks and towards the eyes⁹².

A full discussion of the issues is available in an article by Philip Agre of UCLA⁹³. He lists the following arguments against the deployment of systems:

- High potential for abuse
- Ease of aggregation of data with that from other systems
- Inaccuracy in operation of AFR systems
- An inappropriate technology for the requirements that are made upon it
- Impact of its use in shopping malls, etc, changing the power balance between shopper and retailer
- Lack of understanding by citizens of the possibilities of such systems
- Difficulty of providing notice of the existence of such systems in public places
- Deployment in other countries where controls on abuse are less or absent

System operators should take such observations into account when designing public-facing deployments, working to Codes of Practice that have been agreed locally.

4.1.6 Legal and regulatory dimensions

Privacy issues with regard to AFR include the fear of loss of control through better possibilities of tracking and tracing people, creating high substantial personal profiles and increase video surveillance.

Also of concern is the unwarranted possible link to watchlists, for example of suspected criminals. One measure to establish more transparency and therefore minimise the worries of citizens, is the legal obligation (e.g. in German privacy law) to always give visible notice of the use of video surveillance in public places as metro stations or buses.

4.1.7 Standardisation activities relevant to face recognition

Standardised data formats for the interchange of facial image data are recognised as a requirement for the interoperability between applications and instances of the application. Work is underway in the ISO/IEC standardisation activity to define such formats, with text of ISO/IEC 19794-5 being circulated for comment and balloting by national bodies.

⁹² I Pavlidis *et al*, *The face of fear*, The Lancet **357** (9270) (2001)

⁹³ Philip Agre, *Your face is not a bar code: arguments against automatic face recognition in public places*, dlis.gseis.ucla.edu/people/pagre/bar-code.html (5 May 2003)

4.1.8 Principal research projects developing facial recognition systems

Results of research are available in the open literature and in conferences such as the IEEE International Conference on Automatic Face and Gesture Recognition⁹⁴ and the AVBPA, International Conference on Audio- and Video-based Biometric Person Authentication⁹⁵.

University of Manchester (Dr Tim Cootes) <http://www.st-outreach.org.uk/docs/studies/cs-43.htm> A European Commission funded project, IST-1999-11587 U-FACE (User friendly face access control system for physical access and healthcare applications) ended in October 2002 (<http://www.uface.org>). The same team leads on a DTI-sponsored research project – SCID – that aims to develop technologies to link facial biometrics with vehicle identification technologies to support authentication in ‘drive-in’ retail applications⁹⁶.

Another UK project aiming to use facial image systems is CRIME-VUs, but the automatic aspect of biometrics is less important in this proposal. This work, led by Stirling University, is investigating whether the use of three-dimensional reconstruction of faces can help with the identification of criminals⁹⁷. A further project in the same DTI research portfolio addresses intelligent analysis of CCTV footage to identify unusual and unexpected behaviour⁹⁸.

HISCORE is a project developing a leading edge 3D- and colour subsystem based on off-the-shelf CCTV-cameras and projectors and validate this subsystem in two application areas - face recognition and gesture recognition⁹⁹.

The COST 275 consortium is addressing opportunities for remote, online recognition of consumers using both speech and facial biometrics in a co-operative programme that is scheduled for completion by 2005¹⁰⁰.

4.1.9 Outlook for the future

AFR has the potential for creative integration with other technologies to add value beyond simple authentication in support of the developing vision of *pervasive computing* or *ambient intelligence*. The performance of current basic systems limits its direct usefulness for many applications. However, the large number of extensive databases of photographic images, and the relatively low cost and high availability of hardware, argues for increased investment in new and improved approaches. The key aspects that need to be resolved are¹⁰¹:

- Impact of *partial occlusion* of the face, such as the placement of hands, large sunglasses, and reading matter.
- Variation in *pose* of subjects, beyond about 30-40 degrees of the rotation of the head. Evidence from FRVT2002 shows that morphing of off-axis images into what they could look like when face-on dramatically improves the performance of algorithms.
- Variation in *illumination*. In particular, FRVT2002 showed that changes from internal artificially lit environments to operation outdoors nearly halved the rates of verification.

⁹⁴ The most recent conference in the 5th IEEE International Conference on Automatic Face and Gesture Recognition, Washington, DC (20-21 May 2002)

⁹⁵ The most recent one is the 5th in the series, held in Surrey University, UK
<http://avbpa2003.ee.surrey.ac.uk>

⁹⁶ <http://www.dti-mi.org.uk/newweb/scid.htm>

⁹⁷ <http://www.psychology.stir.ac.uk/crimevus/index.htm>

⁹⁸ <http://www.dcs.qmul.ac.uk/research/vision/projects/ICONS>

⁹⁹ <http://uranus.ee.auth.gr/hiscore>

¹⁰⁰ <http://www.fub.it/cost275/>

¹⁰¹ Ralph Gross *et al*, *Quo Vadis Face Recognition*, Report CMU-RI-TR-01-17 (June 2001), dagwood.vsam.ricmu.edu/FaceRecognition/Html/discussion.htm

- Performance degradation as a function of *time*.
- Changes in *expression*, especially when mouth deformation or eye narrowing occurs.
- Performance dependencies on *gender* and *age*.
- Registration of the probe image and the stored database of faces.

Current areas of research interest include the use of infrared methods¹⁰² (which are claimed to offer more degrees of freedom) and exciting work with three-dimensional methods of coding of the face. There is also early evidence linking improvements in performance to higher resolution images, both in spatial dimension and intensity¹⁰³. Some researchers also believe that there is still much to be gained from a better understanding of how the brain recognises previously met people¹⁰⁴.

There is also some disagreement on whether video sequences help recognition. FRVT2002 results seemed to demonstrate that this is not the case, even degrading the performance of some systems. Another area of continuing research is into three-dimensional imaging of faces. An intermediate stage of taking up to 5 images at different pose angles during enrolment has been examined.

Whatever techniques are used, the route forward could be the integration of

- a) methods that develop a model of the face from a gallery of many images of the face under different conditions and
- b) the result of a knowledge base using the best available information as to how the face changes as a function of the variables mentioned above.

At the same time, new ideas continue to emerge. In early 2003, a software house, Delean Vision¹⁰⁵, announced a new approach, based upon reflectivity of skin surfaces, either from the face or hands. This should depend upon the shape of features on the face, their textures and the colouration. Full images are stored, resulting in a template size of over 100kB.

The potential for integration with systems that offer so-called *intelligent HCI* can be assessed with reference to work such as that of computer-based interpretation of human activities¹⁰⁶. Clearly, there are major risks to users' privacy through the extension of such applications¹⁰⁷, and any R&D projects should build in protection measures to limit the opportunities for such abuse.

The field of intelligent video surveillance has been reviewed as part of the EC funded European Research Network for cognitive AI-enabled Computer Vision Systems¹⁰⁸. Section 4.2.3 of their Roadmap summarises the research agenda:

¹⁰² Francine Prokoski, *History, Current Status, and Future of Infrared Identification*, [IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications \(CVBVS 2000\)](#) and Jonathan Dowdall et al, *Face Detection in the near-IR spectrum* <http://www.cs.unr.edu/~bebis/facedetectionIR.pdf> Image and Vision Computing (paper accepted)

¹⁰³ Comment by Jonathon Phillips at the 4th International conference on Audio- and Video- Based Biometric person Authentication Conference, AVBPA 2003, Surrey (June 2003)

¹⁰⁴ Rama Chellappa et al, *Human and machine recognition of faces: a survey*, Proceedings of the IEEE, **83** (5) 705-740 (May 1995) Section III; Vicki Bruce and Andy Young, *In the eye of the beholder: the science of face perception*, Oxford University Press (1999)

¹⁰⁵ deleanvision.com

¹⁰⁶ Zoran Duric et al, *Integrating Perceptual and Cognitive Modelling for Adaptive and Intelligent Human-Computer Interaction*, Proc of the IEEE, **90**(7) 1272 –1289 (July 2002)

¹⁰⁷ Ioannis Pavlidis et al, *Thermal Imaging for Anxiety Detection*, [IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications \(CVBVS 2000\)](#)

¹⁰⁸ James Crowley, *Cognitive vision research roadmap*, IST-2001-35454, Section 4.3 (draft 2.5 25 March 2003) www.ecvision.info

- Robust, real-time algorithms and systems with the ability to perform with minimal manual reconfiguration on variable environments, with self-calibration and automatic adaptation to cope with changes in lighting, scene geometry and activity;
- Systems able to cope seamlessly with addition or removal of new cameras and sensors, with ease of installation and maintenance in general;
- Systems able to work over periods of months with minimal human intervention;
- Continuous and accurate annotation of activities in the field of view using natural languages, i.e. the recognition of the behaviour of people and vehicles and prediction of further activity based upon the application area, together with decision-making capabilities based upon such data;
- Development of application-independent platforms based upon underlying knowledge bases;
- Particular attention to security and integrity of the data, especially for evidential use of the images. Privacy issues need to be resolved as well as linking to other measures in crime prevention.

4.2 Fingerprint recognition

The use of finger and palm impressions to seal transaction has been prevalent for at least two centuries. However, the scientific study of the ridge detail was not undertaken until the latter part of the 19th century, and even then, this research was focussed on possible classification of groups and not individuals. These studies concluded that ridge detail exhibited a high degree of immutability and uniqueness. The first reference to fingerprints as a 'forensic' tool came in 1880 with the publication of an article by Henry Faulds in the scientific journal, *Nature*. By the early 20th century, fingerprints had largely superseded the use of the 'anthropometric' system of measurement that had been devised and championed by Alphonse Bertillon.¹⁰⁹ Concern about the accuracy of that system had followed a number of high profile mistakes caused by human error and incorrect statistical assumptions that were inherent in the system. It should be noted that the rise of fingerprints as the principal means of verification of identity within criminal justice systems in the early 20th century has resulted in the legislative position being firmly biased towards this form of identification.

The challenge of partially automating the process of identifying possible matches of latent prints left at the scene of crime with previously stored records preoccupied the forensic services of many police forces. Extensive automation of the process, through the development of Automated Fingerprint Identification System (AFIS) technology has only proven feasible in the past quarter century, with final comparison still being left to expert examiners. Three suppliers dominate the market, with relatively few standards locking many systems into one of these proprietary solutions. Capture of the fingerprint data from suspects has also moved from the traditional 'ink and paper' method to **live-scan** optical systems some of which can collect all 10 prints in a single imaging of both hands on a large glass plate.

Many suppliers and commentators argue that AFIS systems should not be regarded as true biometric technologies, and aim to distance their offerings from the algorithms and processes used in conventional systems sold into the criminal justice sector. Nevertheless, a significant majority of non-AFIS biometrics still uses the same minutiae method (the fine detail in the ridge and valley structure of a fingerprint) that underpin AFIS technologies. However, the impossibility of reconstructing a full fingerprint image from the template data, and the major task of translating *these* suppliers' biometric templates into a form that enables direct comparison with those held by criminal records offices, should assure some critics.

¹⁰⁹ Richard Caplan, *How fingerprints came into use for personal identification*, Journal of the American Academy of Dermatology **23** (1), 109-114 (July 1990)

Nevertheless, proposals for national civilian identification schemes (civil ID) do appear to be based upon current AFIS solutions. Indeed, the current proposals for ISO standards for civil systems under development in SC 37 are moving closer to those in use by the criminal justice sector (ANSI/NIST ITL 1-2000). Although data protection legislation in Europe *could* require separation of the two types of system, strong technical and procedural controls would need to be developed to limit the opportunity for 'function creep'. In other countries, the checking of images of fingerprints - obtained at the time of enrolment into civil ID or immigrant visa schemes - against databases of criminals may not be protected in similar ways.

The wealth of data about fingerprints (for example, the experience in legal acceptability of expert evidence in criminal cases, and the incidence of missing fingers or difficult-to-read prints) could underpin any legal challenge to authentication of users by means of this method. *Note, however, that the specific ways in which the biometric is implemented will limit the accuracy of the method and the consequent room for non-repudiation and legal admissibility.*

A recent text on the ways in which fingerprint recognition systems have been developed and tested gives considerably more detail about current practice and capabilities¹¹⁰.

4.2.1 Principal methods

A fingerprint is constructed and classified using three levels of detail in the pattern of curving line structures called *ridges*¹¹¹, where the skin has a higher profile than in surroundings *valleys*:

- The first level of detail consists of the patterns formed by the raised ridges contained on the surfaces of the fingertips and the valleys between them. This level may take account of the pattern, its orientation and other features such as the number of ridges present between measurable points - such as the innermost recurving ridge of a loop pattern and the delta where ridges come together in a clearly distinguishable way.
- Second level detail takes the comparison of one fingerprint impression against another to the minutiae level, where fixed points on the ridges are identified and plotted. Usually these features are plotted at either the point where the ridge divides (at a *bifurcation*), or where it ends (*ridge ending*). Such minutiae maps can then be compared across the two impressions, either manually or using feature comparison algorithms.
- Third level detail takes account of the positions of the individual pores on a friction ridge (*poroscopy*) or the patterns that are formed along the edges of the edges of the ridges (*ridgeology*) - techniques that are being used increasingly within law enforcement applications, especially where only small parts of the detail of finger ridges are available.

However, images are plastically deformed when fingers are pressed against a hard surface in asymmetric ways. These images are also subject to noise in the form of dirt, scratches on the fingerprint surface, etc. Hence it is not possible to match one fingerprint image against another in a simple way. The aim of biometric systems is to extract features in ways that are robust to these effects generally using second level detail.

The most common form of the fingerprint biometric system has two primary components: the sensor and the algorithm that processes the image to a template and subsequently compares captured images in operation of the system with the stored template.

Sensors

¹¹⁰ Davide Maltoni *et al*, *Handbook of Fingerprint Recognition*, Springer-Verlag (2003)

¹¹¹ Asker M Bazen, *Fingerprint Identification – Feature Extraction, Matching, and Database Search*. PhD thesis (August 19th 2002).

Seven types of sensor are recognised:

- **Optical sensing.** Usually offered in the form of an optical prism with a source of light on one face, a camera on another face to sense the light that is reflected off the finger that is pressed against a third face of the prism. Total internal reflection off the ridges modulates the incident light to develop an image of the fingerprint pattern. Initially quite large, smaller units to fit into a PC mouse have been commercialised. Sub-\$100 complete peripherals (PC mouse) have been marketed.
- **Capacitive Silicon.** Introduced in the mid 1990's, these are similar to an unpackaged IC. A thin sliver of silicon is processed into a fine matrixed array of small capacitors with the finger offering the other plate. The distance between a ridge and the silicon plate differs from that between a valley point and its corresponding point on the silicon, leading to a difference in the capacitance, the distribution of which images the fingerprint detail. Two forms are available: dc and ac coupled. A number of European suppliers offer this type of device (Infineon, Fingerprint Cards, ST Microelectronics), and 'whole finger' versions of up to 18mm by 13mm sensing area are available, as well as much smaller ones (down to 10mm by 1mm), for applications where the cost of silicon or miniaturisation are important considerations. In the past, there have been some problems with resistance to electrostatic discharges and performance with very dry or very moist fingers. Current pricing is in the \$25-40 unit price in 10,000 unit quantities, with the aim to reduce this to a \$5 unit cost in the near future. Smaller area devices that can be swept by the finger reduce the cost to about \$10 each in 10,000 unit orders (2002 prices). An example of the device integrated into a component is the Siemens PC mouse, priced at \$129.
- **Electric field sensors.** Similar in form factor, to the capacitive silicon device, an electric-field sensing device is available from Authentec.
- **Thermoelectric sweep sensor.** Atmel offer a 14mm by 0.4mm linear sensor that responds to the difference in temperature and thermal conduction between the ridge in contact with a semiconductor surface and the valley where there is no contact. A version is integrated into the popular iPAQ h5400 Pocket PC.
- **Ultrasonic sensing.** A quite large unit that is claimed to have better performance as it senses the pattern of the ridges underneath the skin surface, thereby reducing the effect of surface dirt and skin cuts. There is one commercial supplier, Ultra-Scan.
- **Pressure array.** BMF/Hitachi have recently a device with a two-dimensional matrix of micro-miniature pressure sensors that is claimed to be more resistant to spoofing by a synthetic finger
- **Electro-optic plastic sensors combined with a photodiode array**

The performance of these devices varies considerably. In particular, users should ascertain whether these devices will meet the criteria required in their specific application relating to:

- Cost
- Robustness, resistance to ageing, durability
- Power consumption in quiescent and operational modes
- Size
- Dot pitch
- Behaviour under electro-static discharge
- Environmental operation for sweaty and dry fingers
- Resistance to false finger submission and other security issues
- Usability

Notwithstanding these concerns, the future of fingerprint biometrics seems to be assured, with many now being available in the top end of consumer and business electronic equipment. Examples are PDAs (HP's iPAQ h5400), laptop PCs (Samsung PC10), mobile phones (DoCoMo F505i) and secure mass storage through the use of USB peripherals with fingerprint access control (e.g. Thumbdrive Touch for up to 256Mb storage priced at \$249)

4.2.2 Principal commercially available systems

This is a fast developing area, as the prospect of volume application to electronic and computer equipment becomes more real. At the time of writing, the main suppliers of hardware in this sector of the fingerprint biometric market are:

- Atmel
- Authentec
- Fingerprint Cards
- Fujitsu
- Identix
- Infineon
- Secugen
- Sony
- ST Microelectronics
- Ultra-Scan
- Veridicom

Companies such as Sagem and Identix are key suppliers in the livescan market.

Algorithms for use with these sensors are developed by a number of companies, amongst which are

- Cogent, NEC, Printrack and Sagem for AFIS systems
- Bioscrypt, Siemens and many others for the smaller size market.

Template size for systems is generally in the range of 250 bytes to 1kbyte, although IBM have used systems with 80kbytes to improve search times through large databases.

4.2.3 High Profile deployments

An early use of fingerprint biometrics was in the securing of payments to the retired and dependants of miners in South Africa. Over the past decade, this has grown to regular payments to over 1 million people, with the original system being superseded by a more modern version.

Many high profile welfare payment systems in the USA have also been secured by the use of fingerprint biometrics, with the primary aim of preventing multiple applications for social security payments in different counties in the same state. The longest established one - in California - has annual running costs of \$11m, but has recently been subjected to criticism for these high costs.

In the UK, asylum seekers now have to register and be fingerprinted. These fingerprints are checked against previous applicants who have been refused entry. Certain ports of entry are equipped with portable units that enable a quick check to be made against the same database.

A major project to register 60m Nigerian voters was undertaken recently using 60,000 'systems in a briefcase' comprising a digital camera and an automatic fingerprint reader unit from Sagem - its *MorphoTouch*.

As from January 2003, asylum seekers applying to countries within most of the EU will be checked against the EURODAC database of fingerprints of such applicants, in order to determine the country responsible for their processing and to prevent multiple applications for permission to stay. Strict controls apply to access and use of the information.

4.2.4 Testing and issues of performance limitation

Testing of algorithms used in fingerprint recognition has been undertaken by a consortium of the Biometric System Lab at the University of Bologna, the Pattern Recognition and Image Processing Laboratory of Michigan State University and the U.S. National Biometric Test Center at San Jose State University. Two rounds of testing have been completed, with results from the later one, FVC2002 released early in 2003¹¹². The total number of algorithms tested in FVC2002 is 31. Four databases of fingerprint images were used as the test group (including one with synthetically generated images). Tests were conducted with two optical and one capacitive scanner. Several aspects of the test should be noted:

- The test was designed to compare the performance of algorithms only, and the use of different types of sensor was incidental to the main purpose of the test
- The sample size was small (90 students) and the average age was unrepresentative of most applications (20 years old)
- Each subject was tested three times, with a minimum of two weeks separating each test
- Only four fingers were tested; the forefinger and middle finger of each hand
- Attempts to examine the effect the impact of wet and dry fingers and exaggerated finger misalignment were included in the third session

The best performing algorithms demonstrated the following performance:

Sensor	Equal error rate	False non-match rate for False match rate of 1%	False non-match rate for False match rate of 0.1%
Optical	0.1%	0.11%	0.21%
Capacitive	0.37%	0.32%	0.61%

These results should be used as a guide to the best performance that can be expected for the algorithm only under the stated testing conditions.

A technology evaluation of large and small scale fingerprint matching technologies has been announced recently by NIST¹¹³. Termed FpVTE (FingerPrint Vendor technology Evaluation), it will use multiple tests to evaluate the performance with combinations of fingers from 1-10, using the methodologies that NIST have developed for automatic face recognition in the FRVT2002 series of tests. It will cover different types of operational systems from (single and multiple finger) livescan as used for visa enrolment and police booking systems through to comparison with rolled and flat inked fingerprints in legacy criminal databases.

The International Biometric Group undertook four rounds of testing between July 1999 and December 2002¹¹⁴. Little information is available publicly on the results of such testing, although the most recent group involved checking of performance twice only - once after enrolment and once again several weeks afterwards. The most recent tests covered systems from the following fingerprint suppliers: Bioscrypt, DigitalPersona, Fujitsu, Identix, Indivos, Siemens, STMicro and Ultra-scan. The 2001 series included evaluation of products from BES, Identix, Precise Biometrics, Sagem Morpho, SecuGen and Sony.

As in any biometric, the key to good performance is in ensuring a high quality enrolment. This requires training of the enrolment officials and clear instructions to end users (either by the official or by the equipment), together with an effective software package that

¹¹² D Maio *et al*, *FVC2002: Second Fingerprint Verification Competition*, (2002) at <http://bias.csr.unibo.it/fvc2002>

¹¹³ <http://fpvte.nist.gov>

¹¹⁴ www.ibgweb.com/reports/public/comparative_biometric_testing.html

detects when the enrolment is of indifferent quality. These may request the user to reposition their finger, or to apply more or less pressure. More than one try should be required to examine repeatability, although the range of variation is of necessity likely to be small, with users often being careful to reposition their fingers. Similarly, in operation, the image capture needs to be optimised, e.g. through regular cleaning of the contact surfaces.

Controversy continues as to whether the template should be updated with time. There are security considerations in not allowing any changes to the template, as the fingerprint details should remain stable over the middle part of the subject's life; during childhood, the resolution of scanners may not be sufficient to obtain the required level of detail, and as people get older, the elasticity of the skin may pose other problems. Nevertheless, very good images may be occasionally detected during operational use, which could improve the subsequent performance. Also as more of the finger is accessed, through unintentional displacements during the operation of the biometric, more minutiae points may be discovered (or a larger part of the fingerprint mapped, in the case of non-minutiae based systems). The decision requires a more detailed understanding of the application and its security demands, although there appears to be some evidence in favour of template updates.

Large scale fingerprint identity systems (such as those used for the matching of fingerprints at the scene of crime) operate in a different environment from those described above – often with specialist hardware and software. The performance of these systems is highly tuned to the particular deployment. With the introduction of civil AFIS systems (for checking of identities before the issue of passports or visas, or use in a border control application), independent assessment of the system performance is required prior to sizing and specification for a given environment. As one of the requirements following from the USA's Enhanced Border Security and Visa Entry Reform Act, NIST was charged with a study on the performance of such specialist systems. The key results of this study¹¹⁵ have been published as an executive summary of the results and recommendations on face, fingerprint and iris recognition (the main conclusions are summarised in Section 6.2), with a more recent detailed report providing the supporting evidence for the conclusions in respect of fingerprint verification. Most of this study refers to a matcher developed using COTS¹¹⁶ hardware and software, although an initial comparison with commercial AFIS systems validates the conclusions from the COTS evaluation.

Security and security evaluations

The first biometric to be evaluated against the Common Criteria was Bioscrypt's Enterprise for NT Logon, version 2.1.3¹¹⁷ with a determination that the system as tested could be trusted to an assurance level of EAL2 - a rather low level of assurance on the scale from EAL1 to EAL7.

Fingerprint systems have featured prominently in the well-reported informal tests carried out in 2002. For example, the tests described in the German magazine *c't* showed that a well-known fingerprint-secured PC mouse was successfully circumvented¹¹⁸. A latent print left on the device, was reactivated, allowing the verification of the preceding person.. Clearly, a software solution to this problem, checking successive images for exact matches could have avoided this problem. In a separate test, false fingers made

¹¹⁵ Charles Wilson *et al*, *Studies of fingerprint matching using the NIST Verification Test Bed (VTS)*, NISTIR 7020, NIST (7 July 2003)

¹¹⁶ COTS: 'Commercial Off The Shelf' components.

¹¹⁷ <http://www.cse-cst.gc.ca/en/services/ccs/bioscrypt.html>

¹¹⁸ *Body Check: Biometric Access Protection Devices and their Programs Put to the Test*, *c't* (11/2002, p 114 translation) <http://www.heise.de/ct/english/02/11/114>

from gelatin were accepted by many fingerprint biometric devices¹¹⁹. The threat that this poses to the security devices should be measured against the difficulty in making such fake fingers if users are unco-operative. These results have prompted extensive research into the hardening of devices through the addition of 'live and well' functionality. Valorie Valencia has characterised such methods as making use of:

- Intrinsic properties of a living body (such as the reflectance spectrum from a live skin surface or the oxygen interchange in blood)
- Signals generated involuntarily by a living body (such as the pulsing of blood, transpiration of gasses and body odour and electrical signals such as ECG).
- Bodily response to a stimulus through a challenge-response approach (e.g. the dynamic change of skin colour when a finger is pressed against a surface)¹²⁰

The Hungarian company, Guardware, was one of the first companies to claim a fingerprint biometric device that addresses these issues in a satisfactory way¹²¹.

4.2.5 User concerns

Anecdotal evidence suggests that some users are concerned about the ability of third parties to abuse the trust placed in single application use of fingerprint biometrics, in particular through the linkage that a fingerprint system could allow to other information, should the biometric be used as a unique identifier. For them, the possible link to existing criminal records adds to their concerns. Clear statements of principle and independent verification of security controls may be one way to assuage these fears. In other cases, the avoidance of centralised databases may be key.

Other commentators believe that it may strike against the principle of informational self-determination: the control that human beings should be able to exercise over personal data about themselves.

4.2.6 Legal and regulatory dimensions

Some countries have specific laws that apply to fingerprint recognition that could limit the wider use of fingerprints in commercial security systems.

4.2.7 Standardisation activities

Standards work in relation to the exchange of data has been accelerated by the formation of ISO/IEC JTC1/SC37. Existing FBI standards¹²² for data compression and interchange of images form the basis for some of this work. Currently the multi-part standard ISO/IEC 19794 for data interchange formats has three parts devoted to fingerprint biometrics:

- Part 2: Finger Minutiae
- Part 3: Finger Patterns
- Part 4: Finger Images

¹¹⁹ T. Matsumoto *et al*, *Impact of Artificial Gummy Fingers on Fingerprint Systems*, Proceedings of SPIE Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

¹²⁰ Valorie Valencia, *Biometric Liveness Testing*, CardTechSecureTech 2002

¹²¹ <http://www.guardware.com>

¹²² NIST, *American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial & Scar Mark & Tattoo (SMT) Information*, ANSI/NIST-ITL 1-2000, NIST Special Publication 500-245 (27 July 2000)

4.2.8 Principal research projects

With the increase in the probability of implementation of solutions using fingerprint biometrics, there is a recognition of the need to accelerate research and development to assure operators, integrators and end users of their robustness, security, usability, etc. Among the target areas for such research are:

- **Device interoperability**, allowing users to enrol on one reader with its specific performance and characteristics, while verification can take place on a number of proprietary platforms.
- **Lightweight fingerprint verification**. Many opportunities for biometric solutions will require operation with restricted memory and processing capabilities. The authentication device maybe be embedded in systems that have very clear limitations and complex algorithms may not port to these, either in terms of storage capacity or the decision times. Examples of systems where such limitations may apply include smart cards, mobile phones and PDAs.
- **Fingerprint watermarking**. Watermarking of fingerprint images aims to embed watermark information along with the fingerprint image without impacting on the performance of the system as a biometric. The aim is improve the security of the fingerprint transfer, storage and use.¹²³
- **Secure devices**. For fingerprint biometrics to be used in medium-to-high security environments, e.g. in laptop computers holding company confidential information, the security of the core devices and their interfaces to applications may have to be improved. Some systems recognise this and Sony's FIU-900 peripheral shows how some of the requirements may be addressed. Storage of secret and private keys (for symmetric and asymmetric cryptography, respectively), tamper-resistance and anti-spoofing measures may all need to be considered.
- **Continuous classification schemes** where fingerprints are not classified in non-overlapping classes, but are characterised by a numerical vector summarising its main features
- **Pattern matching algorithms**, which have shown to be capable of providing very high levels of accuracy
- **Fingerprint image mosaicing techniques** to increase accuracy with the recent increase in interest in small sensors
- **Fingerprint video recognition**. Using a video sequence of images in place of a single still image for the recognition purposes

New sensors are continually being developed. SABRINA, an EC project, is producing prototype versions of a miniature ultrasonic device under the leadership of Hitex¹²⁴. FingerCard was a recently completed EC-sponsored project using Infineon sensors integrated onto smart cards and was directed towards an understanding of the technical, user and commercial opportunities that such a card could offer¹²⁵. The E-POLL project has developed a electronic voting system incorporating fingerprint biometric security¹²⁶. PAIDFAIR is yet another EC project that will use fingerprint biometrics as part of a Digital Rights Management solution¹²⁷. Finally, ViPBoB is a project that addresses the template storage risks, by developing a Virtual PIN. Fingerprint biometrics will be used to demonstrate the system¹²⁸.

4.2.9 Outlook for the future

A greater diversity of fingerprint devices is available than for any other biometric. If they gain acceptance and production volumes rise, the price per unit is bound to fall.

¹²³ <http://biometrics.cse.msu.edu/abstracts.html>

¹²⁴ <http://www.sabrina.uni-karlsruhe.de/publicdescription.html>

¹²⁵ <http://www.iht.com/articles/75010.html> and <http://www.hsb.nl/fingercard.html>

¹²⁶ <http://www.e-poll-project.net/innovations.htm>

¹²⁷ http://virtualgoods.tu-ilmenau.de/2003/VG_Codimeter.pdf

¹²⁸ <http://vipbob.gi-de.com/vipbob/index.html>

Nevertheless, there are still considerable challenges to be met, not least from the user acceptance perspective.

Fingerprint verification may be a good choice for closed user groups, in which users can be given adequate explanation and training, and where the system operates in a controlled environment. It is therefore not surprising that the biometric of choice for logical access control on workstations is the fingerprint, due to the relatively low cost, small size, and the ease of integration of fingerprint authentication devices.

As electronic devices begin to be used in more high value applications, e.g. 3G mobile phone services and e-commerce starts gaining momentum, the attraction of securing these services with biometrics will become ever more evident. The range of possible applications can be deduced from the following current commercial deployments (albeit in small numbers at present):

- PDAs (HP's iPAQ h5400 available at £499 in the UK)
- laptop PCs (Samsung PC10)
- mobile phones (DoCoMo F505i)
- secure mass storage through the use of USB peripherals with fingerprint access control (e.g. Thumbdrive Touch for up to 256Mb storage priced at \$249)
- cars (one-touch personalisation for up to four individual drivers of the Audi A8 using a fingerprint sensor to the side of the gear change adds approximately £1,000 to a £50,000 car. Seats, mirrors, steering column and air conditioning are preset for each person.)

4.3 Iris Recognition

First of all, we should note the existence of two separate methods of making use of the eye as a biometric. Iris Recognition, the newer approach, takes images of the visible, coloured, part of the eye and processes these into templates called iriscode. An older and very different approach, which is no longer being actively marketed, is retinal scanning. Retinal scanning requires considerably more co-operation from the user, imaging the pattern of red blood vessels behind the eyeball and requiring more sophisticated optical instrumentation.

Iris recognition is a relative newcomer to the portfolio of biometric methods, yet it has established itself as a key technology with the potential of addressing many of the more demanding applications for secure authentication. In particular, it holds great promise for use in large scale identification systems, where individual distinctiveness of a template is a critical requirement. It is therefore a competitor to AFIS fingerprint systems and should be considered wherever there are public concerns about crossover use between criminal and civil identification systems. However, the lack of experience in working with large numbers of users puts it at a disadvantage with the century of experience with the use of fingerprints.

4.3.1 Principal methods

Iris recognition systems operate by capturing an image of the eye (generally using visible and IR illumination). The concept patent for iris recognition is held by Iridian, and expires in 2004/5. A variety of algorithms¹²⁹ for extracting biometric data from the iris image and comparing sample against templates have been proposed; those by Daugman, Lim and Noh are implemented in commercial systems.

¹²⁹ Information obtained from the website www.iris-recognition.org maintained by Jan Ernst

Daugman ¹³⁰	2D-Gabor demodulation. Hamming distance for classification. These algorithms are licensed by Iridian, and are used in several commercial systems.
Wildes et al. ¹³¹	Patented early prototype. Sophisticated hardware setting to obtain undistorted and high-quality image data.
Boles and Boashash ¹³²	Zero-crossings of one-dimensional wavelet transforms.
Zhu et al. ¹³³	Gabor- and multiresolution analysis.
Lim et al. ¹³⁴	Wavelet features, competitive learning approach. Used in some commercial systems
Muron et al. ¹³⁵	Highly proprietary hardware. Using optical Fourier power spectrum.
Tisse et al. ¹³⁶	Frequency analysis of the <i>analytic image</i>
Noh et al. ¹³⁷	Multiresolution ICA approach Used in some commercial systems

4.3.2 Principal commercially available systems

Company	Products	Algorithm
Panasonic	BEM-ET100(<i>Authenticam</i>) BEM-ET300 BEM-ET500	Daugman
Oki	IrisPass-handheld IrisPass-WG	
LG Electronics	IrisAccess 2200 IrisAccess 3000	
Alpha Engineering	Veri-Iris	Noh
Evermedia	EVER COPE EC-1100	Lim
Senex	TrueEye	
Neurotechnologija	VeriEye	
IriTech	Iris2000	

¹³⁰ Daugman J. *High Confidence Visual Recognition of Persons by a Test of Statistical Independence*, PAMI 15(11) Nov 1993, 1148-1161

¹³¹ Wildes R, Asmuth JC, Green GL, Hsu SC, Kolczynski RJ, Matey JR & McBride SE. *A system for automated iris recognition*, IEEE Workshop on Applications of Computer Vision, 1994

Wildes RP. *Iris Recognition: An Emerging Biometric Technology*, PIEEE 85(9) Sept 1997, 1348-1363

Wildes RP, Asmuth JC, Hanna KJ, Hsu SC, Kolczynski RJ, Matey JR, McBride SE. *Automated, non-invasive iris recognition system and method*, U.S. Patent No. 5,572,596 issued November 5 1996

¹³² Boles WW & Boashash B. *A human identification technique using images of the iris and wavelet transform*, IEEE Trans. Signal Processing, 46(4) Apr 1998, 1185-1198

¹³³ Zhu Y, Tan T & Wang Y. *Biometric Personal Identification Based on Iris Patterns*, ICPR2000, Vol II 805-808

¹³⁴ Lim S, Lee K, Byeon O & Kim T. *Effective Iris Recognition System by Optimised Feature Vectors and Classifier* in 6th Pacific Rim International Conference on Artificial Intelligence (PRICAI2000) eds Mizoguchi R & Slaney JK, Springer Lecture Notes in Computer Science, vol 1886, 167-176

¹³⁵ Muron A, Kois P & Pospisil J. *Identification of persons by means of the Fourier spectra of the optical transmission binary models of the human irises*, Optics Communications, 192 (3-6) 2001, 161-167

¹³⁶ Tisse C, Martin L, Torres L, Robert M. *Person identification technique using human iris recognition*, 15th International Conference on Vision Interface, Calgary, Canada, May 2002

¹³⁷ Noh S-I, Pae K, Lee C & Kim J. *Multiresolution Independent Component Analysis for Iris Identification*, International Technical Conference on Circuits, Systems, Computers and Communications, Phuket, Thailand, July 2002

4.3.3 High Profile deployments

Netherlands – Amsterdam Schiphol airport – PRIVIUM system

Launched in October 2001, the PRIVIUM system allows subscribers to clear immigration members using iris recognition and smart card as proof of identity. The scheme is open to all European Economic Area passport holders and basic subscription costs €99. There is no central database—the iriscodes for both eyes are stored on the smart card. The system uses the LG IrisAccess 2200 equipment, and currently has around 4000 members.

Pakistan – UNHCR – Repatriation programme for Afghan refugees

In Pakistan, the United Nations High Commissioner for Refugees (UNHCR) is using iris recognition to help stem fraud whereby some refugees returning to Afghanistan were doubling back across the border to claim repatriation allowances multiple times. Their system uses the LG IrisAccess 2200 equipment, and has over 22000 enrolments.

United Arab Emirates – Expellee tracking and border control system

Commencing in 2003, for travellers arriving at air, sea and land ports, a 1:many check is made against a database of irises of previous expellees. The database contains some 83 500 people (by May 2003).

Canada – Canadian Customs and Revenue Agency (CCRA) – CANPASS-Air

Pre-approved travellers will be able to clear immigration using iris recognition as proof of identity. The scheme is to be open to US and Canadian citizens and permanent residents, and costs \$CAN 50. The rollout commenced in March 2003 at Vancouver International Airport.

Pilots

UK – Nationwide Building Society

One of the earliest public tests of iris recognition was in 1998, when the Nationwide Building Society ran a trial using Sensar iris recognition equipment in an NCR automated teller machine outside their offices in Swindon. Public response was very positive, though the rollout of such ATMs over the banking network would not have been economic. Similar trials were subsequently run at several other banks in other countries, e.g. Dresdner Bank in Frankfurt; Bank United in Houston.

Netherlands – BZK and TOV – Rotterdam e-reporting pilot project

A small-scale trial was run by the alien police in Rotterdam, using an iris recognition system for registration and reporting of aliens.

Saudi Arabia

In 2002, Saudi Arabia's Ministry of the Interior ran an evaluation of iris recognition for tracking Hajj pilgrims. Some 20,000 selected pilgrims were enrolled over a two week period.

UK – Heathrow

A six-month trial of the use of iris recognition for expedited processing of arrivals through immigration.

Japan – Narita – E-Airport

A three-month trial running January to March 2003, allowing Japan Airlines frequent flyers to register iris and face images for subsequent expedited check-in. The trial used BEM-ET500 equipment.

4.3.4 Testing and issues of performance limitation

Existing studies show that iris recognition should be accurate enough for an identification search in large databases. One problem with the technology however is that there are no existing (sequestered) databases of a size commensurate with the performance capabilities of the technology. This prevents a third party evaluation of the extent of the performance capabilities of the technology. (Fingerprint technology, by contrast, can be tested on very large legacy databases from criminal justice systems.) The evaluations of the technology that have been publicly reported are all of systems using the Iridian algorithms.

Mansfield, et al. 2001 – Biometric product testing final report

An evaluation of the IrisAccess 2200 system in a scenario of access control in an office environment. Available on the CESG website www.cesg.gov.uk.

Cambier, J. 2002 – Iridian cross-comparison test.

A technology evaluation using a large database of iris codes collected from several different applications, allowing 1 billion different iris comparisons. Available from Iridian Technologies website www.iridiantech.com

DoD ARL 2002

Results of the Department of Defense / Army Research Lab scenario evaluation were reported at the Biometrics Consortium Conference in February 2002.

Sandia 1996

In 1996 Sandia evaluated a prototype system. Their report is available at http://infoserve.sandia.gov/sand_doc/1996/961033.pdf

4.3.5 User concerns

Safety

Occasionally people express concerns about the safety of iris recognition. In part this concern stems from a misconception on how the system operates, and an assumption that the iris is “scanned” by laser. In fact the iris is imaged by a normal camera, though additional illumination may be provided through use of near infrared LEDs. Analysis of illumination levels for the Iridian based systems shows that, even under worst-case assumptions, these are still significantly lower than the maximum permitted levels of the relevant standards.

Inclusivity

As with any biometric, there will be groups of people unable to use the system, or having additional difficulties in using the system. One obvious case is due to the rare condition known called aniridia, where eyes have no iris. Further cases are blind people who, depending on the type of system, may find it very difficult to aligning their eyes with the camera; and those with nystagmus (tremor of the eyes). Systems mounted at normal eye-height may be impossible to use by people in wheelchairs. In order to get the best possible enrolment, people may have to remove hard contact lenses (if worn) when enrolling.

4.3.6 Legal and regulatory dimensions

No specific regulations appear to limit the use of this technology.

4.3.7 Standardisation activities

An Iris image interchange format is in the processes of being standardised in ISO/IEC JTC1/SC37.

4.3.8 Principal research projects

Iris recognition vendors are known to be working to improve “liveness” testing within their devices. Work is also underway investigating the possibilities for iris recognition based on images taken at greater distances than at present, i.e. 2-3 metres as opposed to 20-30 centimetres.

4.3.9 Outlook for the future

As larger-scale applications come about, larger databases will become available for performance evaluation.

Improvements in image acquisition are likely, making it easier for people to use the system, e.g. removing the need for alignment with the system, and for acquiring usable iris images with poorer illumination, at greater distances, and from moving targets

4.4 Retinal Scanning

Retinal scanning is the other eye biometric. Developed in the 1980's, it was the first of the highly automated, high accuracy systems and as such became a favourite of Hollywood films. Even now, many years after it has been eclipsed by iris recognition, security specialists and journalists still confuse the two technologists.

4.4.1 Principal methods

One supplier, EyeDentify, commercialised the technique in the 1980's. The user was asked to fixate on an alignment mark and a low intensity infrared light swept in a circle centred at the fovea, the area of sharpest vision in the eye. 320 measurements of the reflectivity of the retina were taken during this sweep, identifying the presence of blood vessels when this reflectivity changes. These results are then converted into a small template, typically from 72-96 bytes.

4.4.2 Principal commercially available systems

Currently, the sole supplier of equipment does not appear to be actively marketing devices or software. A system appears to be available for the identification of animals using retinal scanning.

4.4.3 High Profile deployments

Many of the systems were deployed in areas subject to high security, such as banks, prisons and military areas.

4.4.4 Testing and issues of performance limitation

The EyeDentify Information Security system was evaluated in 1989 by the National Computer Security Center (part of the NSA at that time) under the TCSEC scheme for

assessment of the security of Information and Authentication subsystems (a predecessor of the Common Criteria), meeting the requirements for class D1¹³⁸.

4.4.5 User concerns

The early commercial implementations of this technology were difficult to use by untrained personnel. When added to fears about the safety of the equipment, this meant that operators were unwilling to consider its use other than in very high security environments, or in closed communities of users, such as prisons or military establishments. A comment in an internal test report by a reseller summarises this succinctly: 'Not tested because employees are afraid of this device'. Various reports on the health aspects of the operation of retinal scanning were commissioned by EyeDentify.

4.4.6 Legal and regulatory dimensions

No legal limitations are recorded.

4.4.7 Standardisation activities

There are no known activities in this area.

4.4.8 Principal research projects

No major projects are underway.

4.4.9 Outlook for the future

The installed base of equipment, together with its acknowledged high performance, should guarantee a continuing interest in this method. Rumours of new entrants to the retinal scanning market continue to surface from time to time. Nevertheless, any new version will face stiff competition from the more established iris recognition technique.

4.5 Hand geometry

This biometric is one of the more mature approaches to human identification and has proved particularly useful in both physical access control and in cross border verification. US patents were issued as early as 1971, but the current limited range of devices goes back to 1986 and the granting of a patent to David Sidlauskas in 1988¹³⁹. The company he founded in 1986, Recognition Systems, appears to have maintained a similar core technology since its initial range of products. Its proprietary and undisclosed algorithm produces a template of 9 bytes for the pseudo three-dimensional representation of a hand, which is normally 'averaged' or updated once a confirmed authentication deviates by a predefined margin beyond acceptable limits¹⁴⁰. This *Handkey* device is quite bulky since the whole hand is placed on a reflective platen and located through butting four location pillars into the skin surface between the base of fingers and thumb. A smaller unit has been subsequently introduced by BioMet Partners - the Digi-2 - which only required the placement of two fingers on a plate with a single vertical locating pillar.

¹³⁸ NCSC, *Final Evaluation Report EyeDentify, Inc EIS System*, CSC-EPL-90/006 (24 September 1990)

¹³⁹ David Sidlauskas, *3D hand profile identification apparatus*, US Patent 4736203 (5 April 1988)

¹⁴⁰ Richard Zunkel, *Hand geometry based verification*, Chapter 4 in Anil Jain *et al*, *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers (1999). This method uses two 2-dimensional shadows of the fingers taken at right angles.

4.5.1 Principal methods

The Recognition Systems unit operates on silhouettes of the plan view of the hand obscuring the reflection of light from a highly polished aluminium surface, together with a side view obtained by reflections off a side mirror. 96 measurements of the gross hand features are taken and reduced to the 9 byte template. For optimum performance, users should be trained to locate the hand by firstly touching the platen with forefinger and middle fingers, and then gliding it to mate with the vertical pillars at the base of the fingers. The system is designed to be used with the right hand face down, although operation is also possible with the left hand positioned palm upwards.

Less information is available about the design and optimal operation of the Digi-2, although it is public knowledge that major system redesign was required to ensure reproducible performance at the major reference installation at Walt Disney World.

4.5.2 Principal commercially available systems

Although there have been numerous studies of alternative hand geometry systems, the market consists almost exclusively of two units, as described above. The majority of installed units are those of the Recognition Systems' *Handkey* in its various versions - although it is understood that the core technology remains substantially unchanged from the initial units. Currently, more than 70,000 units are installed. Although networking of units is offered, many installations are standalone physical access control systems with the templates of persons permitted access to a room or building stored in the reader, and accessed through a PIN issued to each user (although it should be noted that in general, knowledge of the PIN is not a secret).

4.5.3 High Profile deployments

The *Handkey* formed the basis of many of the initial INSPASS deployments at US and Canadian airports in the 1990's, to ensure fast and automatic verification of identities at immigration control. Initial experience with the product demonstrated that even though it had performed well in laboratory tests at Sandia Laboratories, further work was needed to meet the operational performance required for 'trusted traveller' application. For a variety of reasons, the numbers of airports at which this service was offered and the user population stabilised several years ago (50,000 frequent travellers enrolled and monthly use by an average of 23,000 people¹⁴¹). With the introduction of the US-VISIT system, the future of INSPASS remains unclear. A similar system is in use for 100,000 Israeli citizens returning through Ben Gurion airport in Tel Aviv, and a combined biometric is due to be introduced for Arab workers crossing into Israel.

4.5.4 Testing and issues of performance limitation

The sales of hand geometry equipment were given a substantial boost by the very favourable results of the 1989-91 evaluation of its performance by Sandia National Laboratories (as one of six biometric methods tested on 100 volunteers)¹⁴². The one try EER for the ID3D-U unit tested at 0.2 %, with 0.1% FRR attainable at a different threshold when three tries were allowed. A study conducted several years later by the same laboratory under real operational conditions (units sited outside buildings) showed considerably higher failure rates that required sophisticated optimisation techniques to ensure correct operation. Direct sunlight affected the performance adversely, and dust and sand was also found to be detrimental.

¹⁴¹ Testimony by Martin Huddart before Senate subcommittee on technology, terrorism and government information, www.iwar.org.uk/comsec/resources/senate-biometrics/te111401st-huddart.htm (14 November 2001)

¹⁴² James Holmes *et al*, *A performance evaluation of biometric identification devices*, Sandia report SAND91-0276 (June 1991)

In the CESG/BWG testing programme of 2000, a Recognition Systems HandKey II was tested in a 'normal office environment' scenario. No failures to enrol or acquire were noted in the generally young group of technically oriented subjects. Equal error rate performance under these somewhat idealised conditions was ascertained to be just over 1% with a substantial improvement if the users were allowed the conventional three tries. The IBG conducted a test on the system in December 2002 as part of its fourth round of comparative testing.

4.5.5 User concerns

The same Sandia tests showed that hand geometry was favoured by users, possibly because of their frustration in the poor performance of some other systems on trial. Over a third of the respondents felt that this unit was the most friendly and fun to use, requiring least proficiency in use.

4.5.6 Legal and regulatory dimensions

There appear to be no additional constraints on hand geometry in the legal systems studied in this work.

4.5.7 Standardisation activities

None commenced at present.

4.5.8 Principal research projects

Hand geometry has been deployed extensively in physical access control systems and there continues to be interest in linking this approach with other methods of authentication, such as palmprints¹⁴³. Some research continues in developing alternatives to the existing proprietary algorithms.

4.5.9 Outlook for the future

Hand geometry addresses the needs of a clear niche in the marketplace - access control and time and attendance where the ultimate in security is not a critical factor. As a well-established and well-characterised system, it is likely to continue to serve this marketplace, although other methods using cheaper and more compact hardware (e.g. those using fingerprints) are likely to draw customers away from this sector. Issues of security, robustness and user acceptance will determine the extent of this migration.

4.6 Vein Pattern

Towards the end of the 1980's, Joe Rice noted the prominence of veins on the back of peoples' hands and surmised that there would be sufficient variation between individuals to offer this as a biometric method of authentication. Subsequent work by the holders of the Veincheck licence, the UK's BTG, demonstrated the feasibility of robust template formation and the practicality of its use. Imaging of the pattern was aided by the use of infra-red illumination. The non-invasive nature of the biometric encouraged prediction of its more extensive use, and although the system development has been completed, no commercialised product is currently available. In the CESG/BWG 'normal office environment' tests carried out in 2000, a development prototype of the Veincheck failed to perform very well.

¹⁴³ Ajar Kumar *et al*, *Personal verification using palmprint and hand geometry biometric*

Recently, an alternative system based upon so-called Vascular Pattern Recognition has been commercialised by TechSphere¹⁴⁴ of South Korea and distributed by Identica Corporation of Canada. Relatively few details of the core technology are available on the company's website but the VP-II system is claimed to be usable by 99.98% of the population. Patterns are captured by an infra-red optical system with a temperature sensor providing a measure of security against spoofing. Fujitsu have also introduced a system based upon vascular features.

Research continues on this method¹⁴⁵.

4.7 Speaker Verification

The distinctiveness of people's voices is due to both physiological and behavioural differences in speech production. The physiological differences are due to the differences in the shape of the vocal tract. Behavioural differences are due to speaking style, and include aspects such as accents and language. The behavioural element means that even identical twins will have some differences in their voices.

4.7.1 Principal methods

Speaker verification systems fall into two classes depending on whether the recognition is text dependent or text independent.

Text dependent

Text dependent systems know in advance what the speaker is supposed to say. Typically the person will speak a short 'passphrase' that will then be compared against a model or template based on that person's utterance of the same words during enrolment. Sometimes there is a single, fixed passphrase – this raises the possibility of an attack using a recording. To overcome this problem, the system may enrol the person using multiple words or phrases, perhaps the digits "0" to "9". Then the person can be asked to speak a random selection of these. This challenge-response method makes it much harder to attack a system using recordings.

Explicit knowledge of the words being used means that the systems can be fairly accurate at recognition on fairly short amount of speech, *provided the speaker is being cooperative*.

Text-dependent speaker verification is generally used for "positive" 1-to-1 verification applications.

Text independent

Text independent systems, do not know beforehand what the speaker will say. Generally such systems will have to make use of whatever speech is available for both enrolment and verification. To get a reasonable performance, the systems require a far greater amount of speech. Such systems are more robust for recognising uncooperative speakers. Text independent speaker verification is more likely to be used for forensic or covert applications.

4.7.2 Commercially available products

¹⁴⁴ <http://www.tech-sphere.com/english/home.htm>

¹⁴⁵ AISAT Research, *Thermographic imaging of vein pattern in the back of the hand*, www.cowan.edu.au/fste/aisat/research.htm

There are a variety of commercially available speaker verification products, ranging from the basic speaker verification SDK, through products targeted at particular applications, to services allowing the speaker verification task to be outsourced. Often products are integrated with speech recognition.

SDKs and 'Engines'

Examples:

- Nuance Verifier
- SpeechWorks' SpeechSecure
- VeriVoice SL
- Anovea SVLib

Application specific products

Examples:

- SpeakNSet – (a password reset application)
- OTG's SecurPBX (protection for voicemail, long-distance trunk calls, etc)
- OTG's Help Yourself (automated PKI profile administration and recovery)
- Vocent Password Reset
- Vocent Confirmed Caller

Services

Examples:

- Buytel (now Voicevault)

4.7.3 Deployments

There are many deployments of speaker verification systems. Some of the major types of application are listed below. Most applications are telephone-based – this is an obvious niche for speaker verification biometrics.

Password reset

A large proportion of calls to IT helpdesks involve password reset. There are now a number of automated password reset products on the market that use speaker verification to help ensure that only the account owner can reset their password. Such systems can be more secure than relying on the IT helpdesk staff to correctly identify the caller, and also can offer a considerable cost saving.

Automated parolee monitoring/curfew systems

Speaker verification systems are also being used for monitoring parolees, to ensure that they attend rehabilitation, obey curfew orders, etc. Such systems may call the parolee at the location where they are supposed to be, and ask them to repeat phrases to allow verification. Alternatively the parolee may have to call in from a particular phone line at a certain time, and their presence at the appropriate location is checked using calling line ID, and speaker verification.

Example: In the UK, this has been deployed in the Youth Justice Board's Intensive Supervision and Surveillance Programme for house arrest and curfew enforcement. A similar system has been deployed in the USA under the ShadowTrack name.

Telephone shopping

Instead of having to remember a PIN to authorise expenditure on their accounts, customer authentication can be based on speaker verification.

Examples of the method are:

- In the USA, the Home Shopping Network deployed speaker verification in 1999 to identify and authenticate frequent shoppers.
- In Australia – Optus – Trial (commencing 2002) of voice verification to authorise payments to top-up their mobile phones.

Customer Call Centres

Speaker verification can be used instead of PIN and/or operators asking personal questions to authenticate the caller.

Examples of this application are:

- In UK – Nationwide Building Society (Trial)
- In Brazil – Banco Bradesco – Telephone banking

Staff access

Example of this use is in Canada – Bell Canada – Speech Enabled Field Access System

4.7.4 Testing and Performance

NIST runs a regular programme of technology evaluations for speaker verification systems. Some results are reported¹⁴⁶ but these do not include performance of commercially available systems. Additionally a number of scenario evaluations have been conducted as listed in the following table.

Vendor	System	Test
Alpha Microsystems	Ver-A-Tel	Sandia 1991 ¹⁴⁷
ECCO	VoiceKey	
Voice Strategies	VACS	Sandia 1993 ¹⁴⁸
Enigma		
Nuance	v7.0.4	CCIR 2001 ¹⁴⁹
	v6.2.4	CCIR 2000 ¹⁵⁰
OTG / T-Netix	SecurPBX SpeakEZ v1	NPL/BWG/CESG 2000 ¹⁵¹
Texas Instruments		Mitre 1977 ¹⁵²

¹⁴⁶ G. R. Doddington *et al*, *The NIST Speaker Recognition Evaluation – Overview, Methodology, Results, Perspective* See also <http://www.nist.gov/speech/publications/index.htm>, <http://www.nist.gov/speech/tests/spk/index.htm>

¹⁴⁷ J.P. Holmes *et al*, *A performance evaluation of biometric identification devices*. Sandia Report SAND91-0276, June 1991. http://infoserve.sandia.gov/sand_doc/1991/910276.pdf

¹⁴⁸ J. R Rodriguez I *et al*, *A performance evaluation of Biometric Identification Devices*, Sandia report SAND93-1930

¹⁴⁹ *Evaluation of Nuance v7.0.4 Speaker Verification Performance on the Dialogues Spotlight UK English Database*, Dialogues Spotlight Technology Report, CCIR, 2001
http://spotlight.ccir.ed.ac.uk/public_documents/technology_reports/verifier_report_V7.pdf

¹⁵⁰ *Large Scale Evaluation of Automatic Speaker Verification Technology*, Dialogues Spotlight Technology Report, CCIR, May 2000
http://spotlight.ccir.ed.ac.uk/public_documents/technology_reports/Verifier_report.pdf

¹⁵¹ A J Mansfield *et al*, *Biometric Product Testing Final Report*
http://www.cesg.gov.uk/technology/biometrics/media/Biometric_Test_Report_pt1.pdf

¹⁵² A Fejfar and J W Myers, *The testing of three automatic identity verification techniques*. Proc. International Conference on Crime Countermeasures, Oxford, July, 1977

4.7.5 Standardisation

Work on SVAPI (Speaker Verification Application Programmers Interface) predated the work on BioAPI. However speaker verification community seems to be underrepresented on SC37 Biometric Standards. For example, as yet there are no proposals for a biometric speech data interchange format.

4.7.6 Research projects

In the UK, PUMA, a DTI-sponsored project using speaker verification, aims to develop an innovative approach to fraud prevention and improved human-machine interaction through adaptive personalisation of the human-machine interface in mobile communication devices such as cellphones and PDAs¹⁵³. In a project aimed to finish in 2005, the COST 275 consortium is using both speaker verification and facial recognition to authenticate consumers over the Internet¹⁵⁴.

4.7.7 Outlook for the future

One of the current problems for speaker verification, that of coping with low quality microphone types, and noise on the telephone link may be much alleviated as the technology in these areas improves.

Current systems do not make use of individual's phraseology, style, the idioms they use and other speech data that humans use in the recognition task. The use of such information could lead to improvements in text independent speaker recognition. Currently there seems to be little work in developing standards for interchange of biometric speech data.

4.8 Dynamic signature verification/recognition (DSV/DSR)

Writing is typically a multidimensional phenomenon. It is, on the one hand, a dynamic phenomenon, involving psychological, neuro-psychological, and motor dimensions. On the other hand, it is a physical phenomenon, not only with the artistic, symbolic and graphological dimension.

Capture of the writing dynamics enables the determination of characteristic time functions from which more dynamic features - like the duration of writing or the average writing speed - can be determined. It offers the opportunity to determine the specific writing frequency for a particular person through the transformation of the writing signal.

From the point of view of forensic handwriting comparison, the key to the verification of the authenticity of questionable signatures lies in the reconstruction of the writing motion and its elements. The difference between genuine and copied signatures is based on the amount of pressure applied and on the structure of the writing line. Furthermore, the determination must reflect the observation that signatures from the same person may show different writing speeds.

Dynamic signature recognition systems can either work in verification or identification mode. Recognising signatures is the comparison of a typical behaviour. The identification of two dynamic signatures can be directly traced back to the signals of the captured motion.

4.8.1 Principal methods

¹⁵³ <http://www.dti-mi.org.uk/newweb/puma.htm>

¹⁵⁴ <http://www.fub.it/cost275>

A wide range of equipment is available for digitising signatures: pen pads (both with and without display) and special pens. Recording devices are distinguished by the type and number of sensors used, e.g. acceleration sensors, power sensors or a combination of the two. Additional distinguishing features are the number and resolution of recordable writing signals. An interesting alternative was developed to prototype level by Rolls Royce in the UK, using the acoustic emissions generated when a pen moves across a surface. Uniquely, in this case, the spatial form of the written signature is not captured.

The quality of data captured from these input devices varies widely, and as of the present time, there is no standardisation for hardware devices. It is likely that a larger organisation will use a number of different input devices such as a mixture of tablets (also called "pads"), tablets with a display, Tablet PCs and Personal Digital Assistants (PDA). Specially designed pens had not been commercialised to a great extent as of early 2003.

Usually the signer relies on optical feedback of his writing results on paper. If the input device does offer a display, it has to deliver an exact optical feedback throughout the writing process. Should users realise that their signature varies from the usual result on paper, usually they will alter the way of writing in response. A secure and unambiguous communication between capturing device and processing unit is also necessary. When using a pad or tablet without a display, it is important to keep in mind that first-time users may experience some difficulty when writing on a clean surface while at the same time viewing the captured signature on a nearby monitor. To avoid this problem some suppliers offer the option to use paper and write with a normal pen or a special inking pen.

In general, any signature recognition method aims to authenticate the signature data sample as the genuine version from a specific person. Biometric data can be classified according to the type of features that are used: parameter-based or function-based signature verification. Besides the verification technique, reference construction plays an important role, as it directly influences the verification performance. However, we note that methods for reference construction are rarely discussed in the scientific literature.

4.8.2 Principal commercially available systems

Verification Software Vendors for DSV / DSR

Name	City	Country	Website
CIC	Redwood Shores	USA	www.cic.com
Cybersign	Tokyo	Japan	www.cybersign.jp.com
Softpro	Boeblingen	Germany	www.softpro.de
SQN	Ranconcoas	USA	www.sqnsigs.com
Wondernet	Kibbutz Givat Hashlosa	Israel	www.penflow.com

Capture devices for DSV /DSR - Tablet Manufacturers

Name	City	Country	Website
Acecad	Taipei	Taiwan	www.acecad.com
Interlink Electronics	Camarillo	USA	www.interlinkelectronics.com
MotionTouch Ltd	Surrey	UK	www.motiontouch.com
Topaz Systems	Simi Valley	USA	www.topazsystems.com
UC Logic	Taipei	Taiwan	www.superpen.com
Wacom	Saitama	Japan	www.wacom.co.jp

Capture devices for DSV / DSR - Tablet PC Manufacturers

Name	City	Country	Website
Acer Incorporated	Taipei	Taiwan	www.acer.com

Aopen	Taipei	Taiwan	www.aopen.com
Aplux	Taipei	Taiwan	www.aplux.com
First International	Taipei	Taiwan	www.fic.com.tw
Fujitsu Siemens	Bad Homburg	Germany	www.fujitsu-siemens.com
HP Compaq	Houston	USA	www.hp.com
Motion Computing	Austin	USA	www.motioncomputing.com
NEC	Tokyo	Japan	www.nec.com
PaceBlade Technology	Wanchai	Hong Kong	www.paceblade.com
Sotec	Tokyo	Japan	www.sotec.co.jp
Tatung	Taipei	Taiwan	www.tatung.com
Time Group Ltd.	Lancashire	UK	www.timeeducation.com
Toshiba CSG	Irvine	USA	www.toshiba.com
VIA Technologies	Taipei	Taiwan	www.via.com.tw
ViewSonic	Walnut	USA	www.viewsonic.com
WalkAbout Computers	W. Palm Beach	USA	www.walkabout-comp.com
Wistron Corporation	Taipei	Taiwan	www.wistron.com

Other capturing systems are based on measuring pressure and angles of tilt using a special pen. Vendors like ICA Vertrieb (Stuttgart / Germany)¹⁵⁵ or GouLite (Israel) are offering such devices. Other companies, such as LCI SmartPen (Belgium)¹⁵⁶ and PDI Systems (Germany), seemed to have exited the market since 2000/01, as their websites are no longer operational.

4.8.3 High Profile deployments of DSV / DSR systems

At the time of compilation of this section (January 2003), we were aware of the following high profile European projects:

- Nationwide Building society in the UK announced a roll-out for its customers, using hardware provided by MotionTouch and software supplied by CIC and Florentis
- Mercedes AMG (Daimler Chrysler) are deploying a product liability process with hardware provided by Interlink and software developed by SOFTPRO.

4.8.4 Testing and issues of performance limitation

Dynamic signature recognition addresses the problem of recognising signatures from data captured with a sensitive pad that provides discrete pen trajectory information. In contrast with other pattern recognition techniques, such as speech recognition and optical character recognition, there has been no significant progress over the past few years in making publicly available large corpora of DSV/ DSR training and test data, and no open competitions have been organised. An independent dynamic signature technology benchmark - comparable to the fingerprint verification competition FVC¹⁵⁷ at the University of Bologna - is still awaited and a review of the technical literature on signature verification testing reveals a wide variety of conflicting and contradictory testing protocols.

¹⁵⁵ Website of ICA Vertrieb: www.ica-vertrieb.de/main1081350.htm

¹⁵⁶ GMD: *Usability of Biometrics in Relation to Electronic Signatures EU Study 502533/8* (Version 1.0 September 12, 2000 GMD, p.65)

www.sit.fhg.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf

¹⁵⁷ <http://bias.csr.unibo.it/fvc2002> The aim of the FVC initiative is to encourage the construction of a common basis for research and evaluation of state-of-the-art fingerprint-based biometrics for both industry and academia.

4.8.5 User concerns

It is a centuries old tradition for important documents to be signed as proof of their authenticity. An increasing number of documents are produced and processed electronically in order to accelerate business processes and to reduce the costs of handling through substitution of paper. However, it is important not to minimize the media cuts. Today several substitutes are used which are not very appropriate – for instance an image of the signature is scanned and copied into a document. This is a contradiction to the original aim, as signatures should guarantee the authenticity and integrity of a document, not be capable of undergoing a *cut and paste* procedure.

DSV / DSR approaches capture the shape of a signature as well as the non-visible characteristics of the movement of the hand, so as to allow for a later comparison. The information about the signature is stored in an encrypted form, alongside the document. Optionally, it is possible to integrate these with various forms of electronic signatures. In this case, should the content of the document be changed by an unauthorized person, the display of the signature will automatically indicate that the current status of the document is not authorized. Another option is to protect a document against unauthorised access using signature recognition as an alternative to the common protection of a document by means of a password.

4.8.6 Legal and regulatory dimensions

One could argue that DSV/DSR can be associated with a declaration of intent of the signatories in legal transactions. Traditionally, the act of signing with a conventional written signature offers a (legally binding) declaration, leading to a parallel conclusion for electronically submitted signatures. Also the cultural meaning, and commonly approved acknowledgement of, the handwritten signature should lead to a greater acceptance by end users. In addition, DSV/DSR can be used in the context of digital signatures which themselves are regulated according the EU directive on digital signatures and the respective national implementations in member states.

It is unclear whether, in the absence of strict safeguards against replay and reuse in other applications, the legal admissibility of evidence from DSV/DSR systems may be questioned.

4.8.7 Standardisation activities relevant to DSV / DSR

A typical dynamic signature recognition module includes the classical pattern recognition components of signature data capture, processing, transmission, storage, and authentication. At the system level in real applications, signature recognition techniques may be integrated with other technologies to form a complete solution. All these devices could inter-operate for maximum flexibility. BioAPI standardisation addresses this issue. This protocol offers standardised interfaces to existing dynamic signature recognition technology and thus facilitates interoperability and interchangeability of the technologies.

Another issue is determining the data format for interoperability when the data is required to be shared between multiple systems using signature recognition technologies. Until now, interoperability between different dynamic signature recognisers has not been possible.

Test databases and testing procedures are not available for dynamic signature recognition technology. A standard database and a standard testing procedure will provide users with a comprehensive understanding of a dynamic signature system, and guide users to the right choice.

A working draft for an ISO standard for signs and signatures has been tabled (WD for 19794-7, if approved in the future).

4.8.8 Principal research projects developing DSV / DSR systems

There is only one European research project for signature recognition systems at the time of compilation of this report:

ZAVIR is a project within the focus "IT security" of the programme "Living and working in a networked world" funded by the German Federal Ministry of Education and Research. One aspect of this work deals with on-card matching algorithm for dynamic signatures.

4.8.9 Outlook for the future

Increasing interest for the application- and solution-oriented integration of dynamic signature recognition systems into existing services is evidenced by the growing number of applications that are being addressed.

At present, many organisations are satisfied when they have captured an image of a signature to add it to a document. They are unaware that such an image may be copied and used without authorisation in other documents. Often such companies would be surprised and concerned to learn that the data captured could not be used for authenticating people, and that they will need to authenticate their signatories separately. We believe that there has to be a significant rise in the awareness that there are more characteristics of a signature than those that are just visible.

These solution-oriented views (including the application of smart cards, standardisation and certification) are laying the foundations for widespread market success by encouraging the standardisation of integration capabilities and verifiable quality.

RC/TTL4 RC - TRIALS, TESTING, LEGAL etc 4: A programme of database construction and testing should be initiated especially for those biometric methods for which such large scale databases are still not collected or publicly available. Certain biometric methods (e.g. multimodal biometrics) will require specific algorithm testing schemes and research may be required to devise the most appropriate methods.

4.9 Keystroke Dynamics

Recipients of Morse Code messages in the Second World War noted that certain individuals showed individual patterns of keying. This observation led some researchers in the late 1970's to consider whether the same effect could be replicated on computer keyboards. As the volume of electronically entered information started to increase, the attraction of discovering the extent to which such regularities could form the basis of a behavioural biometric resulted in a number of research papers and one commercial product.

4.9.1 Principal methods

Gaines and his colleagues at the Rand Corporation demonstrated the potential of Keyboard Dynamics (KD) in 1980 by measuring the keystroke latency intervals between adjacent letters in text typed by seven professional secretaries. This required the

collection of a rather large set of input data¹⁵⁸. A 1986 patent suggested that typing your own name would lead to more stable performance and better user acceptability. Alternatively, users could be asked to type out the 1000 most common words in the English language to provide a solid base for subsequent analysis. Subsequent systems have emphasised the text-dependent and text-independent approaches to various degrees, with some attempts to advocate specialised keyboards that also recorded the pressure directed to letters.

4.9.2 Principal commercially available systems

The main supplier of keystroke dynamic software has been through a number of takeovers, the latest being the acquisition by BioNet Systems of the latest versions of the BioPassword product (version 4.5). Prices for licenses during its previous ownership by Net Nanny ranged from \$40-100 per seat depending on the size of the deployment.

4.9.3 High Profile deployments

There have been no large scale deployments.

4.9.4 Testing and issues of performance limitation

Most research papers show results obtained by sub-100 size samples. For example, a 1992 study at the Naval Postgraduate School carried out under relatively uncontrolled conditions demonstrated performance of a commercially available BioPassword Model 2100 using 24 Chinese male officers. High variability in performance was noted between individual users, with a high average of false rejects at the first attempt (4.4%), for a false acceptance rate of 3-4%¹⁵⁹. The suppliers of the commercial software note that a test was undertaken in 2000 by the Financial Services Technology Consortium and the International Biometric Group, but no further information is available.

4.9.5 User concerns

No known assessments.

4.9.6 Legal and regulatory dimensions

Use of keystroke dynamics could be associated with keystroke monitoring programmes whose use could be limited by privacy laws and local codes of conduct.

4.9.7 Standardisation activities

There are no standardisation activities at present

4.9.8 Principal research projects

Keystroke Dynamics continues to offer a major research challenge. The absence of hardware costs allows many universities to set this technique as a research topic for students who are unaware of the considerable difficulties that attend this method and its successful implementation. A slow, but steady, flow of papers reaches the technical

¹⁵⁸ Material on the early years of KD is based upon a paper reviewing the field: Rick Joyce and Gobal Gupta, *Identity authentication based on keystroke latencies* Coomunications of the ACM **33** (2) 168-76 (February 1990)

¹⁵⁹ Hung-I Kuan, *Evaluation of a biometric keystroke typing dynamics computer security system*, Naval Postgraduate School (March 1992)

journals. The FernUniversität Hagen in Germany is interested in the technology¹⁶⁰. Small scale studies of applying neural network based KD to PIN entry have been carried out by the UK's University of Plymouth's Network Research Group, as part of a programme to secure access to mobile devices. 6 digit PINs on a subject group of 14 persons showed a FRR of 30% and FAR of 10%¹⁶¹. Recently, Fabian Monrose and colleagues at Bell Labs have suggested the use of adaptive *hardened passwords* that recode the password based upon attaining of the correct time differences between sets of letters in a typed password by the authorised user¹⁶². Test results carried out on 20 users (1 password and 481 logins) appeared promising. Bergadano and colleagues at Turin University have demonstrated considerable improvement in text-dependant (683 characters), fault tolerant typing dynamics¹⁶³. Their testing of 154 subjects with varying keyboard skills showed a FRR of 4% against FAR of less than 0.01%. Such long texts are not a replacement for password authentication, but extending these techniques to large amounts of freely chosen text could result in improved performance of such systems.

4.9.9 Outlook for the future

In spite of the confident forecasts of many over the past two decades, the QWERTY keyboard has resisted all attempts at displacement by speaker recognition software. By 2010, we anticipate that there will still be many keyboards, although the growth of smarter, embedded intelligence at home, work and leisure, and improvements in the performance of speech recognition, should reduce the proportion of computing terminals that use typed text entry. Unfortunately, current research is unable to guarantee that the performance of KD will improve substantially beyond its current levels, in spite of several interesting recent results. The use of this biometric is, therefore, likely to remain confined to specific niche areas.

4.10 Other biometric methods under development

Many other human characteristics have been proposed over the past three decades, and work continues at generally low levels of commitment. An optimistic assessment of the timescales includes:

- preparation of the research project for funding support and recruitment of the researcher: 2 years;
- the three year average duration of a research project in a university (geared to the duration of PhD programmes);
- either securing of first round venture capital funding or agreement on joint development with an existing corporate laboratory: 1-2 years;
- demonstration of commercial feasibility: 2-3 years;
- testing and refinement of the biometric: 1-2 years.

Such an analysis demonstrated that there will be no novel biometric introduced commercially within the timeframe of this roadmap. However, work is already underway in a number of the following technologies, and the timescales for these should be correspondingly adjusted.

¹⁶⁰ cs.fernuni-hagen.de/researchAreas/cryptography/main_Computer_User.html

¹⁶¹ T Ford and S Furnell, *User Authentication for keypad-based devices using keystroke analysis*,

¹⁶² Fabian Monrose *et al*, *Password hardening based on keystroke dynamics*, International Journal on Information Security, in press

¹⁶³ Francesco Bergadano *et al*, *User authentication through keystroke dynamics*, ACM Transactions in Information and System Security, 5(4) pp 367-397 (November 2002)

DNA recognition¹⁶⁴

A high resolution DNA profile arguably offers the most definitive form of human identification. A match probability derived from a DNA profile can now approach a frequency of one individual in the entire population of the planet and statistical estimations of individual profile frequencies are well supported by population studies. DNA is present in all the body's tissues and is routinely shed in sweat, saliva, skin cells and hair, etc and provides a pervasive trace source for use individual identification. Unfortunately DNA extraction and amplification - the processes used to derive DNA profiles from biological samples - are time consuming and expensive. According to many commentators, an instantaneous, sensitive, affordable and non-invasive method of DNA profiling is the 'Holy Grail' of human identification.

Glass-and-silicon chip micro-reactor laboratories offer a promising route to a solution to this problem. The micro-lab - some are as small as 1 cm^3 - is fabricated so that all of the reagents, mixing and temperature controls, and analytical pathways form integrated chip components. Being self-contained and disposable, the device is labour saving and less error prone, and less vulnerable to contamination by intrusive DNA than current procedures. The micro-channel architecture, micro-etching and electro-osmotic design of the chip components are optimised to aid the analytical process.

New generation single-nucleotide polymorphism (SNP) profiling micro-reactors will offer a further advantage in that DNA profiles are determined by a single base change and not fragment length, avoiding the necessity for a gel-electrophoresis component to resolve DNA lengths present. This should increase the efficiency of analysis and allow each result to be encoded in the minimum number of binary digits, making the whole process more amenable to electronic transmission, database storage and remote verification.

At present, connections to the external world are necessary to provide power and control systems to the chip. Portable control systems with remote access to computer databases linked to disposable devices could offer a way to use DNA micro-laboratory chips in mass screening or scene of crime scenarios.

No biometric ever seems to offer a single solution in identification and in the case of DNA it is the lack of a means of remote detection that is the flaw. There may be sufficient cellular debris and genetic material in exhaled breath - for example - to provide a DNA profile, so an instant DNA breathalyser may not be far over the horizon.

Drivers for the development of such novel systems are not limited to advanced forms of biometrics; other applications include medical diagnostics, and food and agriculture, as well as forensic, commercial and security related uses.

Gait recognition

The way in which people walk has been investigated for a number of years by several research groups, and in particular Southampton University in the UK and Georgia Institute of Technology. Two principal approaches have been documented, the model based and the model-free¹⁶⁵. Models have been based on the pendulum-like action of the movement of the thighs. Model-free representations determine 'eigengaits' from a principal components analysis of the motion using an optical flow model. Interest has increased from defence users of CCTV systems anxious to obtain more useful information from people walking at a considerable distance from the cameras, and hence beyond the working distance of facial recognition biometrics.

¹⁶⁴ Acknowledgement is made to Martin Evison and Ray Allen of Sheffield University who provided material for this section.

¹⁶⁵ A Kale *et al*, *Gait analysis for human identification*, 4th Audio and Video-based biometric person based authentication, AVBPA 2003 706-14 (June 2003); John Carter and Mark Nixon, *Measuring gait signatures which are invariant to their trajectory*, *Measurement + Control* **32** 265-9 (November 1999)

A related technique - useful for tracking individuals in a closed user group - is Overhead View Person Recognition. This technique fixes upon characteristic features of a person, e.g. hair colour and texture, to track a person using a network of ceiling mounted cameras¹⁶⁶.

Skin reflectivity

Lumidigm have patented a method of characterising the reflectivity, absorbance and scattering of light from the skin of individuals, as a function of wavelength of incident light and the distance between the light source and the skin surface. The method is under development for a commercialised product¹⁶⁷. A related technique is based upon the scattering of light from the nail bed under the fingernails. Spectrometry of the light absorbed by blood and scattered by skin is claimed to offer a way of distinguishing individuals¹⁶⁸.

Lip movement biometrics

This biometric could be an adjunct to either facial recognition or speaker verification systems, with the aim of improving the performance of either of these two methods¹⁶⁹. IDIAP at Martigny in Switzerland are making significant progress in this field.

Ear-based biometrics

Systems have been proposed that make use of

- a) The outer shape of the ear. This already used by a number of police forces to identify criminals, and the subject of the European Commission funded FEARID project. Research into the use of this feature as a biometric has been reported by a number of groups¹⁷⁰.
- b) The otoacoustic emissions measuring the response to a transient input signal broadcast into the ear¹⁷¹.

Odour recognition

In lists of biometric methods, odour recognition is usually added to illustrate the diversity of the field. The detail accompanying this claim is often very sketchy; not surprisingly, in view of the absence of any recent work in the field. In an overview report on biometrics published in 1995, forecasts of commercialisation of the technique within two years of further development were made. At the time, Leeds University and Mastiff Electronic Systems had been developing Scentinel for 8 years. The company, which licensed technology from Bloodhound Sensors, highlighted initial results in an article in the Financial Times of the same year, demonstrating how profiles of four subjects could be captured using 16 sensors, each of which was tuned to a different chemical¹⁷². Since then, little has been heard of this technology, in spite of Bloodhound's managing director

¹⁶⁶ Ira Cohen *et al*, *Vision-based overhead view person recognition* (2000)

¹⁶⁷ www.lumidigm.com

¹⁶⁸ Taegeun Kim and Yong Woo Kim, *Individual identification by extraction of nail bed pattern of the finger nail using confocal scanning optical system*, *Hankook Kwanghak Hoeji* **13** (2) 155-61 (April 2002)

¹⁶⁹ J S Mason and J D Brand, *The role of dynamics in visual speech biometrics* (2002)

¹⁷⁰ Belen Moreno *et al*, *On the use of outer ear images for personal identification in security applications*, 469-76 (1999); Mark Burge and Wilhelm Burger, *Ear biometrics in computer vision*, 822-6 (2000)

¹⁷¹ *Early warning system could combat fraud*, *The Guardian* (UK), (13 January 2003)

¹⁷² Clive Cookson, *A brave new olfactory world*, *Financial Times* (8 June 1995)

suggesting that it would be '*more reliable and convenient than other biometrics such as those based upon voice recognition or hand-prints*'.

Since that time, development of electronic noses has advanced. Many different types of sensor have been developed, aiming to reduce the size of the hardware, make the pattern recognition algorithms more robust and counter the drift in performance of most sensors. Several dozen companies have developed electronic nose products for a wide range of applications. These include tracking unpleasant smells to their source such as those from farm animals and fungi in buildings, diagnosis of certain medical conditions, monitoring of industrial scale processes on foods and beverages, fundamental studies on biological processes and combustion process in jet engines, and design and developments of perfumes and fragrances. DARPA are also funding studies on explosive mine detection¹⁷³.

Sensor developments that are particularly of interest in the context of human odour sensing include the microfabrication of channels and micropumps, and the construction of CMOS sensors that use FET transistors sensitive to specific gases and vapours. The new nano-technology paradigm is the key to developing gas chromatographs, mass and optical spectrometers that could perform the complex analyses of human generated odours.

The extent to which electronically sensed individually distinct odours can be measured remains uncertain, although certain clues are coming to light. For example, analysis of breath for halitosis has been demonstrated using a 40 element sensor array, with varying sensitivities¹⁷⁴. Rome University has recently demonstrated how an electronic nose can determine the vapourised concentration of a male pheromone from axillas of students; tests showed a bimodal distribution whose origin is the subject of further research¹⁷⁵.

In December 2002, DARPA solicited bids for 'odortype detection' biometrics based upon observations in mice that the same set of genes that code for the recognition of self/non-self in internal immune systems (the Major Histocompatibility Complex - MHC) also code for individual odour types¹⁷⁶. Limited evidence exists for parallel expression of the individuality of odours for human beings. The programme envisages a test-ready sensor at the end of 5 years and 6 months after its start, by which time most of the fundamental questions would have been resolved.

Forensic dental biometrics

Anil Jain and colleagues at Michigan State University have started work on semi-automatic recognition of individuals after death using the deceased person's dentition¹⁷⁷. Although generally biometrics does not concern itself with the identification of dead bodies, the numbers of victims of massacres or large scale terrorist actions merit consideration of automation of the process.

Pressure sequence

An interesting behavioural biometric has been described by Pieter Hartel. On the basis of small scale testing, Pieter claims that there is a distinctiveness in the way that individuals tap a musical tune or rhythm, data which can be captured using a polymer thick film

¹⁷³ T.C. Pearce *et al*, *Handbook of Machine Olfaction: Electronic nose technology*, Wiley-VCH (2003)

¹⁷⁴ *ibid*, quotes the results from S Ehrmann *et al*, *Applications of a gas sensor microarray to human breath analysis*, *Sensors and Actuators, B*, **65** 247-249 (2000)

¹⁷⁵ Corrado di Natale, *Human skin odour analysis by means of an electronic nose*, *Sensors and actuators B* **65** pp 216-219 (2000)

¹⁷⁶ *The US Army Research Office broad agency announcement DAAD19-03-R-0004* (December 2002)

¹⁷⁷ Anil Jain *et al*, *Dental biometrics: human identification using dental radiographs*, 4th Audio-and video-based biometric person authentication conference AVBPA 2003 429-37 (June 2003)

piezoelectric or piezoresistive sensor capable of integration with conventional smart cards. These initial tests on 34 subjects generated an EER of about 2%¹⁷⁸.

4.11 Multiple biometrics

The previous sections have shown that no biometric technology offers a perfect solution to authenticating individuals, even though some are beginning to demonstrate very impressive performance in certain application spaces. For those methods that are less accurate, yet may be more suitable in certain systems on the grounds of cost, availability of sensors, etc., combining more than one instance of the biometric (e.g. both eyes or more than one finger) is an option; as is the integration of results from more than one biometric technology (multi-modal biometrics). Alternatively, combining a biometric (or more than one) with a non-biometric authentication technology could also lead to improved security. A final way in which multiple biometrics could be implemented is for more than one type of algorithm to be used for the same underlying technology. For example, a video camera could take a sequence of images; these would be distributed to a number of software modules, each of which would attempt to match the images against a database of templates (which could be more than one for each individual). One module could operate optimally for 'full face on' images, whereas others might be able to make better use of a number of images from different angles. In addition, it might be shown that certain individuals were more readily identified using specific algorithms.

The fusion of data is of course critical in this type of application and research continues on determining models for such fusion. (Clearly, a simple model for fusion of data, at the output of two biometric systems, has severe limitations. Combining in either OR or AND mode leads to improvement in one type of error at the expense of an increase in the other rate.) Fusion of outputs from a high performance system and one with a weaker performance presents additional challenges.

Other benefits that may result from the use of multiple biometrics include provision of fallback measures in case of disabled users and the opportunity of adjusting security thresholds for differing situations and times.

Key requirements for success in future research is the creation of large databases of simultaneously acquired data for the individual modalities, and for testing and evaluation methodologies that will aid in the development of this promising approach to biometric authentication.

4.11.1 Principal methods

Ross and Jain note that there are three ways of fusing all-biometric data¹⁷⁹, although a fourth approach has also been described:

- Fusion at the feature extraction level, creating a complex template that represents the individuality of the person in the aggregation of data from the respective biometric systems. The informational value of the combined template depends upon the degree of independence of the individual traits that are used in the biometric systems.
- Fusion at the matching score level, bringing together the match scores from each of the biometric technologies, and applying specialised techniques to arrive at a final decision.
- Fusion at the decision level, with a voting scheme to determine the outcome of independently derived pass/fail decisions from the individual biometric technologies.

¹⁷⁸ Neil Henderson *et al*, *Polymer thick-film sensors: possibilities for smart card biometrics*, www.ub.utwente.nl

¹⁷⁹ Arun Ross and Anil Jain, *Information Fusion in Biometrics*, (preprint, 14 November 2002)

- 'Layered Biometrics', in which users must pass each successive biometric test before passing onto the next one. Successful completion of this route allows the user access to the protected resources.

4.11.2 Principal commercially available systems

Systems were available from Keyware (Belgium) and Dialog Communication Systems, the suppliers of BioID¹⁸⁰. Keyware sold off its biometric components to Identix in 2002. It is believed that a Malaysian company is still offering multiple biometric systems.

BioID combined recognition approaches based upon facial, voice and lip movement biometrics. In the case of face and lip biometrics, a result is only considered reliable if the best match to a template exceeds the match to the next ranking template by a pre-defined threshold. Fusion at the matching score level offered systems integrators or administrators a variable security threshold, based upon a weighted summation of two or three acceptable results from each of the base biometrics.

4.11.3 High Profile deployments

At the time of writing, there were very few pilots or deployments using more than one biometric method. Nevertheless, the recommendation by NIST for the use of both facial and fingerprint recognition for immigrant visas to the USA may require consideration of multimodal strategies that such a proposal implies.

4.11.4 Testing and issues of performance limitation

Large scale testing of multimodal (and multiple) biometric systems is still to be undertaken. As the section below on standardisation makes clear, the absence of agreed protocols and large databases is a limiting factor in the application of multiple biometrics. One of the best compilations of data is the European XM2VTS database which consists of facial images, sequences of video and audio recordings of speech obtained from 295 subjects, and collected in four sessions at monthly intervals.

4.11.5 User concerns

The studies associated with this roadmap demonstrate the considerable challenge in developing a user-friendly system with just one biometric. More ingenuity will be required to ensure that end users accept that a second or third system is required, and that these methods are integrated in the most appropriate way. Much will depend on the specific requirements of the application. Parallel or serial operation, the extent to which users have to make a conscious effort to divert themselves from the operation without the biometric, and the explanations which are offered; all will be crucial in determining the acceptance of more complexity.

4.11.6 Legal and regulatory dimensions

There appear to be no specific legal barriers to the use of multi-biometric systems over and above any restrictions relating to the individual biometric methods, although proportionality could be an issue unless the rationale for its use were explained and accepted by end users.

4.11.7 Standardisation activities

¹⁸⁰ Robert Frischholz and Ulrich Dieckmann, *BioID: a multimodal biometric identification system*, IEEE Computer, 64-68 (February 2000)

A proposal for a study project was made in the USA's INCITS Technical Committee M1 to clarify the taxonomies of operation and specify methods of evaluation of the performance of this type of system¹⁸¹. Subsequently, the Korean national standards agency, KATS, put forward a proposal for an API framework that would enable the combination of results from at the Biometric Service Provider level - not at the biometric feature level¹⁸². This work was not progressed and a new proposal for a Technical Report is under discussion.

4.11.8 Principal research projects

This is an active area of research in which European companies and consortia (e.g. the European Commission funded BANCA project¹⁸³) have played a major role in the immediate past. The University of Surrey's team at the Centre for Vision, Speech and Signal Processing continues to work with a number of European partners to optimise the performance of systems, testing against the X2M2VTS multimodal database. Other pioneering studies are in progress at the Pattern Recognition and Image Processing Laboratory at Michigan State University.

In the UK, IAMBIC, a DTI-sponsored project, has used multimodal biometrics and intelligent agents to develop new frameworks for secure access control in on-line environments¹⁸⁴. Fingerprint, speech and facial recognition were fused and trialled in a healthcare setting. One interesting feature was the inclusion of user-behaviour monitoring at the server.

4.11.9 Outlook for the future

The use of multiple biometric strategies, whether these are multimodal or just using two or more approaches for the same biometric method, appears to have a promising future. The research to date has shown that performance can be improved over the use of a single system, but most of the studies have been carried out on relatively small datasets. This roadmap demonstrates the complexity of deploying a system using even one biometric. Adding more complexity through the use of a further biometric will have to be justified on a clear cost-benefit basis.

RC/C3 RC - COMPONENTS 3: In view of the limitations of individual biometric methods, further research is needed to optimise the performance of multi-modal biometrics. This should focus on improvements in the approach to fusion of measures, as well as to address the requirements of specific applications and services

4.12 Future developments

This review of the component technologies demonstrates the diversity of biometric methods. It is difficult to explain why these should all be considered in the same context, since the difference in performance and applicability between fingerprint and iris methods on the one side and keyboard dynamics and hand geometry are substantial.

In looking towards the future, one obvious question concerns the ultimate performance of a specific method. Given the best algorithms and a co-operative population, what are the

¹⁸¹ M1/03-0141 *Study Project proposal: Evaluating Multi-Modal Biometric Systems: Concepts of Operation and Methods of Performance Evaluation* (17 March 2003)

¹⁸² ISO/IEC JTC 1/SC37, N164: *New Work Item Proposal on a Multi-Modal Biometric Framework* (6 May 2003)

¹⁸³ <http://falbala.ibermatica.com/banca/index.html>

¹⁸⁴ <http://www.iambic-project.org>

limits to enrolment and operation? A detailed analysis of the competing ways of implementing each technology could indicate that more effort should be devoted to a specific approach, or that the technology will never attain the robustness and repeatability demanded by some applications.

A similar question could be posed regarding the templates used by different systems. How can one characterise the proximity to 'uniqueness' in a population, whether at the national level or in a closed user group? Other related unknowns include the variation or entropy for specific classes of the population, whether segmented by gender, by age, ethnicity, etc. Finally, relatively little work has been undertaken on long term stability of templates (over periods in excess of 5 years), in spite of the assumption that many potential operators make that their investment will keep on returning value for the lifetime of their customers or employees. Both fingerprints and iris patterns should exhibit such stability, but specific implementations, whether using a given type of sensor or algorithm could influence the stability. Most of the world's criminal fingerprint records are likely to consist of young males, and the ability of 80-year old women to provide usable fingerprints to silicon sensors remains to be demonstrated.

The hunt for a better biometric continues, with new ideas being examined. The use of real-time DNA analysis has been discussed in the popular press, even though it may be many years before all of the problems are resolved¹⁸⁵. A methodology to help inventors with their ideas would be helpful, and the research described above should help them determine whether there is a commercial business case for their proposal.

RC/C4 RC – COMPONENTS 4: Research into the ultimate limits of performance with various methods of implementing specific biometric techniques

RC/C5 RC – COMPONENTS 5: Research into the 'uniqueness' of a template, and the extent to which it depends upon demographic factors such as gender, age, ethnicity, etc. Do such templates exhibit stability over extended periods of time (> 5 years)?

RC/C6 RC – COMPONENTS 6: A methodology to determine whether novel methods of using the human body for secure authentication are worth supporting

RC/C7 RC – COMPONENTS 7: Use of DNA as a biometric, including the development of protection mechanisms.

¹⁸⁵ *The Case for national DNA identification cards*, 2003 Duke L. & Tech Rev. 0002, www.law.duke.edu/journals/dltr/articles/2003dltr0002.html (31 January 2003)

5. Critical Issues in the Application of Biometrics

The successful deployment and operation of applications using biometrics depends not only on the technology and its integration with other functionality in a service, but needs to take account of the 'human' and 'social' elements. A series of BIOVISION studies summarised the current state of the art in each area, identified the crucial issues still to be resolved, and assessed their impact on a range of applications that are the subject of this roadmap. A number of unresolved issues are proposed as the subject of proposals for research projects or calls for social interventions such as new or amended legislation and codes of practice.

5.1 End user perceptions

Biometrics as a technology has taken a long time to become established in practical applications and still has some way to go before gaining mass acceptance levels. The fascination with the biometric technology of the last decade has now moved to a more objective thinking about the use of biometrics in typical everyday applications. Vendors are more aware of biometrics and how they might be used to their advantage. It is understood that desired response time, available performance or required accuracy rates are playing an important role in the decision process. But until now, a more in depth understanding of human factors has been neglected.

Issues of usability have generally been left to "programmers", who have not concentrated on issuing guidance around usability issues to improve the end-user perception and experience. This difficulty is compounded by the fact that vendors, consultants, systems integrators and users seem to speak different languages, leading to potential misunderstanding and confusion.

Software support

The first key activity of the BIOVISION project team in this area was the development of Pentakis. This complements the BANTAM (Biometric and Token Technology Application Modelling Language) methodology that may be used across barriers of both language and expertise. Furthermore, its use extends into aspects of procurement and training, providing prospective users and developers with a complete package. Note that the BANTAM User Guide¹⁸⁶ provides extensive practical guidance for both users and developers in this context.

To encourage a wider public acceptance and thus usage of biometrics, it is extremely important to develop systems that are easy to understand and easy to use. Training plays a large part in this respect and, ideally, a comprehensive training package should be devised at the time of application development. All too often, however, detailed information about a specific application is not easy to find, not comprehensive and not in an understandable form.

Initially, it appears that people have a spontaneously positive attitude towards biometrics. At a second glance there is a tendency to be sceptical, especially with regard to the privacy issues when using biometrics. The way that users are given assistance during their first contact with a biometric system is key to its acceptance and their willingness to use it in future. A comprehensive explanation of the system and good operating instructions at the time of registration will have a positive influence on a user's evaluation of the technology and subsequent use under real operational conditions. In particular users may well want to know how the technology works, where the data is stored, which data is registered, how the data is protected, who has access to the data and who is operating the system. Users have also expressed worries that their biometric data could be counterfeited or misused. However these doubts appeared to depend on the system operator.

¹⁸⁶ Julian Ashbourn, *BANTAM user guide*, Springer (2002)

We need to expand our thinking from individual device performance through to considering the performance of the system as a whole - including the interaction between human and technology. Most biometric systems require a degree of user interaction at some point, thereby necessitating consideration of user psychology. In this respect, there is a distinction between a 'professional' user (someone such as a systems administrator or an individual who uses a specialist application) and a 'general' user (someone who is required to use the system in a number of circumstances).

In order to understand aspects of user psychology and the associated impact upon systems performance, it is important to obtain metrics that are robust and useful. The User Psychology Index (UPI) has been developed over several years in order to provide a suitable methodology with which to assess this dimension. More recently, it has been translated into an easy to use software utility, a revised version of which is included within the Pentakis software programme. Pentakis additionally includes modules with which to assess transaction times, scalability, population profile analysis and cost analysis. These are all related areas in the context of acceptable implementations of applications featuring biometric identity verification. There will be further developments of the Pentakis concept in the future.

Developing a framework

Until recently, security research had largely ignored usability issues. Studies which showed that many users circumvent IT security have led Bruce Schneier to coin the phrase that security is only as good as it's weakest link, and that users are the "weakest link" in the security chain. This sentence is catchy, but not entirely helpful, because it implicitly places the blame for this state of affairs on the users. The security research community has begun to realise that usability in real-world operation and user acceptance are essential pre-requisites for effective security systems, and has started to adopt user-centred design approaches and methods to ensure usability and acceptance. As part of the second strand of BIOVISION activity in this area, the end user perception team commenced work in this area specifically addressing biometric systems.

The conceptual framework for a user-centred approach has four interacting key concepts:

- users,
- their goals and task,
- the technology, and
- the context of operation.

Essentially, the user and the technology interact to achieve a specific goal (users tend to have a standard set of goals, and a number of tasks they are involved with to achieve them). This interaction takes place in a particular physical and social context. In BIOVISION, the team has started to create a user-centred taxonomy of all the characteristics of any of the four key concepts that could be relevant to the implementation of biometric technology. For example, users can have physical characteristics that make operation of certain biometric systems difficult, or beliefs or attitudes that pre-dispose them against certain types of operation. In some tasks, speedy access is imperative, in others it is not. The impact of factors in the physical environment – such as lighting – are reasonably well understood, but the implications of different social contexts are less well ascertained. The BIOVISION project has started to collect data to populate the taxonomy with relevant factors.

We have noted that the context affects the interaction between user and system - and vice versa. For example, systems working well for the individual single user in a quiet office may not perform adequately in a shared office. On the one hand, a user interface can operate well when the user can focus on the task without undue interference, while it is not surprising that the same system shows poor performance when the user's attention is distracted. As offices and other environments grow more complex, such group interactions multiply.

Existing knowledge about these factors is largely based on observations of specific implementations. This data can help to identify some relevant factors. For instance, empirical findings from the BioTrusT project and from the Federal German Consumer Association have shown that:

- Contact with biometrics, and therefore using authentication systems based on personal human characteristics, appears to make people more sensitive to the implications for their use.
- Users have a definite need for information about the mechanisms of operation of such systems.
- Consumers are well aware of the disadvantages of conventional methods and would prefer biometric methods instead of passwords or PINs. At the same time the need for secure storage and handling of biometric data was very pronounced among the users.
- Enrolment should be performed by experienced staff who are aware of the quality levels that are required of the recorded data.
- User guidance is also important. Users want a detailed explanation of the way in which they are asked to present their biometric features. This is important as active co-operation from the user is nearly always required.
- There appear to be no one single biometric characteristic that is suitable for all kind of people. People are as different as their physical characteristics are individual.

However, there is a pressing need for systematic studies of performance in real-world context - and furthermore, these studies should address extended use.

We have no scientific approaches to compare performance of mechanisms in the field; a methodology similar to the performance testing method described in Section 4 is required. Similarly, data on user attitudes have been largely collected from one-off focus groups. There have been no studies of how user perceptions and attitudes develop as a result of longer-term interaction, or how users prioritise conflicting goals, beliefs and attitudes.

In-depth and contextualised research on end-user-perception has started addressing the gaps in the taxonomy. We have focussed on collecting data on performance in real-world contexts, conducted in-depth analysis of qualitative data (using Grounded Theory analysis) to construct models of perceptions, beliefs, and decision-making processes of different user groups, and in different contexts of use.

Finally, user-centred design proscribes going beyond studying users and their interactions with the technology. We have applied participatory design methods to involve prospective users in the process of identifying requirements and designing a technology solution. We have conducted a pilot workshop with users from one specific domain (the health sector) and with specific biometrics manufacturers. The aim of the workshop was start engagement in a process of collaborative design. Starting from the key problems that users encounter in achieving their goals, developers work through scenarios to determine if biometric technology can help to solve those problems, and how it would have to be implemented to operate in this specific context.

The empirical work undertaken by the team identified a key result: user acceptance of biometric solutions depends in the main on whether the solution offers benefits in terms of convenience, rather than whether it results in enhanced security. The relief from mental demands that multiple PINs and passwords place on individuals was almost palpable. However, while biometrics can an inherent advantage over knowledge-based mechanisms, this advantage can only be realised if a biometric solution

- provides a good fit to the production and security tasks that users have to carry out, i.e. it is well integrated into the work process
- performs well (in respect of acceptable speed and low error rate) in all aspects of its use (during installation, at registration, in daily use and under exceptional conditions)

- is trusted to be safe with the biometric data secured and without the potential for reuse for other purposes.

Most users that were interviewed would welcome the introduction of additional features to personal electronic applications that improve safety or convenience in their use.

However, there is a bifurcation when they are asked about the use in enhancing public safety and in passport and border control applications. In general, the older respondents welcomed these uses, with the perception often expressed in terms of 'it would help to catch illegal immigrants and criminals, while the ordinary citizen has nothing to worry about'. The other group of participants, however, was distinctly sceptical about the benefits and saw potential threats. For them,

- such applications are seen as 'for the convenience of government agencies, rather than for the citizen'
- agencies are not trusted to secure the biometric data to an adequate extent
- data would be used for purposes other than those advertised.

Previous work in relation to multimedia applications suggests that risks to users must be made explicit in advance of any deployment, with users being given a choice as to whether to use them. Furthermore, it seems that implementation standards and the opportunities for redress that should be a feature of commercial implementations should also apply to government applications.

The research priorities that this work has uncovered include:

- New forms of requirements capture and application design are needed.
- Performance measures of systems in daily use under operational conditions need to be researched and standardised for ease of cross-comparison
- Evolution of the perceptions of end users and the influence of the social groups of which they are a part need to be understood, as a pre-requisite for engaging the most effective forms of managing the fears and concerns of users
- Studies of the long term risks and of the potential of biometric methods to elicit mental and physical conditions
- Improvements in the legal and regulatory framework to include the provision of recourse to law and financial redress in case of intentional or unintentional misuse.

RC/TTL5 RC - TRIALS, TESTING, LEGAL, etc 5: Further research is needed, based upon the initial proposals in the BIOVISION project, that will test perceptions by end users and the social groups of which they are members. This should also examine the evolution of such perceptions and whether different techniques apply to other social groups and cultures.

RC/PS1 RC - PRODUCTS AND SOLUTIONS 1: Transparent - yet not covert - systems with excellent adaptive user interfaces, delivering apparently 'instantaneous' authentication for end users

RC/PS2 RC - PRODUCTS AND SOLUTIONS 2: Systems that are easy to install securely, with useful and appropriate feedback if they fail

RC/C8 RC - COMPONENTS 8: Systems that minimise the mental and physical load on the end user, particularly if that end user is physically or mentally disabled.

5.2 Security

Improving security, or improving usability while maintaining security, is a main driver for using biometrics. Though biometrics have been successfully deployed to improve security in many applications, in general these are closed systems with co-operative users. There are several security issues that have yet to be fully addressed if biometric methods are to be deployed more widely.

What is Security?

The need for security, and the meaning of security for any application, will depend on the purpose of the application and the environment in which it will operate. For access control, the risk is typically unauthorised individuals masquerading as authorised users – in biometric terms individuals attempting to make their biometric features look like someone else's – and the measure of security will be the level of protection offered against unauthorised access. In such cases the distinction between authorised users and others is usually clear.

For other applications, the chief risk may be individuals establishing multiple identities, for the purpose of extracting multiple benefits or credentials in different names – in biometric terms, users attempting to make their biometric features NOT look like themselves. Here the distinction between authorised and unauthorised users is less clear in that a user may have both a legitimate identity and other, illegitimate ones.

The security requirements and measures are quite different for these two cases, and practical applications may be even more complex. Real-world applications can embody a range of different functions, each with its own distinct set of security risks and associated security requirements.

Few high security applications

To date most biometric deployments have relatively low security requirements, either by design, or by the nature of the application. Of the potential future applications for biometrics, their use for national identification systems will require substantially higher levels of security than those for current biometric systems, especially if the biometric templates and/or images are stored in a central database. Security would also need to be strengthened when the same biometric is used for a variety of applications.

'Live and well' features

There is a pressing need to improve biometric products to make it much harder to spoof the devices by artificial means, or by mimicry. While it is true that existing publicised exploits have been performed on relatively cheap low-end devices, it is not clear whether the more sophisticated, and expensive, currently available systems would be much better. Moreover, for negative ID systems, e.g. for establishing a unique identity, these 'live and well' features must address the fact that it is generally easier for someone to appear not as themselves (false non-match) than to appear as someone else (false match).

Template protection & consent

Work has commenced on template protection techniques that can bind a biometric template to a particular application, disabling its use by any other application (without the application provider's consent). Such techniques may be extensible allowing the user to withdraw consent and disable the template (as they do not have the option to change their biometrics).

People and security

People are often the weakest link in a security system. A biometric ID system may need to protect against

- collusion between a fraudster and enrollee or enroler,
- insider fraud directed against the company or an enrollee, and
- intentional or unintentional bypass of security procedures
- fraud perpetuated by legitimate enrollees, through the establishing of multiple identities.

Security evaluations

For biometrics to become accepted as a security technology it would seem appropriate that biometric systems are formally evaluated for security. The Common Criteria (CC) framework has been validated for many other IT systems, although accreditation can be time consuming and expensive. Even if vendors intend their products to be offered for such evaluation only at some point in the future, development of software and hardware should be undertaken in a way that will facilitate such an evaluation process. At present, however, only two biometric systems have been evaluated under the Common Criteria, and these only at a basic assurance level (EAL2)¹⁸⁷. In part this may be due to the high cost of CC evaluation in relation to the value of assets currently protected using biometrics, and also that there are not a standard set of security tests. It should also be noted, however, that suppliers are reluctant to publicise the details of the proprietary algorithms used in their engines, and that for those biometric technologies that are still developing (e.g. face recognition), these algorithms are subject to continuing change. Assessing the security of a biometric without a formal certification continues to be problematic for system designers and operators.

A further issue is the difficulty inherent in statistical testing – the number of impostor attempts required is inversely proportional to the error rate required, and it is simply infeasible to make, say, 3×10^{11} attempts to show an error rate of 10^{-11} (an error rate required for some national ID systems, for example). In time, these issues may be addressed by standard security evaluation methodologies for biometrics, and by an improved understanding of the scaling of the performance of biometric systems as larger biometric deployments are made.

RC/Sec1 RC - SYSTEMS AND DESIGN: SECURITY 1: Methods are required to evaluate and compare the security of biometric systems. Schemes other than the Common Criteria framework should be investigated for their suitability. The level of security should appropriate to the application and the risks involved. In particular the binding of the application to the result of the biometric authentication has to be secure. In view of the value of databases of biometric identifiers to other people and organisations, these may need to be secured against both internal and external threats using state-of-the-art techniques. Appropriate security is also required for the templates during their transmission between database and application. All security measures subject should be periodically subject to a review.

RC/Sec2 RC - SYSTEMS AND DESIGN: SECURITY 2: Methods for the design and secure implementation of appropriately secondary systems that cope with both false match and false non-match errors. Such strategies may be required to operate in a gradual manner.

RC/Sec3 RC - SYSTEMS AND DESIGN: SECURITY 3: Development of design methodologies that support the secure integration of biometric data in applications such as the Criminal Justice Sector, while limiting the opportunity for misuse and 'function creep'. These could make use of binding of the user's identity, the application, template and user's expression of consent as well as validation by external Trusted Third Parties.

¹⁸⁷ The results on only one have been published.

RC/Sec4 RC - SYSTEMS AND DESIGN: SECURITY 4: Biometric data for different applications (or held centrally and on-card) may require to be of different types (or held in incompatible formats) in order that centrally held information cannot be misused.

RC/Sec5 RC - SYSTEMS AND DESIGN: SECURITY 5: Provision of 'live and well' features in biometric systems is a high priority, especially when these are unattended or only intermittently attended by security personnel. Testing of the liveness of the biometric signal needs to be commensurate with other security aspects of the system

RC/TTL6 RC - TRIALS, TESTING, LEGAL, etc 6: Tools and methods for the forensic investigation of the abuse of biometric methods.

RC/C9 RC – COMPONENTS 9: Performance improvements are needed to reduce the possibility of chance matches between different people, and for identification of non-cooperative users in negative identification applications

5.3 Safety and medical issues

One of the issues that causes concern in the application of biometrics is that there may be a direct or indirect medical risk. We aimed to examine these concerns for the specific cases of face and iris recognition, fingerprint and hand geometry biometrics.

Many established commentators in the field of biometrics maintain that 'user acceptance' ought to be considered as one of the most significant factors in the successful take-up of biometric applications. However, the term 'user acceptance' encompasses many aspects, from individual psychology to ergonomics, but rarely has it been examined with respect to the medical aspects. This is mainly due to the limited knowledge about biometrics amongst the general public partly due to the limited deployment in the everyday life of citizen, consumer and employee. As biometrics gains prominence, we anticipate that curiosity or speculation could make potential users question the direct or indirect effects of biometric techniques on their health.

The diffusion of inaccurate or uninformed data may have impact adversely on a specific technique, as well as on the wider biometric world. Such hostility could easily feed upon other concerns such as privacy. A clear assessment of the medical issues should pre-empt these concerns, so that, for example, reluctance to use certain sensors is not easily justified on hygiene fears.

There are, of course, international standards for the safety of many of the components used in biometric systems, and these should be used wherever possible. Nevertheless, care will be required in the interpretation of these in the context of novel technologies. These considerations are termed the **direct medical implications** of the application of biometrics and their impact should be examined for those systems that are likely to be most widely used.

There is another class of medical concern, termed **indirect medical implication**, where physical or mental characteristics or conditions might be deducible from biometric measurements. Some methods, such as iris recognition, have specific concerns. Followers of iridology would claim that medical conditions could be diagnosed from an iris image. However this has little or no scientific or medical support. Reassurance to such individuals as to the information that is stored in the template may go some way towards countering even their concerns. The scientific basis for the elucidation of certain

behavioural traits or physical conditions from biometric signals has begun to be analysed, with some initial results available on the assessment of anxiety states.¹⁸⁸ Of course, the possible future use of DNA analysis as a biometric (not a feasible option currently) raises potential issues of privacy and indirect medical implication, whilst other proposed techniques that are not strictly biometrics could add to the confusion in the mind of the public at large.¹⁸⁹

RC/Med RC - SYSTEMS AND DESIGN: MEDICAL ASPECTS: Further development of the BIOVISION methodologies for ensuring health and safety in systems using biometrics and the non-disclosure of medical conditions.

5.4 Future directions in the underlying technologies and applications

The individual descriptions of technologies in Section 4 show how the future direction of each method is being shaped by the requirements of applications. The detailed studies completed by the BIOVISION consortium (summarised in Section 3.1) offer a framework for considering the matching of functional requirements with what a commercially available system can offer.

The members of the consortium have looked at the research programmes and the subsequent formation of SMEs in some cases to capitalise upon that research. It acknowledges that some projects were successful in advancing the fundamental aspects of biometrics. For example, the Fourth framework BIOTEST project laid the groundwork for testing and reporting, which is now being adopted by ISO/IEC SC37 SG5 as an international standard.

However, many projects appear to be disconnected from developments in the commercial sector and from any viable applications. Often, basic information about the subtleties of the using biometrics is rediscovered, sometimes quite late in the lifetime of the activities. In any proposals, the sponsoring body should insist on clearer setting of objectives, especially if the results of the work are directed towards impacting on the market.

It is clear that the research and commercial dissemination routes often do not meet. Research meetings speak to other researchers, with potential commercial users finding difficulty in interpreting the significance of their findings. In turn, commercially run conferences often fail to take account of ongoing research projects, for fear of confusing the target audience most of whom appear to be newcomers to the field. An example of the response of the commercial sector to the opportunity of showcasing cutting edge research is the award of prizes for such studies by the organisers of *Biometrics 2002* in London¹⁹⁰. We anticipate that the European Biometric Forum will play a key role in co-ordination through the EBF of research projects, interpretation and demonstration.

RC/RA RC - RESEARCH ACTIVITIES: Following the initial phase of establishing research teams throughout European organisations, funding bodies should now ensure that new research projects are based upon a solid appreciation of both the current status of the research as well as the realities of commercially viable

¹⁸⁸ Frank Deane et al, *Theoretical Examination of the Effects of Anxiety and Electronic Performance Monitoring on Behavioural Biometric Security Systems*, Interacting with Computers 7(4) pp 395-411 (1995); Ioannis Pavlidis et al, *Thermal Imaging for Anxiety Detection*, [IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications \(CVBVS 2000\)](http://www.htc.honeywell.com/people/ioannis_pavlidis/Publications/Docs/IEEE_ICIP_01.pdf).

http://www.htc.honeywell.com/people/ioannis_pavlidis/Publications/Docs/IEEE_ICIP_01.pdf

¹⁸⁹ US General Accounting Office, *Investigative Techniques: Federal Agency Views on the Potential Application of 'Brain Fingerprinting'*, GAO-02-22 (October 2001)

<http://www.fas.org/sfp/othergov/polygraph/brainfinger.pdf>

¹⁹⁰ *Biometrics 2002: 5th world conference and exhibition on the practical application of biometrics*, London 7-8 November 2002

deployments. If the European biometrics sector is to flourish, timely sharing of knowledge between the research and commercial sector is vital.

5.5 Legal and regulatory dimensions

Data protection

The legal and data protection issues surrounding biometrics have given rise to much comment and concern. These concerns have arisen from the user community due to worries that their biometric data will not be properly protected, may be accessed or stolen and used for criminal or fraudulent purposes or indeed that they may be tracked and traced while going about their daily activities. Some commentators believe that there are inherent dangers in the application of any biometric, and that these are sufficiently serious to warrant critical examination of any proposals for their use. This has appeared to be the position of some EU Data Protection Commissioners; as demonstrated in responses to a questionnaire that was sent to all the Commissioners¹⁹¹.

The EU Commission itself has classified biometrics as a privacy enhancing technology and it is understood that the Commission would wish biometric technologies to be developed more towards the preservation of users' privacy¹⁹², an opportunity that has been downplayed in discussions on deployments of these technologies. For example, a securely designed access control system using a fingerprint or iris recognition biometric can offer a better solution to a medical database system, than one using keys (which can be lent to unauthorised personnel) and passwords (with their reduced accountability and ease of abuse). In this way, a biometric can be a positive measure to improve the privacy of the individual – provided that the system is designed and implemented with an appropriate methodology. Such systems can offer a clear competitive advantage if the whole life costs (including training and reassurance to end users) are taken into account. *Privacy Best Practices* offers initial guidance for operators and users.

In reality, there are a number of different viewpoints, and the opportunities and dangers are dependent to a large extent on the context in which a biometric is deployed and the way in which protection of personal data is viewed by the system designer and operator. It is not helpful to reduce the debate to the place where the template is stored, whether on a card held by the individual or in a central database. A useful approach is to conduct a Privacy Impact Assessment at an early stage of the design (using the Privacy Best Practices as developed in draft form in BIOVISION), to allow a public discussion on the proposed deployment and its security, and then to continue to offer information and support to end users during the implementation and rollout of the system (see also Section 3.8).

The intention of BIOVISION has been to develop best practice in this area. The answer to the resolving these differing viewpoints may lie in addressing these concerns directly and provide guidance to the biometrics industry and to those that use biometric technology, to ensure that its use complies with data protection and (or) privacy requirements. Indeed, some commentators believe that it may be necessary to update current data protection regulations to take into account the new issues exposed by this relatively new technology.

The starting point for discussion on the privacy aspects of biometrics in Europe is the 1995 EU Directive on Personal Data¹⁹³ and the national laws that implement this directive

¹⁹¹ BIOVISION project: Astrid Albrecht, *Best Practices in deployment of biometric systems* (2003). In particular, CNIL - the French DP authority seems to be able to call in any proposal for the use of biometrics in the public arena.

¹⁹² The Article 29 Working Party on Data Protection is completing a study on biometrics which is due for publication in mid 2003.

¹⁹³ Directive 95/46/EC http://europa.eu.int/comm/internal_market/privacy/law_en.htm

in the respective Member States¹⁹⁴. This transposition has led to notable divergences in terms of the Member State requirements with regards to biometrics and the review of law and practice in the individual countries is a major output of the BIOVISION activities in this area¹⁹⁵. These issues have been examined through a questionnaire to the Data Protection Commissioners, which has ascertained their current views on the application of biometrics.

Additional legal issues

From a contractual perspective, for those companies that are manufacturing, developing and purchasing such technologies there are many new issues to be faced. These require that in the contractual area there is a great need for transparent, fair, comprehensive and non-discriminating conditions, which are also valid for the necessary informed consent for data processing.

Enterprise applications of biometrics are steadily increasing for such applications as physical and logical access. It has to be further examined which legal requirements are to be fulfilled in terms of industrial law and participation of the companies' data protection officer. Whereas, for example in Germany strong legal requirements exist, in other European countries this is not mandatory but may increase the employees' acceptance of a biometric system. At the current stage, operators who have to take the employees rights into consideration cannot be sure of meeting the legal requirements also in terms of protection the privacy of the users.

The consortium has provided the first input to the biometric community that will help it in dealing with the legal and contractual issues involved in the use of biometrics.

It is increasingly becoming apparent that one of the drivers for this particular sector is that of regulation and legislation. This is apparent from many sources including the expected tender from the UK Home Office for a biometric programme in 10 UK airports as well as the programme for biometrics in the passports and visas of all the US visa waiver countries. The BIOVISION project has examined and catalogued such regulatory issues¹⁹⁶.

Biometrics and Privacy-Enhancing Technologies

PETs offer technical solutions to the challenge of maintaining the data subject's control over their personal data. These also enable organisations that use such data to avoid reliance on people and procedures. For example, employees can make mistakes, can be subverted by bribes or be blackmailed. Managers can decide to allow 'function creep' following pressure to cut costs or justify the business case for a new service. Procedures can also not be followed, for instance when a security officer relaxes rules on writing down passwords in the face of widespread disobedience of the original security policy.

Texts such as Fischer-Hubner's define a range of possible objectives of PETs¹⁹⁷:

- Anonymity or pseudonymity
- Depersonalisation, rendering data into an anonymous format
- Unobservability
- Unlinkability
- Delocalisation

¹⁹⁴ http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm

¹⁹⁵ Astrid Albrecht, *op cit*, collates responses from the data protection commissioners of Denmark, France, Germany, Portugal, Sweden and the UK

¹⁹⁶ BIOVISION report: Astrid Albrecht and Martin Walsh, *Report on legal and privacy issues* (July 2003)

¹⁹⁷ Simone Fischer-Hubner, *IT-Security and Privacy: design and use of privacy-enhancing security mechanisms*, Springer-Verlag (2001)

Biometric methods offer a measure of protection for personal data, through auditable access control, either to filing cabinets of manually held data through physical access control, or to material held in databases through electronic control of access. If viewed in this way, they can be seen to be privacy-enhancing. However, databases of biometric identifiers - whether these are images of faces or fingerprints, templates, or pointers to where these are stored - are liable to be targets for criminals. They could be governments that wish to extend the use of the biometric to other services that were not envisaged in the initial proposals. The management of private organisations could trade their authentication capabilities if the local legal environment did not preclude this. In each of these cases, a biometric system incorporating privacy-enhancing measures could support the rights of the individual data subject.

One of the earliest attempts to create a commercially viable privacy enhancing biometric was the Mytec optical computer. A coherent light source reflected off an optical fingerprint-sensing device, and coded the fingerprint into the two-dimensional *Biocrypt* image using a proprietary one-way optical function. This could then operate the protected applications, e.g. through releasing the private key in a PKI system. Only the reapplication of the correct finger would enable that function to be performed. As the fingerprint was itself optically encoded, it would not be possible to regenerate the initial image or link it to a specific individual.

ZN Vision has developed a Privacy Filter that blurs facial images in a CCTV system and sets an alarm once a face is recognised by its algorithms, decoding the image for use by the legally permitted authorities¹⁹⁸.

More recently, other systems have been proposed. For example, Philips engineers have proposed a delta-contracting and epsilon-revealing function, along with 'helper' functions to code the biometric information robustly and securely¹⁹⁹. There are other approaches such as hiding watermark functionality within the template generation algorithm and the use of cancellable biometrics through the application-dependent distortion of the image (notification of a stolen biometric allows the re-enrolment to a different distortion function)²⁰⁰.

RC/TTL7 RC - TRIALS, TESTING, LEGAL, etc 7: Further development of the Best Practices, based upon experience of similar codes in other fields. One specific application could be in the integration with Privacy Impact Assessments, together with advice to auditors confirming the adherence to such a Code.

RC/TTL8 RC - TRIALS, TESTING, LEGAL, etc 8: Further studies should continue to monitor the progress towards a uniform interpretation of the privacy issues surrounding the use of biometrics in the countries of the EU (including the Newly Accessioning States), and support the activity of the Article 29 Working Party with impartial information about developments in biometrics. Users' experience in the application of biometrics should be collated and interpreted with the aim of either lobbying for a revision in the legal regime or for retention of the *status quo*.

RC/TTL9 RC - TRIALS, TESTING, LEGAL, etc 9: The status of those unable to use the preferred biometric solutions should be recognised, whether these are in the private or in the public sector. Solutions are required that will limit the long term exclusion of such individuals from the opportunities offered by uniform secure authentication.

¹⁹⁸ *Tamed snoopers*, www.zn-ag.com/news/2001/en_wiwo_2001_10_11.htm

¹⁹⁹ Jean-Paul Linnartz and Pim Tuyls, *New shielding functions to enhance privacy and prevent misuse of biometric templates*, 4th International conference on Audio- and Video- Based Biometric person Authentication Conference, AVBPA 2003, Surrey (June 2003)

²⁰⁰ N K Ratha *et al*, *Enhancing security and privacy in biometrics-based authentication systems*, IBM Systems Journal **40** (3) 614-634 (2001)

RC/TTL10 RC - TRIALS, TESTING, LEGAL, etc 10: Work is required to develop a framework for the legal admissibility of biometric data. This should build upon the existing procedures for scene of crime fingerprints and handwritten signatures.

5.6 Standardisation activities in biometrics

The wide range of different biometric methods (see section 4), and the ways in which such methods are implemented by the 200+ suppliers, fails to allow for complete standardisation. The templates are defined in proprietary ways with (often secret) algorithms that process the raw images or signals from the biometric sensors into templates which form the basis for future comparisons. It is only in the case of fingerprints that there is a standard approach for the basic building block in many systems. In these systems, the ends of fingerprint ridges or points where a ridge splits into two (*minutiae*) represent key points. Nevertheless, each supplier using this approach will code the minutiae in different ways.

Several years ago, the industry recognised that one of the deterrents to the adoption of biometric methods was the lack of any interoperability between systems. Most of the suppliers of devices and sensors, or the specialist software that was needed to operate a biometric-enabled system, were relatively small and undercapitalised. Even if the companies survived, upgrades might not be compatible and maintenance costs were unpredictable, if the customer was tied to the one supplier. The **BioAPI** initiative was one of a number of application programming interfaces that were proposed in 1998-9 to provide a measure of reassurance. The initial consortium included Compaq (now HP), Microsoft, IBM, Novell and companies that later became Identix and eTrue. (Microsoft continued to partner a small private company in developing a lower (device) level API called BAPI²⁰¹, and this major player has committed to introducing this *de facto* standard in the next version of its operating system.) Intel joined the BioAPI consortium, bringing with it the Human Resources Services extension to the CDSA from the Open Group. Version 1.1 of BioAPI, along with a final reference implementation, was released in March 2001 and approved as an ANSI/INCITS standard 358-2002 in February of 2002.

BioAPI²⁰² allows a common way of communicating between the basic technology of a biometric device and another application. The goal was to support as wide a range of applications while remaining neutral to both vendor and biometric method. It consists of a set of function calls in C together with defined data structures, specific error handling routines and conformance requirements. A number of optional features are included, such as control of the user interface, implementation in client/server mode and data signing and encryption. The data structure of the Biometric Information Record (BIR) - albeit with an opaque template block - is defined as well. Its interoperability with Intel's Common Data Security Architecture (CDSA) allows a more complete security environment to be defined.

The BIR is designed to conform to an already defined standard for the file format containing the biometric template. The emerging **CBEFF** standard (currently renamed as the Common Biometric Exchange Framework Format) had been published originally in March 1999. It describes a set of data elements in the form of a header and biometric data, with the data header containing information such as version number, length of data, type of biometric (and, for example, which finger it relates to), whether or not the data is encrypted, and the domain of applicability (e.g. only for verification). The owner of the specific format and the specific type is coded in the file in a standard way, against a

²⁰¹ BAPI – The biometric standard

<http://www.iosoftware.com/Documents/The%20Biometric%20Standard.pdf>

²⁰² www.bioapi.org

registration with the authority, the IBIA (International Biometric Industry Association). A number of changes have been proposed and an augmented version is currently available in draft form²⁰³. The file format is harmonised with the BioAPI BIR and with the financial industry's X9.84 standard.

A working group in the American Bankers Association produced a standard for the financial services sector that has since been adopted by ANSI, the US national standards body, with work in progress to develop it into an international ISO standard. **X9.84** describes the mechanisms to maintain the confidentiality and integrity of biometric data in transmission and storage, as well as to authenticate the source of such data. It specifies the management of this data throughout its life cycle, the security of the hardware, and its application both to verification and identification of employees and customers as well as to physical and logical access control. The biometric record used in X9.84 is compatible with the CBEFF file structure.

As another example of application specific standards, Intel has issued guidelines for the use of fingerprint sensors in notebook computers and evaluated three silicon sensors against these guidelines²⁰⁴.

Meanwhile, other standards had been under development. For example, ISO's sub-committee **SC17** on Cards and Personal Identification continues to work with the International Civil Aviation Organisation (ICAO) on standards for the airline industry. Another group, **SC27**, on IT security techniques is also working on security testing and evaluation of biometrics. The potential overlap between these two bodies and possible activities under the new biometrics group, **SC37**, was one of the concerns expressed by national bodies that opposed the creation of the new ISO sub-committee on biometrics.

The UK government's Biometric Working Group (**BWG**) was started several years ago to co-ordinate the efforts of individual departments and to progress the development of these methods through research and specific tasks related to the needs of the government community. CESG, the Communications Electronic Security Group, operates this activity with funding from the Office of the eEnvoy.

BWG has supported the UK's National Physical Laboratory in developing its competence as the world's prime testing centre for biometrics, publishing the Best Practices²⁰⁵ guidance for testing and reporting which also forms the basis for a special working group in the new ISO biometrics sub-committee SC37. (Note that the original work that led to the NPL's pre-eminence was the outcome of another European research programme, BIOTEST.) The BWG has also developed the Protection Profile for the security evaluation of biometric devices under the Common Criteria scheme²⁰⁶.

A similar body to the BWG is the US **Biometrics Consortium**. Although it has a larger membership and a wider remit than the BWG, both research and standards-oriented work is undertaken within the various BC working groups. Its six-monthly workshop/conferences are very well attended with detailed technical presentations.

Other more specialised activities are also underway in specific countries, e.g. the **AAMVA** (American Association of Motor Vehicle Administrators) research into a

²⁰³ Fernando Podio *et al*, NIST (National Institute of Standards and Technology), *Revised CBEFF NIST/BC Biometric WG Draft of Common Biometric Exchange Framework Format (CBEFF) Draft NISTIR 6529-A* in internal review. (v7, available to national standards organisations as ISO/IEC JTC1/SC 37 N37)

²⁰⁴ *Biometric User Authentication: Fingerprint Sensor Product Guidelines*
<http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf>
 (15 September 2003)

²⁰⁵ A Mansfield and J Wayman, *Best Practices in Testing and Reporting Performance of Biometric Devices* (V 2.01, August 2002) www.cesg.gov.uk/technology/biometrics

²⁰⁶ <http://www.cesg.gov.uk/technology/biometrics/media/bdpp082.pdf> (Draft Issue 0.82, 5 September 2001)

standard for driving licenses in the USA and Canada, which is investigating the use of biometrics in this *de facto* identity card.

During 2002 there was an ongoing discussion on the benefits of 'fast tracking' certain of the more generic standards at the international level through ISO/IEC, the joint International Standards Organisation and International Electrotechnical Committee²⁰⁷. This resulted in the creation of subcommittee **SC 37**, whose inaugural meeting was held in Orlando, USA in December 2002, with a remit to address four activities:

- APIs, such as the BioAPI
- File formats, such as the augmented version of CBEFF
- Profile development, based upon these two
- Standardisation of biometric templates.

As a result, both BioAPI and CBEFF are being put forward for adoption as standard, and provided that no major objections are received, these should attain the status of a standard in late 2004 (current versions for ballot by national standards bodies are FCD19784 and CD19785, respectively). Work has also commenced on a number of additional standards, among which are Biometric Data Interchange Formats for the images from face, fingerprints and iris recognition (part of the ISO/IEC multi-part standard WD19794) and a standard for biometric testing and reporting (NP19795). Six working groups carry on the work of the sub-committee SC37, with the first meetings held in Ottawa in April 2003 and Rome in September 2003:

- WG1. Harmonized biometric vocabulary
- WG2. Biometric technical interfaces (BioAPI and CBEFF)
- WG3. Biometric data interchange formats
- WG4. Biometric functional architecture and related profiles²⁰⁸
- WG5. Biometric testing and reporting
- WG6. Cross-jurisdictional and societal aspects

The harmonised vocabulary is likely to be incorporated as part of a current standard, ISO 2382.

RC/S1 RC - STANDARDS 1: Interface standards are needed for all aspects of the operation of systems using a biometric. These should be in a form that is easily used by the design community and readily applicable to the variety of applications that are described in this roadmap.

RC/S2 RC - STANDARDS 2: The prime driver of standardisation appears to be early application to border security and towards improvements in the physical security of transportation systems (especially in airports). Will this impact upon the usefulness of such standards in other application areas?

RC/S3 RC - STANDARDS 3: Standards should be appropriate for specific application areas (including the legal and societal context). Work on 'profiles' should be grounded in case studies of existing and proposed systems

²⁰⁷ A preparatory paper on the need to address interoperability in smart card and biometrics was prepared by FhG-SIT and Giesecke & Devrient in the autumn of 2002. Bruno Struif *et al*, *TB 1 - BioNorm: Need for specifications and standardisation to achieve interoperability in the field of smart cards and biometrics*, www.electronic-identity.org (23 October 2002)

²⁰⁸ A standards profile for a specific function (e.g. verification of identity) is a complete collection of references to other standards with the options in those standards defined specifically for the function.

RC/S4 RC - STANDARDS 4: Work to support the standards activities in testing, validating, accrediting and accepting deployed systems at the hardware, algorithm and user acceptance levels.

RC/S5 RC - STANDARDS 5: Although a study group (SG6) has been formed to examine legal and societal aspects of standardisation, historically, standards bodies have been reluctant to develop international standards in this area. At present, the usefulness (and acceptability to some national bodies) of such a standard remains to be proven.

RC/S6 RC - STANDARDS 6: Relatively few players are taking an active role in the development of standards, even though standardisation initiatives are being accelerated to meet the requirements of border control applications. Other national bodies (including many in the EU) are unaware of the implications of such standards. Sharing of knowledge should be encouraged through the formation of a European special interest group.

6. The immediate outlook for the application of biometrics

6.1 Overview

For many years consultants have predicted the imminent take-off of the market for biometrics, through the acceptance of these technologies as a cornerstone of improved security or more convenient access to personalised services. For many reasons this take-off has failed to materialise. These have included the lack of an objective valuation of the resources that needed to be protected by advanced security mechanisms. Even when such data was available (e.g. for fraudulent credit card transactions), deployment and operational costs far outweighed the savings that could be made. For a long time, the industry attempted to convince everyone of its maturity, in spite of the slow progress to standardisation, the unresolved doubts on privacy and the generally limited capital base of the suppliers of core technology. It was also recognised that the government sector (which includes in Europe, most of the education and health sectors and much of the transport infrastructure) would probably have to give the lead, since - just as the biometrics industry was beginning to address these criticisms - the retrenchment in IT spending in 2000-3 placed a halt on major infrastructural expenditure. The growth in identity theft in the USA appeared to be insufficient to galvanise the private sector into addressing the need for stronger authentication. Other reasons of a more general nature are discussed in Section 7.1.

It was only the response to the threat of terrorism posed by the open borders in the USA that appeared to guarantee a future income stream to biometric equipment suppliers, even though revenues from this group of applications will only start to flow towards the end of the period under review in this section, 2003-5. Furthermore, as the result of the Enhanced Border Security Act²⁰⁹, a requirement has been placed on the countries of the European Union to have a biometric-enabled travel document programme in place by October 2004 for those travellers visiting the USA. In parallel, a number of European countries (among which are the Netherlands, the UK and Germany) have decided to improve the security of their travel documents through the possible use of a biometric. In the UK, this coincided with a consultation exercise on a nationwide Entitlement Card that would provide some of the functions of a national identity card. Among the options for this card (and indeed the issue of future key documents such as the passport and driving licence) was a national biometric database that would ensure the unique identity of every citizen²¹⁰.

It remains to be seen what the impact of these government activities will be on the private sector. It is certain that the impetus that it has given to standards work and to the improvement in secure and robust biometric sensors will feed through into a re-appraisal of the opportunities for their more widespread use.

Status and growth of the market for biometrics

Throughout 2002, a number of reports had been produced that attempt to forecast the future revenues in the biometric sector through to 2007 and beyond. Some have sufficient detail to enable an assessment to be made of the market in Europe. The table below summarises the key figures. It is immediately clear that there is considerable confusion as to the meaning of the 'biometrics industry'. Does it include revenues from the very large-scale AFIS systems which have been dominated by a few very large companies and which represents a market that dwarfs the other biometric applications? Some forecasters include the revenues of system integrators; some do not. The reliability of forecasts in the

²⁰⁹ Enhanced Border Security and Visa Entry Reform Act (14 May 2002)

²¹⁰ Note that such a database would be unlikely to be adopted in other EU countries such as Germany.

longer term is also in doubt, since decisions on many of the opportunities such as the UK's national biometric database have not yet been made. We have, therefore, chosen to limit the analysis of the near term future to 2005.

2002			2005		
	World	Europe	World	Europe	
Jan 02 ²¹¹		\$70m		\$240m	Includes logical access, civil ID and criminal justice applications
April 02 ²¹²	\$200m		\$1.5bn	\$500m	Excludes integrator revenues, end user purchases and AFIS
Summer 02 ²¹³	\$600m		\$2.2bn	(\$200m) ²¹⁴	Includes AFIS, civil ID and middleware
Autumn 02 ²¹⁵	\$260m				
Dec 02 ²¹⁶	\$110m		\$476m		'moderate forecast'
April 03 ²¹⁷	\$946m				Includes AFIS, civil ID

Table: Forecast revenues for biometrics 2002-2005 as reported in 2002-3

IBG's analysis of the predicted market share of the individual technologies shows surprisingly little change during the period 2001 to 2003 (Note that AFIS systems are excluded in their predictions)²¹⁸:

	2001 share	2003 share	2002	2002
Fingerprint and finger-scanning	49	52	42	38
Facial recognition	15	11	13	17
Hand geometry	10	10	12	18
Iris recognition	6	7	11	17
Speaker verification	4	4	5	3
Dynamic signature systems	3	2	6	6
Middleware	12	12	10	

Table: Market share of biometric technologies (2001/2003 from IBG compared with data from two other consultants' reports)

The additional columns list the distribution of revenues in 2002 according to two other consultants' reports.

²¹¹ IDC, *For your eyes only - Biometrics and hardware authentication in Europe* (January 2002)

²¹² R Norton, *Where will Biometric Revenues grow from 2002 to 2006?*, IBIA Biometrics Advocacy Report, IV (6) 5 April 2002

²¹³ International Biometrics Group, *The future of biometrics: trends to 2004*, Biometrics 2002 conference and exhibition (London, 6 November 2002, based upon the IBG's *Biometric market report 2003-2007*)

²¹⁴ Europe and Australia will account for \$190m (13% of total) in 2004

²¹⁵ Elsevier Advanced Technology, *The biometric industry report: forecast and analysis to 2006*, (review in *Biometric Technology Today*, January 2003)

²¹⁶ Allied Business Intelligence, *Biometric Systems: Worldwide deployments, market drivers and major players* (2002)

²¹⁷ Business Communications Company, *RG-276 The global biometrics market*, predicting an average annual growth rate of nearly 30% to 2007 (\$3.4bn; compare IBG's forecast of \$4bn by the same date) www.bccresearch.com/editors/RG-276.html

²¹⁸ IDC quotes global figures of fingerprint recognition (44%); facial recognition (14%); speaker verification (10%); iris recognition (8%); other (24%). Emma Nash, *Pay attention, 007: biometrics has some real-world potential*, *Computing* (7 August 2003), p.22

Biometrics supporting services

The categorisation of application areas shown in the table below attempts to avoid double counting, and illustrates the diversity of opportunities that could exploit the specific characteristics of biometric technologies. In the succeeding sections, we examine current initiatives and future trends in a selection of the most promising domains. These have also been chosen to demonstrate the variety of drivers that will impact upon the adoption of new solutions using biometrics:

- the impact of decisions taken outside of the European Union (improvements in the security of air travel);
- the challenge of integration of many diverse and complex services in the Internet age provided by a single supplier (government-to-citizen services);
- fragmentation of responsibility for the development of new security solutions in a single sector (physical and electronic service security in the health sector);
- cost-benefit, security and robustness considerations (security of services in the financial sector).

Sector			Comments
Government	Fundamental identify services	National ID card Passport Birth and death registration Social security card	Significant work is underway in the UK and the Netherlands governments in respect of passport and national cards (UK Passport Service committed to use in 2005 onwards). Use of biometrics in welfare benefit payment has been a long-standing feature of some states programmes in the USA.
	Government to Citizen services	Registration of home, change of address Driving licence Asylum seekers card Work permit Immigration visas Tax payment Wills & testaments Voting - registration e-Voting Physical access to buildings	Governments in Europe are committed to an increase in the proportion of services that are directly accessible electronically (most cite a substantial portion by 2005). In the UK, possible use of a national biometric database in the issue of driving licenses after 2007
	Health	Medical card Primary care Hospital services Physical security of hospitals and institutions Pharmaceutical testing records Databases - data protection & integrity Integrity and sourcing of food Support for the disabled	
	Education	Examination and tests References Child protection register Physical security in buildings	Iris and fingerprint recognition systems have been introduced into a few UK schools for library book control and meal payments.

	Criminal Justice	AFIS Criminal records Prisons, probation, tagging Identity of officials Personal weapon control Surveillance of public spaces	Extension of the AFIS systems to other biometrics: palmprints and facial images. UK is developing a roadmap for future use of biometrics in this sector. UK's use of face recognition in CCTV cameras in Newham is likely to be extended.
	Defence	'Friend or foe' on battlefield ID cards Weapon control Tracking human activities on ground	Extension of the US Department of Defense smart card to include a biometric.
	Transport	Cross-border travel Security of hubs (airport, stations) Security of access to vehicles (trucks, planes) Passenger-baggage reconciliation Ticket control Alert for previously convicted disruptive passengers on flights (International) driving licence	Numerous trials of face, fingerprint and iris systems. Main driver will be the requirements of the US for biometric identity checks at borders from 2004 onwards. Use of fingerprint security for airport staff at London's City airport.
	Critical infrastructures	Logistics Food, water, sewerage, fuel, electricity, telecomms networks	TWIC programme for all workers in transport sector in the US (12 -15 million) envisages the use of biometric authentication.
Internal organisations	Physical access control	Access to buildings Time and attendance Single cash and ID card	Time and attendance is a large market for biometrics in the USA
	Process flow	Logical access and accountability	
	Databases	HR and customer databases - data protection and integrity	
	CRM	Identifying customers at call centres	
	Logical access	Email and IT for business processes	
	Background checks	Search for previous criminal convictions – under mandatory schemes	
Manufacturing	Access control	To specific machines and processes	
Financial services	Personal	Opening and moving accounts Aggregation of accounts Electronic (web) transactions Insurance	
	Point of sale	Credit and debit cards	Relatively little activity currently. In the UK, introduction of PIN needs to be completed first.
	Back office	Accountability of transaction Interbank transfers Dealer desks	
Leisure services	Age-limited services	Tobacco, alcohol, TV and video and Internet	
	Removal of banned or excluded people	Casinos Night clubs Football hooligans	
	Privileged services	Frequent users (air miles, loyalty cards) Airport lounges 'All inclusive' resorts Gyms and fitness centres Digital Rights Management (originating or using copyright material) Season tickets (train, football, theme parks)	
	Specific users only	Leasing/lending valuable artworks Dating services	
	Service sharing	Car personalisation (rental and family) Personalisation of PC and TV settings in a family	

	Hotels	Meals, rooms, gym: payment and personalisation	
Home security	Physical access	Replacement of keys on doors	
	Theft protection	Personalisation of products and services	
Telecomms	Theft protection	Mobile and fixed phone authentication	

Table: Selection of services that could make use of biometric technologies

6.2 Biometrics applied to identity and identity documents

For many governments, the most significant element in their relationship with citizens is the establishing of a unique and usable identity. From registration at birth, to issue of identity cards, social security and health cards and passports, through to registration at death, a stable and unalterable identity for each person is an underlying requirement for such a relationship. It is the key to operation of an efficient system of law and order, to the collection of taxes and distribution of benefits, and to the re-entry of citizens to their home country. Most governments, even in the European Union, still have distributed identity systems, resulting in the absence of a coherent single view across all their services. With their commitment to electronic delivery of services, it is likely that governments will want to unify these systems. Inevitably, this will impact on commercially delivered services, through the blurring of the boundaries between the public and private sectors, and the use of more reliable identities and services developed by the state.

More secure identities are likely to benefit the individual through efficiencies in the operation of government and in the reduction of identity fraud (see Section 6.5). There are, however, considerable hazards in maintaining aggregated databases, even if they operated under the safeguards of the European privacy and data protection regime. Not only would such databases be tempting targets both for criminals in each state, and entities outside of the country, the freedom of action for individuals could be reduced from that enjoyed currently (See Section 1.2 for a further discussion of the issues). There are many legitimate reasons for using multiple identities, and government agencies need to recognise the arguments for proportionality in their dealings with their citizens. In many instances, the option for anonymity in the use of services is questioned by authorities. The threat of terrorism has even legitimised the American concept of TIA - Terrorist (previously Total) Information Awareness - the nation-wide mining of all electronically collected data in an effort to track suspicious activity. The extension of such measures to other aims of governments, such as the reduction of the 'black economy', is an obvious example of 'function creep', even though the side-effects of these actions could be socially unpredictable and destabilising.

National identification schemes for governments are more complex than they appear to many naïve commentators. Even in the EU, there is a wide diversity of approaches to the issuance and operation of documents and identification numbers²¹⁹, reflecting the custom and practice in the member states before the formation of the Union. For example, a universal personal number is only used in some countries; there are no identity cards in a

²¹⁹ editors ARTTIC, *Electronic Identity White Paper*, E-ID White Paper, part of the eEurope Smart Card Charter and initiative (January 2003); and B&L Management Consulting GmbH, *Study on the deployment and interoperability of electronic and biometric authentication and identification*, Draft Final Report for the European Commission (June 2003), and recommendations from the Brussels Workshop (3 April 2003). Porvoo EID Group, *Report on Seminar on Interoperable European Electronic ID/Public Service cards*, (Dublin, 20-21 November 2002). For a recent compilation of national identity schemes worldwide, see chair Joe Fontana, *A national identity card for Canada? Report of the standing committee on citizenship and immigration*, <http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06-e.htm> (October 2003)

few states; and depending on where you are, identity cards may be required to be carried on the person at all times; registration authorities may be centralised or delegated to local municipalities.

The main options for modern national identification schemes include:

- A universal single identifier, usually in the form of a serially allocated number
- A database entry linked to identifier, recording either permanent information (date of birth, gender, identity of parents) or including variable information such as address.
- A paper document recording the birth of the individual, with date of birth, gender and parental details.
- An identity card, issued at birth or at a specific age, which may record overtly or in a machine readable form only, information such as the universal identifier and some or all of the information in the database.
- An identity card with electronic functionality, such as digital certificates for use in transactions that make use of PKI (Public Key Encryption) security technologies
- An identity card with or without electronic functionality that stores a biometric template or image for comparison of the identity of the principal with the person presenting the card.
- A social security or health card, specifically issued for the respective purposes, but with some use as an identification document.
- A machine readable travel document (most commonly, a citizen's passport) issued in formats defined by ICAO²²⁰
- A driving licence. Although issued for a specific purpose, it is often used as an identification document, especially in the US.

As the move towards e-government gains momentum, proposals for a new range of identity cards with electronic functionality have resulted. The most eagerly anticipated was the Finnish PKI card; however, the take-up has been somewhat disappointing (only 10,000 issued by April 2003) at a cost of 29 euros and validity of only three years. A larger acceptance has been seen in the Estonian card, of which more than 130,000 were issued in its first year of operation. The new Italian card has the option of fingerprint encoding²²¹ while the Belgian government commenced the issue of such cards in April 2003 at a cost of approximately 10 euro. Interoperability of these electronic cards has been examined in a White Paper from the Finnish Population Registration Centre²²².

In the move towards more secure systems, suppliers of database and biometric solutions have undoubtedly skewed the debate in favour of their commercial aims with over-simplified scenarios. Increasingly, however, there is evidence of more careful analysis of the feasibility of such schemes, the cost (both in the initial deployment, as well as the on-going enrolment and maintenance), the extent of the benefits to stakeholders, etc.²²³ The debate needs to be conducted with a recognition of the numerous options, and the implications for the convenience and protection of individuals, as well as for interoperability within a state and between states both in the EU and world-wide.

Biometric methods are viewed as critical components in many of the proposals, with face, iris and fingerprint recognition technologies particularly evident in many of the proposals and trial implementations. At present, no countries in Europe have a full biometric-enabled identification document (although Spanish cards store a fingerprint image). Outside of Europe, there have been a number of deployments and a number of others have been announced. Examples include:

²²⁰ International Civil Aviation Organisation

²²¹ Mario Gentili, *Italian electronic identity card - principle and architecture*, Proc of the 27th VLDB conference, Rome (2001)

²²² available at project EUCLID's site: www.electronic-identity.org

²²³ Thien-Loc Nguyen, *National Identification Systems*, MSc thesis, Massachusetts Institute of Technology (June 2003), at theory.lcs.mit.edu/~cis/theses/nguyentl-masters.ps; and Computer Science and Telecommunications Board, National Research Council, *Ids - Not that easy: Questions about nationwide identity systems*, National Academy Press (2001)

- Brunei (ultimate use 400,000, started July 2000, 8k smart card with two thumbprint templates)
- Hong Kong (to start in July 2003 using thumbprints)
- Macau's *Citizen Card* with dual fingerprint identification (540,000 people)
- Malaysian MyKad identity cards (3 million in circulation in January 2003) and passports (the latter with a pair of thumbprints coded at 500 bytes per print)²²⁴
- Mauritania (1.1m citizens, fingerprints)
- Nigeria (60m fingerprint registrations)
- Oman (to start in November 2003 with a fingerprint verifier)
- Peru (13m people enrolled, fingerprints, stored as 2D bar code)
- Uganda (face recognition)

However, it is clear that if the underlying register of individuals has been compromised, the addition of a biometric identifier to the existing range of identity documents based upon this register will only compound the problems. Hence, any data cleansing should be done before the introduction of new identity cards with biometric authentication. At the same time, the political decision is required as to how widespread will be the sharing of such primary data between departments in a government. In most EU countries, this will be limited by law. In others, the need to reduce the possibilities of widespread identity theft may lead to a compromise that is agreed with the citizen. In such cases, the use of technical and procedural measures to limit sharing in instances where it is not permitted may reassure some individuals. Nevertheless, an open debate is needed, with the recognition that identity databases will be very attractive targets for criminal activity. The need to provide for change of identity in legitimate cases, for example such as in witness protection programmes, has to be borne in mind in any designs.

Undoubtedly the main driver for the more widespread use of biometrics in travel documents in the near future has been the decision of the US Congress to mandate their inclusion i) in visas for travellers to the US and ii) in passports for any country currently exempted under the Visa Waiver programme²²⁵. Although the legislation appears to require such countries to have a *programme* in place to issue such passports from October 2004, certain statements from senior US officials seem to indicate that *any* passports issued after that date must have biometric identifier(s). Industry sources believe that this is an unattainable goal. The simultaneous revision of the passports of over 20 major countries, with new equipment needed to securely seal in the silicon integrated circuit, the setting up of Public Key Infrastructures to secure the electronic data into the chip, and testing the new range of passports together with the integration of processes of biometric enrolment and issue of passports seems unlikely to be completed within this timescale. By mid July 2003, there had still been no public statement of the biometrics to be used, nor any details of the technical specifications. Indeed, at this time, the ISO standards organisation were still discussing the standards for formats of the exchange of biometric data and the APIs and file formats that would be used.

The leading EU countries involved in the development of biometric methods in identity and travel documents have been the UK, the Netherlands, Germany and Italy. In the summer of 2002, the Home Office in the UK issued a consultation document on 'Entitlement Cards', strongly linking the proposal for a new type of card to the increasing incidence of identity fraud²²⁶. The consultation, which closed at the end of January 2003, focussed strongly on the use of biometrics in reducing the opportunity for multiple applications for identification documents. In the absence of pre-existing identity cards, a national database of individuals using one or more biometric methods would ensure that anyone attempting to apply for a second passport or driving licence would be identified. In time, the proposal envisaged that every person above the age of 16 would be registered, and those who did not require a driving licence or passport would be issued with an

²²⁴ Eddy Cheah, *The new Malaysian smart passport*, Keesing's Journal of Documents issue 1 (2003)

²²⁵ US Congress, *Enhanced Border Security and Visa Entry Reform Act* (2002)

²²⁶ *Entitlement Cards and Identity Fraud: A Consultation*, (Home Office, July 2002)

Entitlement Card. The results of the consultation are expected soon, and plans for trialling of the various options are underway. The response of the UK's Information Commissioner highlighted the numerous options that were offered in the paper, making it difficult for him to assess the extent to which the benefits of such a unique plan would 'outweigh the risks to privacy, human rights and social values'²²⁷. He laid particular stress on fitness for the range of identified purposes; he notes the need for clearer proposals with safeguards in relation to the quality, amount and adequacy of data; and recommended that the database underlying the proposal store the minimum amount of data necessary to allow the system to work correctly. In a separate move, the Home Office has committed itself to the issue of supplementary passport cards with a biometric identifier²²⁸.

Additionally, the UK has had considerable experience in the operation of an Asylum Seeker's Card. For over 18 months, all asylum seekers are required to register for a smart card and provide a set of fingerprints using a liveness electronic capture system. These are stored in a database. Individuals who attempt to re-enter the UK as asylum seekers after their claims have been dismissed are caught by immigration officers equipped with fingerprint readers at the ports of entry.

The Netherlands has also been active in this area, hosting the first European conference to explore the options for the application of biometrics in travel documents²²⁹. Having completely updated its range of passports, identity cards and emergency issue identity documents in October 2001, the aim of the Dutch authorities is to introduce usable and secure biometric authentication to reduce the incidence of 'look alike fraud'. It has trialled a number of applications using biometrics and the Ministry of Justice is rolling out a PKI-based electronic card to its 40,000 employees using smart card and RFID technology. Fingerprint biometrics with the match of template to image presented at the reader taking place on the card itself.

France's standardisation committee, AFNOR, has a specialist working committee on biometrics, CN FTS/GE1. By examining the opportunities for its use by the French government and other large organisations, it has recommended that fingerprint authentication is used on the grounds of

- Ready availability of cost-effective terminal equipment for fingerprint capture
- Individual granularity is possible under 1:N comparison
- Storage of minutiae using the template defined by AAMVA (Northern American driving licence organisation) is possible using either 2-dimensional barcodes or smart cards, since the required storage amounts to 1 kbyte per fingerprint²³⁰.

For a number of years, ICAO has been examining the options for a standard biometric in passports and other machine readable documents. On the basis of these studies²³¹, it has recently recommended that the primary identifier should be a standardised digitally stored

²²⁷ *Entitlement Cards and Identity Fraud: the Information Commissioner's Response to the Government Consultation Paper*, (January 2003) www.dataprotection.gov.uk See also the comments by George Radwanski, Privacy Commissioner of Canada against the introduction of a national identity card in that country, in his statement to the Canadian House of commons on 18 March 2003 at www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp

²²⁸ UK Passport Service, *Corporate and Business Plans 2003-8*, (2003) envisages the completion of an implementation plan and business case for biometrics in passports by March 2004. The Passport Card, which is suggested to be used for travel within the EU, is likely to go ahead beforehand, but will only use digitised facial images.

²²⁹ Ministry of the Interior and Kingdom Relations, *European conference for issuing authorities of travel documents: exploring the use of biometrics in travel documents*, The Hague (June 2002)

²³⁰ AFNOR document CN FTS N39, *Recommendation of the AFNOR Committee CN FTS/GE1 regarding biometric application to different organisation, like French government and other AFNOR committees*, statement for consideration by the BIOVISION consortium (3 June 2003)

²³¹ *Executive Summary: Technical Report on ICAO work on selection and testing of a biometric technology for identity confirmation with machine readable travel documents (MRTDs)*, www.icao.int/en/atb/fal/mrtd/biometric_tech.htm

facial image in support of facial recognition technologies. Furthermore, it recognises that countries can use 'standardised digitally stored fingerprint and iris images as additional globally interoperable biometrics'. Countries are encouraged to store this type of data on 32 kbyte contactless smart cards²³². These recommendations recognise that there are no standard templates for these technologies, and that mandating of proprietary solutions would not be acceptable. In view of the reduction of the price of higher capacity devices, some ICAO delegates would have preferred the use of 512kbyte storage media (either IC or optical memory cards).

The ISO biometrics sub-committee SC37 has begun the standardisation process for the interchange of such biometric images with the text of committee drafts ISO/IEC 19794-5 (facial image format for data interchange), 19794-4 (finger image based interchange format) and 19794-6 (iris format for data interchange) being circulated for comment by national bodies. Comments on working drafts were reviewed at the meeting of ISO/IEC SC 37/SG3 in Rome in early September 2003 and will be further developed in the run up to the February 2004 meeting in Sydney.

There are other organisations also considering more secure identity documents. The International Labour Office in Geneva is reviewing Convention 108 for seafarer's national identity documents. In its recent report, it discusses the results of its consultations with governments²³³. Russia, China and Japan considered that the use of biometrics was problematic. The UK and the US supported its inclusion, although the US wanted the template, and not the 'biometric per se', to be stored for reasons of privacy. The Netherlands stated that, *if* a biometric were to be used, it should be in accordance with ICAO standards, while Portugal considered the use of fingerprints to be essential. The first national office to introduce this type of document could be the Liberian International Ship and Corporate Registry, who propose to store fingerprints on the identity cards of seamen in ships flying the Liberian flag. Recently, the ILO has moved towards the use of a template of a fingerprint as the biometric of choice.

Clearly, securing identity documents (especially for travel) will be an early large-scale application of biometrics, and successful deployments could pave the way for more widespread use both by governments and private enterprise. Much of the detail of the operation of the biometric component in these systems remains to be determined. Although data interchange formats for biometric images are being proposed and a standard for the interchange of minutiae in fingerprints is also under consideration (ISO/IEC 19794-2), how these will be applied is still to be resolved. For example, the specific case of a national biometric database envisaged under the UK's Entitlement Card paper, proposals appear to require that every citizen is uniquely identified and checked against the biometric data of all other citizens. If the level of alarms due to false matches begins to rise, substantial human intervention will be required. Few biometric methods can address the required levels of accuracy. With presently available commercial implementations, facial recognition falls many orders of magnitude short of the required performance. In contrast, theoretical modelling of the operation of iris recognition systems together with a recent analysis of many groups of tests suggests that this method could be used successfully. However, deployments of this biometric to date have been relatively small (20,000 maximum population size). More detailed studies will be required to determine the proportion of the population unable to use the system, either through failure to enrol successfully, or through problems in day-to-day operation. This leaves fingerprint identification as the most likely contender, in spite of privacy concerns and the unease amongst certain sections in society about the possible crossover between criminal and civil AFIS systems. Experience from the many instances of quasi-automated criminal AFIS systems (notably the near 5m UK records and the FBI's 45m IAFIS system in the US) can lead to more confident predictions about the performance of a civil system

²³² Tom Kinneging, *ICAO opts in favour of non-contact chip technology*, Keesing's Journal of Documents Issue 1 pp 3-6 (2003)

²³³ International Labour Office, *Report VII (1): Improved security of seafarers' identification* (2003). Page 12 summarises the responses of governments to proposals for biometrics.

using minutiae. The minimum number of fingerprints required for a given level of false matches can be determined from consideration of such data.

In the USA, NIST (the National Institute of Science and Technology), was tasked with determining the minimum requirements for a system that would address the demands of the system envisaged under the USA Patriot Act (2001) and the Enhanced Border Security and Visa Entry Reform Act (2002)²³⁴. Taken together these translate to:

- Denial of a visa for a foreign national identified as having a criminal (presence on the FBI's IAFIS 45m database) or being on a 'watch list'
- Verification that a person who has been issued with the visa matches the identity of the person at the entry point into the USA

The conclusion of this study is that for the timescale envisaged, only facial and fingerprint systems are commercially available with the requisite size of databases of images for testing the performance of systems. The first requirement, identification against the total criminal database is a major challenge. Not only did existing technology demonstrate a 2% failure to acquire rate, single finger performance on identification is inadequate. The authors of the report suggest 4 fingerprints would be a minimum requirement (thumb and index fingers of both hands), although 6 would be preferable, especially for women who consistently show a higher proportion of poor images. The implication of the NIST findings (not explicitly stated) is that a full 'tenprint' set obtained by a livescan electronic hardware is necessary, with a backup of a facial recognition system. Comparison of the performance of facial and fingerprint identification for different database sizes was quoted as follows:

Gallery size	Single fingerprint recognition rate	Facial recognition rate
100		90%
500	95%	
1000		83%
10,000	90%	77%
100,000	86%	

The recommendation for the second requirement, for verification at the port of entry, is for a dual biometric system using two fingerprint images (not a proprietary template using minutiae) together with a facial image. At less than 10 kilobytes per image, the verification of visa identities would require a 32K IC card. This system could be compared with the Basel project at Israeli-Palestinian border crossings: face recognition and hand geometry biometrics have been combined on an 8K contactless smart card for verification of identity of the 120,000 daily workers who used to travel between the two countries.

With the 10 new states joining the EU in 2004, the opportunities for the introduction and use of biometrically-secured identity documents could be a major source of revenue for suppliers and integrators. In 2000, the population of the 25 states was over 450m people. What proportion of this population would be covered remains to be determined. The UK government for example, has consulted on a proposal to cover everyone over the age of 16 (51 million) over a 6 year period, together with a number of other non-casual visitors to the UK. If accepted, the deployment would be considerably advanced by the end of 2010, the time horizon of this report²³⁵. We note that no other member state has made

²³⁴ NIST, *NIST standards for biometric accuracy, tamper resistance and interoperability*, (13 November 2002). The facial recognition results build on the FRVT2002 results summarised in 4.1.4 and the fingerprint performance for AFIS-type systems derives from a study: Charles Wilson *et al*, *Studies of fingerprint matching using the NIST Verification Test Bed (VTS)*, NISTIR 7020, NIST (7 July 2003)

²³⁵ The Home Secretary has indicated that he intends to put forward these proposals for approval by the Cabinet in the summer of 2003.

corresponding proposals. However, we would expect that countries with advanced electronic identity cards (e.g. Finland and Estonia) would consider the use of biometrics, especially if the British example were seen to be on a successful path. The new Italian identity card has provision for the inclusion of a biometric, and it is understood that the Spanish government is actively considering a new form of identity card. Netherlands has issued a commercial call for information on the use of biometrics. The German authorities have paid particular attention to the possibilities offered by decentralised use of biometrics in passports, with specific reference to ways in which facial recognition could be used. As we discuss in the following section, soon after 2005, travellers to the US will require some form of biometric, either in the passport itself, or in a document issued in conjunction with the passport (in 2002, there were nearly 8.3m visitors from Western Europe to the US)²³⁶. Although, political decisions will dominate the date at which the take-up of biometrics starts to increase significantly, there seems to be little doubt that in the second half of the decade, millions of European citizens will start to use these technologies.

The introduction of a biometric-enabled identity card requires considerable preparatory work. In particular, the purpose of the biometric element should be clarified from the start. Is it to establish a single unique identity, or is it to ensure that a user has no previous criminal convictions, or to assist in the authentication of identity when government or commercial services are used - or a mix of each of these? The choice of biometric method will be determined by the performance requirements, acceptability by citizens, security requirements, etc. It is instructive to compare the performance of the largest current biometric systems - the AFIS systems used by police forces throughout the world. In particular, the FBI's IAFIS 10-print matching system has been characterised in some detail²³⁷. The majority of electronic checks of the 45 million records were completed in between 4 and 7 minutes (depending on civilian or criminal requirements), although considerable numbers took longer than 2 hours. The FTE (Failure to Enrol) rate is about 0.5% for criminal searches and 2.5% for civilian background searches.

Clearly biometric systems with improved performance may be required. Should this be the case, the consequent delay in launching a system will be evident. The Diagrammatic Form of a Roadmap (end page of this document) illustrates the timescales based upon the best estimates from the industry. Had requirements for the deployment been clearly articulated by mid 2003, a supplier with a development programme underway already could deliver a product, P2, in time for trials starting in 2005. Legislation may be required to permit some aspects of operation of such a system, and this should be feasible in parallel with trialing and prototyping. Procurement is estimated at approximately one year, ready for initial deployment at the beginning of 2008. Supplier S2, without a programme in place, will take longer to develop a solution and may miss the deadline. If, however, governments demand a more radical solution requiring research (taken to be a three-year project), the message of this analysis is that deployment is unlikely before 2010. Unexpected changes in the drivers for development (or inhibitors, e.g. resistance by special interest groups) will modify the start date for deployments.

In the light of this background survey, it is instructive to review the recommendations of the Brussels workshop of experts called to discuss the results of the preliminary report on electronic and biometric authentication and identification²³⁸:

²³⁶ GAO, *Implications of Eliminating the Visa Waiver Program*, <http://www.gao.gov/new.items/d0338.pdf> (November 2002) page 14. In a survey carried out in October 2002, only 3 of the EU countries stated that they would be able to meet these obligations by the requisite date.

²³⁷ GAO, *Technology Assessment: using biometrics for border security*, GAO-03-174, page 149

²³⁸ B&L Management Consulting GmbH, *Study on the deployment and interoperability of electronic and biometric authentication and identification: Recommendations from the Brussels Workshop* (3 April 2003); the list of recommendations are the Editor's summary of a more comprehensive paper.

- Better communication of the issues surrounding user acceptance of these new technologies, to decision makers in governments and to solution providers, while providing transparency and reassurance to the end users.
- Development of use cases to demonstrate interoperability in border control, document handling (both in private and public sectors) and in access to electronic services on an international basis.
- Development of a framework for interoperability
- Undertaking several large scale independent operational tests using biometrics within the framework for interoperability.
- Consideration of how multiple biometrics can be used in this type of large scale system.
- Encouraging vendors towards a degree of standardisation in biometric templates, but recognising that in the short term, the image itself has to be used in applications where interoperability is required.
- Development of guidelines for the best possible image capture during enrolment
- Extension of BioAPI to include security aspects and XML-based standards
- Proactive communication of the existing legal and privacy requirements to those who are unaware of their significance. Although these do not specifically address biometrics, there appears to be no need to make changes to the legal framework (with the possible exception of a directive on authentication in general). However, a Code of Conduct and Best Practices are currently under development and these should be widely disseminated once completed.
- The evidential value of biometrics in law needs to be improved²³⁹, with further independent evaluations, such as those under the Common Criteria.
- Development of business cases for electronic and biometric identification that demonstrate their legal viability

Some time into the future, a biometric-enabled identity could form the basis of a cashless society, based upon the use of the biometric alone. Although its technical feasibility can be visualised, for many citizens, such a technological solution would be viewed with concern - at least in today's environment. The R&D projects which have been undertaken (examples of which are listed in Appendix 3) point to exciting possibilities, but without a corresponding understanding of the societal changes that would either encourage their use or the problems that need to be resolved, such futuristic designs may remain firmly in the realm of science fiction.

Nevertheless, there are many organisations and individuals that have concerns with the introduction of identity cards, and comments have been made that, although citizens are in general in favour of their introduction (or at least not actively against their deployment), once the cost and legal implications for the individual citizen are clarified, the opposition to their use can increase substantially²⁴⁰.

6.3 Secure air travel through the use of biometrics

The tourist industry is one of the largest in the world, contributing approximately 10% of the world's GDP. The World Travel and Tourism Council estimates that in 2003, travel and tourism in the EU will account for over 7m jobs (4.4% of total employment), with an

²³⁹ Work on development of the fundamental scientific data on fingerprint uniqueness is being undertaken as part of project TSWG Task T-1595 *Statistical Analysis of Forensic Ridge Matching Criteria*.

²⁴⁰ see chair Joe Fontana, *A national identity card for Canada? Report of the standing committee on citizenship and immigration*, <http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06-e.htm> (October 2003)

indirect impact on a further 13m jobs. Over the next ten years, it is forecast to increase at a compound growth rate of 4.2%²⁴¹.

Although by no means the greatest component of tourism, air travel is seen by governments as the highest priority for improved security in the wake of the events of September 11th. However, any new security measures will inevitably impact on the traveller, the airport authority and the airline unless these are introduced in ways that acknowledge the realities of current processes and minimise the additional costs and inconveniences that will result. In spite of occasional reduction due to war and terrorist incidents, air travel has shown a continuing strong growth rate that is scheduled to continue into the foreseeable future. Over 1980-2000, passenger numbers increased at nearly 6% pa, with the number of passenger kilometres increasing even faster.

Biometric authentication can play a role in increasing the security in travel in a number of ways:

- Restriction of physical access to parts of airports, railway stations, etc to those who have been vetted and then authorised to enter such areas (An example is the recent announcement of fingerprint authentication of all airport workers at the City airport in London)
- Authentication of pilots, drivers of trains, buses and trucks, stewards and those involved in supporting operations such as air traffic control.
- Issue of tamper-resistant visas to immigrants and visitors in their home countries, and authentication at border entry and exit.
- Authentication of holders of passports at ports of entry and exit (as well as ticket purchase if required)
- Operation of watch lists for specific individuals who may be travelling with false documentation or under aliases.
- Reconciliation of baggage with passengers at boarding, in transit and on arrival
- Tracking of individuals and groups of people at airports and railway stations, and observance of unusual activities.

This section aims to illustrate the complexities in deployment of biometric solutions, bearing in mind some of the elements from the longer term scenarios developed in section 3.5. (Note that this aspect of the Roadmap was completed before the significance of the US proposals for tighter control on travel was recognised). A proposal to introduce a biometric on a passport as part of a package of security measures can have implications on operations far removed from those envisaged by politicians in framing laws.

Aims and objectives

The principal objective may be to reduce the likelihood of terrorists entering the destination country of a flight, or to limit the probability of hijackers seizing control of aircraft. However, some politicians may decide that this is an opportunity to tighten up on immigration (people overstaying their allowed time in the country) and on prospective asylum seekers. For others, it may be the time to consider adding other criminals to watch lists, perhaps even catching up with those travellers who failed to pay their taxes or parking fines. There will always be the aim of reducing costs, especially if people are employed in large numbers, whether by airlines, airport operators or government agencies. Finally, the traveller should not be forgotten; air travel is particularly stressful and making the process more convenient could be a useful bonus.

Decisions

²⁴¹ World Travel and Tourism Council, *European Union travel and tourism. A world of opportunity*, (2003, based upon assumptions of either no war in Iraq or a quick, decisive and contained military action)

Balancing all these objectives is not a simple matter, and decisions are made by key players that may act to the detriment of other stakeholders. Of course, supplier and system integrators can lobby for their individual solutions, which may be incompatible with those in other airports or countries, but which may be adopted because laws are framed in their favour. Once the high level decisions are taken, implementation will require adjustment of these aims, while the day-to-day operations are left in the hands of the frontline managers, especially in the early stages of a deployment. Responsibility for data collected, checked, added to and passed onto another actor will move back and forth between the various players, with each message having to be delivered securely and each message incurring an additional cost. Throughout this process, issues of interoperability with existing processes and systems, and between this airport's or airline's services and those in other countries, will have to be addressed. In all of these changes, the biometric has to be robustly integrated, in spite of the performance limitations, the legal frameworks, the difficulty of enrolling and linking the biometric data to the correct identity, etc that are noted elsewhere in this Roadmap. After deployment, it may not be clear that any more terrorists or criminals are caught; they may have been sufficiently deterred to try other means of achieving their aims. At best, it may have been a tool in reducing the risk to travellers or governments.

The stakeholders

We can characterise a number of different groups that have a voice in determining the operation of biometric systems in the aviation environment:

- determining the framework for the deployment, and the rules under which these operate: parliaments, Ministry of the Interior, passport issuing authorities, regulators, Ministry of Finance
- setting the day-to-day operation of these rules: immigration officers, customs officials, border police
- bodies providing the infrastructure for travel: airport operators, reservation systems, carriers (including check-in staff and departure lounge personnel), communications network operators, media,
- travellers, criminals, mass media, etc.

The trials

A number of European initiatives have looked at the way in which biometrics can play a part in enhancing aviation security²⁴². Probably the longest running and highest profile scheme is Privium at Schiphol airport with iris recognition biometrics used for verification of the identity of trusted (and pre-enrolled travellers). The iris code is stored in a secure way on a smart card (for data privacy considerations), and additional benefits are offered in return for a service costing from 99 euros pa. The take up remains rather low. A trial of the same biometric is underway at London's Heathrow airport.

Contrast this with the 150,000 Israeli users of a hand geometry system at Ben Gurion airport. A similar series of continuing pilots was conducted by US and Canada under the INSPASS programme but internal politics and problems with costs apparently curtailed their use. Finally, mention must be made of three initiatives that could yield useful insights into the future use of biometrics. The European Commission-funded project, *S-Travel* led by SITA, will run a pilot over 2003-4, modifying the Departure Control Systems on Alitalia flights between Athens and Milan. The second initiative, *Travelscape*, aims to develop a future view on the best way forward in air travel, so as to provide all stakeholders, from governments to airlines and travellers, with a better and safer experience. Finally, IATA's *Simplifying Passenger Travel* programme (SPT) has

²⁴² A list of biometric installations at airports, the technologies used at each, and the integrator and website for further information is available in a BIOVISION report: Michael Behrens *et al*, *Discussion paper on actual testing programs and recommendations: Annex 1* (July 2003)

launched test beds in Australia, Canada, Japan, the Netherlands and the UK that use biometrics for improvement of aviation security and passenger convenience²⁴³.

The key factors

All will measure performance and success in different ways. Fast throughput at lowest cost will be of prime importance to airport authorities and carriers. Convenience and trustworthiness will be key to the end user experience. Immigration officials will want the fewest possible false alarms, but with the highest security and probability of capturing criminals. In designing the processes, software and hardware, integrators need to take account of all of these competing factors:

- Cost (including that related to secure messaging) and return on investment over the timescales of interest to the respective parties, balanced by cost savings by removing existing paper-based processes
- Aggressive timescales to build and deploy
- Transaction times (especially at peak times or seasons of the year)
- Penalties for failure in detection or throughput
- Responsibilities for the respective activities
- Complexity of the technical infrastructures
- Impact on other processes
- Physical restrictions on space - footprint of the hardware
- Distribution of checks along the sequence of check-in, passport check, security check, boarding, etc.
- Robustness of solutions, actions in case of failure of the biometric (fallback options), exception handling especially at peak times, response to unco-operative individuals or groups or intentional damage to the hardware by travellers or insiders
- Error handling, separation of processes, redundancy, aggregation of data
- Liability if a traveller misses a flight or connections or is refused entry to the country²⁴⁴.
- Privacy considerations; who owns the data, for what other purposes can it be used, and what controls are in place to limit the use in other countries?
- Interoperability and scalability of solutions - role of standards bodies in providing tailored solutions that do not overburden particular players. Calibration of nominally identical systems between airports.

Role of the European Biometric Forum

In complex applications of biometrics - such as aviation, it is important that the numerous stakeholders appreciate the different perspectives before decisions are taken. In addition to sharing the understanding the significance of the factors that have been highlighted in this roadmap, and the information gained from the numerous trials, the EBF should provide a resource for those who are newcomers to the field. This can be in the form of vendor-independent summaries of the results, presentations and displays on current best practice, and access to consultants who are recognised as having the requisite experience.

The commitments

At the end of the recent meeting of G8 Ministers of Justice and Home Affairs, a high level working group on biometric technologies was announced, co-chaired by the US and

²⁴³ IATA Annual Report 2003

²⁴⁴ The difficulties of operating watch lists have been demonstrated by current, non-biometric, systems of checking on the backgrounds of passengers; see EPIC, *Documents show errors in TSA's 'No-Fly' watchlist*, www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html

France. The meeting would report on ways to develop the technologies, including the manner of assessing their effectiveness²⁴⁵.

The US has already led with an announcement that as from the beginning of the 2004, all visitors travelling to the US by air and sea will be fingerprinted and photographed on arrival, with a Congress appropriation for \$400m for the first part of the US-VISIT project²⁴⁶. Procedures to check visitors at the exit from the US are also envisaged. This is part of the programme to gradually include biometric verification of identity for all 23 million annual visitors to the US, the technical background and financial assessment for which was published by the US General Accounting Office in November 2002²⁴⁷. This very comprehensive report concluded that there were three considerations to be addressed before going ahead with such a system:

- A decision is needed on how the technology would be used
- A cost-benefit analysis is required
- A trade-off analysis is also needed between the increased security offered by biometrics and the impact on areas such as privacy and the economy.

The GAO costed four different scenarios:

	Initial cost, \$	Annual recurring cost, \$
Watch list check before issue of travel documents	53m	73m
Watch list check before entry to the US	330m	237m
Issue of visas with biometrics	1.4 - 2.8bn	0.7 - 1.5bn
Issue of passports with biometrics	4.5 - 8.8bn	1.6 - 2.4bn

A more recent report from the GAO complains that security and privacy had not been addressed at a quite late stage in the development of the exit-entry project for visitors to the US²⁴⁸. The latest assessment is for tender documents to be returned by the Autumn of 2003, with the awarding of the contracts in early summer of 2004. As the GAO notes, however, 'effective security cannot be achieved by relying on security alone. Technology and people must work together as part of the overall process'²⁴⁹.

In late July 2003, the US announced plans for the inclusion of biometrics in its own passports. Production of documents with a contactless smart IC and compressed full face image (but with no further biometric) would begin on the same day as the requirement for Visa Waiver countries - 26 October 2004²⁵⁰.

Andrew Schulman has analysed a previous attempt to introduce biometrics as part of the US/Mexico Border Crossing Card²⁵¹. Surprisingly, fingerprints were taken and coded onto the cards, but the budget for fingerprint readers was never made available. The

²⁴⁵ US Department of State, *G-8 Countries urge use of biometrics in fight against terrorism*, www.iwar.org.uk/news-archive/2003/05-08.htm

²⁴⁶ Wall Street Journal Europe, In anti-terror move, US visitors on visas will be fingerprinted, (20 May 2003); Department of Homeland Security, Remarks by Under Secretary Asa Hutchinson on the launch of the US-VISIT program, www.dhs.gov/dhspublic/display?theme=44&content=738&print=true

²⁴⁷ US General Accounting Office, *Technology Assessment: Using biometrics for border security*, GAO-03-174 (November 2002) <http://www.gao.gov/new.items/d03174.pdf>

²⁴⁸ General Accounting Office, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning* <http://www.gao.gov/new.items/d03563.pdf>

²⁴⁹ Nancy Kingsbury, *Border Security: challenges in implementing border technology*, testimony before the US Senate, 12 March 2003 GAO-03-546T

²⁵⁰ John Leyden, *US names the day for biometric passports*, The Register (22 July 2003)

²⁵¹ Andrew Schulman, *The US/Mexico Border Crossing Card (BCC): A case study in biometric. Machine readable ID* (Revision 29 April 2002)

detailed examination of the history of this project should serve as a warning to governments on how not to design, implement and deploy such complex technologies.

In June, the European Commission has announced the results of a feasibility study into a common Visa Information System (VIS) to be used by the Member States of the EU²⁵². This will be a two-tier system comprising of a C-VIS (a central VIS) and an N-VIS, a National VIS. It recommended that guidelines for system development and the setting up of a legal basis for its use should be agreed by the Council of Ministers by the end of 2003. By analysing the three options of face, fingerprint and iris recognition, it recommended the use of fingerprint biometrics as the primary identification method, while 'a second biometric identifier such as facial recognition could be implemented to improve the accuracy'. This would appear to go against the ICAO recommendation that will be followed by the USA in its discussions with Visa Waiver countries. The feasibility study calculated the system development costs would be in the range of 130-200m euros.

More recently, the EU's Justice and Home Affairs Directorate appeared to align its thinking with that of the ICAO recommendations²⁵³. Facial images would be the primary identifier to ensure interoperability, while a second biometric, the fingerprint would be used for background checks on a 1-to-many basis.

6.4 E-health applications: biometrics as a series of point solutions?

In the era of exponential expansion in the application of technologies for the mass market following the Second World War, no sector has appeared to offer more to the citizen, but delivered less, than the medical field. With a rapidly ageing population, the breakdown of the extended family and rising expectations of individual happiness and freedom from pain, the pressures on health services in Europe have been increasing year upon year. There is no sign that these pressures will abate over the next 10 years. However, the necessary investment in IT to improve efficiencies and security (e.g. to reduce errors due to manual record keeping) has fallen behind the corresponding investment in the private sector. Authentication of medical and social support personnel, correct identification of patients, and physical access control to buildings are examples of opportunities for biometric systems. Other aspects are described in a comprehensive European Commission funded study on benchmarking for the progress of ICT adoption by the health sector²⁵⁴. Key issues identified in this report include privacy, confidentiality, reliability and effectiveness. However, much of the analysis of the issues is at a high level, and consideration of specific security mechanisms is often absent.

The fragmentation of responsibilities and budgets within the health services of individual countries is likely to limit large scale deployment of such systems, unless legislation mandates improvements across the sector. At this time (Summer 2003), there is no indication of any such proposals in the EU. We anticipate that any such legislation would result from a high profile event that brought the limitations of current systems to the attention of lawmakers. In the USA, the recognition of the need to improve security of patient records moving between the various stakeholders in the sector resulted in the Health Insurance Portability and Accounting Act (HIPAA), which requires greater attention to authentication (but not requiring the stronger security potentially offered by biometric solutions). In the meantime, point solutions - such as the use of iris recognition

²⁵² *European Commission recommends using biometrics for new EU-wide Visa Information System*, eGovernment News, <http://europa.eu.int/ISPO> (11 June 2003)

²⁵³ *Biometric identifiers for visa and residence permit for third country nationals - European Commission puts forward proposal* http://europa.eu.int/comm/justice_home/news/intro/wai/news_240903_1_en.htm (24 September 2003)

²⁵⁴ A review of the issues in the application of ICT technologies to the health sector is presented in the EC funded SIBIS report, *SIBIS - Workpackage 2: Topic research and indicator development: Topic report 9: Health* (July 2002)

in a hospital in Bad Reichenhall in Bavaria to prevent child abduction - are likely to proliferate²⁵⁵.

In this section, we look to two areas of potential deployment: the personal services sector, where medical support and social welfare support for the aged overlap; and the general hospital and general practitioner environment.

Scenario: social welfare and medical support for the elderly living at home

A unique token, the **Single Access Key (SAK)** could extend the time that the increasingly infirm can remain in the family home without having to move to a communal environment with the additional expense and restriction on personal liberty that this entails. By reducing all devices, cards and identity documents to just a single and simple-to-use device, the SAK would enable the holders to move through the complexities of modern life, even as their faculties were failing. This device could be smart card, a smart watch or bracelet or even an implanted RFID chip that would allow the user to access all types of systems in his daily life, whether in public or private transport, movement through the home, access to email or withdrawal of cash.

The list of applications is extensive and only a selection is listed below to illustrate the range of services:

- Remote management of home systems: alarms, heating, appliances, etc.
- Payments: at petrol stations, etc.
- Remote bank transactions over the phone or Internet.
- Medical surveillance for disabled and elderly people, especially in closed environments: home, hospitals, etc.

Scenario description

Mary, a very busy executive, departs from home everyday leaving her mother, Joan, a disoriented elderly person, alone at home in a village far from the nearest town and close to the national border. However, she leaves in the confidence that an 'integrated biometric system' takes care of her mum, and that she is not being abandoned without any support. In case for an emergency, she would be advised by the integrated system.

When Mary leaves, she opens the car with the single access key that 'configures' the car (she shares it with her husband who is somewhat taller and more heavily built) and starts it up with the same key. On her way to the office she fills in the car in the petrol station to take advantage of the cheaper fuel prices in her home country and pays automatically using her SAK, while at the same time the automatic timer sets off a phone call to her office switching on the heating and the microwave to deliver a hot cup coffee on her arrival.

She walks through the entrance without the need for a key or other card as the contactless SAK has communicated with the face recognition system there, confirming that the image matches the template on her key. Her computer is already configured in line with her calendar and high priority jobs that have been activated by the incoming emails from her manager. The built-in camera monitors her actions and gestures, communicating with the SAK to ensure that when she leaves the desk, any confidential documents or applications are temporarily closed down. Any specific transactions that require a specific legal attestation of identity are confirmed with the computer's fingerprint system, which again can communicate with the SAK to offer a local check on the identity of the user.

Suddenly, she receives an emergency call from the home monitoring service that her mother had been noted behaving in an atypical way by the indoor camera. The call centre

²⁵⁵ USA: *Newborn infants protected against abduction with iris recognition*, Business Wire (20 November 2002)

had confirmed that she had not moved back into the vision area of the camera, while the general movement detector was showing no activity in the house. A doctor who happened to be registered to the system as visiting family a few streets away was called on his mobile communication system and his fingerprint template was then downloaded temporarily to Joan's front door so allow him to enter the house. On finding that she was unconscious, the doctor calls for an ambulance, in the meantime being able to provide appropriate temporary medication, based upon Joan's medical file which he accesses using a face and voice biometric at Joan's broadband-enabled computer. These medical records are updated immediately, so that when Joan arrives at the hospital - which happens to be across the border, the next stage of medical support can be delivered seamlessly, improving her chances of a quick recovery.

Her own health record on her SAK is updated after she signs in with her fingerprint and the fingerprint of the doctor - a mechanism that was instituted to assure patients that no secret information is stored without their knowledge. For her, the SAK is a bracelet, as she has difficulty in remembering to take a card with her wherever she goes. Its other advantage is that the doctor can programme in a warning sound to remind her to take the pills at the required time. These will be stored in her house in a container that has a very cheap fingerprint sensor; it will send a message back to the SAK when it is opened, cancelling the reminder and ensuring that only the specific patient is able to take the expensive and dangerous medication.

An anonymised record (but securely cross-linked to her previous use of medical facilities) is sent to the independent office for monitoring side effects of medication in the country where the hospital is sited, as well as to her health insurance company in her native country, which authorises payment to the hospital and doctors. An audit record is encrypted using the biometrically validated digital signatures of the patient and doctor. These records will be automatically scanned monthly to assess performance of doctors and hospitals across the country. However, since the data protection authorities of Joan's native country have expressed reservations about some aspects of the use of biometrics for such financial accountability, a second level of anonymisation is applied for Joan. In this way, her identity is protected with cryptographic protocols.

When Mary arrives at the hospital, she sees that her mother is in good shape, but not able to recognise her after the shock. Nevertheless, the authentication offered by Mary's SAK card is proof enough to discharge Joan into her care.

On her way home, Mary remembers that she failed to sign off the final job she was completing. That is no problem for the biometric enabled world, as she is able to use an intermediary service from a motorway service station. However, this uses voice and face as the only biometric methods, not the enhanced fingerprint system which offers the higher level of authentication. (One had been in place but had been vandalised so often that the operators had removed it). However, seeing that her mother is by her side, the intermediary service calculates the risk associated with accepting the authentication offered by both persons together, agreeing that to be sufficient to meet the immediate requirements of the service, provided that Mary signs it off again using the more secure system at the next opportunity.

In the evening, their neighbours come round to enquire after Joan's health, and Mary takes the opportunity to enrol them into the house entry system as authorised visitors, but only to be allowed in when the house is occupied and the warning system is activated. At other times, Joan's privacy is protected, so that they have to ring the doorbell as any other visitor.

Finally Mary retires to bed exhausted after a hard day - but this time there is no need to be authenticated by any biometric. She falls asleep while reading a book: the latest, tenth, novel in the Harry Potter saga, as the movement sensor by her bed triggers the gradual reduction of the light levels in the bedroom.

In her own room, Joan is kept under the ever watchful eye of the bedroom camera, continuously checking for abnormal reactions to the medication, backed up by an hourly visual confirmation by a nurse at the hospital where earlier in the day she had received such timely treatment.

Commentary on the scenario

Again, as in many instances in this report, the emphasis in this scenario is on usability and on integrated services that simplify the world for the end user, while allowing them control of their privacy. Integration with intelligent systems, that have context awareness built in, or use interfaces that allow intuitive programming by end users. Diversity of sensors and service operators offering different levels of security appropriate to the needs and abilities of the user. Transparency and seamless operation wherever possible, but over identification when a clear business need is required (electronic transaction at the office, addition of sensitive information to an Electronic Patient Record). For the older person or one who is often confused, these measures will be particularly important, but only if they are robust and 'fail to safety'.

Protection of the privacy of individuals, while taking advantage of the biometric authentication is the subject of active research at present. Papers have hinted at methods that could be used²⁵⁶.

Much of the technology is available in component form today. However, progress towards an integrated service as described is likely to be slow, unless towns or regions with an exceptionally high proportion of elderly people decide to work as a community to demonstrate the business case for such a scenario. The cost of such systems would be substantially less than that of major modifications to the physical environment of the elderly person (addition of bathrooms downstairs or electric stair lifts on staircases) - costs that are already borne by either the state or the individual. Early demonstration of the use of integrated technologies could provide the stimulus for more extensive deployment of systems.

Hospital and family doctor services

Provision for health services in the EU is characterised by the diversity of different schemes and services. In March 2003, the Council of the EU proposed a EU-wide health insurance card from the Summer of 2004, to replace the paper documents for cross-border access to health services, although there are no plans to include a biometric authentication. In many countries, IT investment has not kept up with the requirement to provide an efficient and safe operating environment²⁵⁷.

Aims of an electronic, biometric-secured health card

There are a number of possible reasons for better authentication in the health sector. Traditionally hospitals have been open sites with little control on visitors to patients, unless these were under arrest or confined under mental health regulations. In spite of the

²⁵⁶ Gerit Bleumer, *Biometric yet privacy protecting person authentication*, Information Hiding LNCS 1525 (1998) Springer Verlag pp 99-100; Jean-Paul Linnartz and Pim Tuyls, *New shielding functions to enhance privacy and prevent misuse of biometric templates*, 4th Conference on Audio- and Video-based Biometric Person Authentication, AVBPA 2003, pp 393-402

²⁵⁷ A benchmark study showed that a junior doctor in the British National Health Service spends up to a third of his time on unnecessary and secretarial duties. The European Commission is paying for a research project that should provide guidance to decision makers in member states on the cost models that should support a range of e-Health investments. See 7th Annual European Conference on Electronic Health Records London UK (December 2002). In the UK, the budget for IT services in year 2002/3 is approximately £1.6bn out of a total NHS cost of £68bn. An additional allocation of £1bn for IT services was added under the NHS Modernisation Fund in the seven year period from 1998 with the aim of contributing to the doubling of the IT spend

valuable equipment (both IT and specialist monitoring systems), patients being at their most vulnerable (old people and babies in particular), and the availability of drugs, hospitals in general are not designed as physically secure places. There have also been a number of well-documented cases of individuals passing themselves off as medical practitioners. Hospital patient records are also not well secured, and a recent report of Irish Republican terror groups attempting to infiltrate hospitals in Northern Ireland to gain such data is unlikely to be the only case.

Outside of the hospital, the Electronic Patient Record (EPR) initiative aims to offer portability of a person's medical history, so that wherever they are - abroad or involved in an accident, patients will be treated quickly in line with their past medical interventions²⁵⁸. Another opportunity that is being exploited by a number of US biometric suppliers is in the signing off of the results of legally mandated tests on pharmaceutical products, a clear example of the use of biometrics as a tool for non-repudiation.

In summary, the range of possibilities is very wide indeed:

- E-diagnosis
- Drugs Distribution and prescription
- Credential Checking
- Secure information for the supply chain
- Health Insurance Card
- Secure and accountable transition from paper legacy systems
- Traceability of Diagnostic Data
- Set up Supply Chain
- Order Trials accountability in case of litigation
- Data Integrity
- Clinical trial integrity
- Physical access
- Emergency procedures

Nevertheless, the range of stakeholders is extensive, with management responsibilities often distributed across a number of government agencies and departments, together with conflicts in priorities between doctors and managers.

Actors in the health sector

- Ministry of Health
- Regulatory and legislative authorities (including data protection)
- Insurance companies
- Hospital management
- Medical Staff
- Laboratory Staff
- Ancillary staff
- Service providers
- Medical Researchers
- Ambulance services
- Patients
- Patient organisations
- Visitors
- Miscreants

Current Status

²⁵⁸ The UK's NHS has a target to create an EPR infrastructure in every acute hospital by 2005. Other countries in the EU, such as Sweden, Ireland and Austria have parallel plans.

The Netherlands has undertaken initial trials for the distribution of methadone to habitual drug users. Although the use of a biometric was considered in the trial, it was decided not to use it at that stage. Interviews with participants during the trial showed a high degree of acceptability of fingerprint authentication, and it is understood that a future roll-out will include the use of fingerprint authentication. This could be the beginning of an extension to a number of biometric-authenticated services for those with chronic diseases. Trials with Parkinson's disease patients have used fingerprint biometrics.

In the UK, there have been a number of continuing intermediate scale trials (at the level of several thousand users) by the NHS Information Authority, both as substitutes for passwords in PCs, for the protection of sensitive medical records and for use by patients in accessing their own records. Little information is available on the extent to which these have been successful, although the leading integrator, ISL (Informer Systems Ltd) claims usage of its authentication solutions at more than 600 installations with over 25,000 users.

Other trials that have been noted, that make use of biometrics, include:

- Physical access control in Sweden
- The use of soleprints to identify babies in Germany
- Sign off of testing of pharmaceutical products in the USA
- Proposed telemedicine trials in Italy

The use of Public Key Infrastructures in the medical sector ought to be tracked, since investment in the renewal of a security infrastructure could be accompanied by use of biometrics to replace the less than adequate password that protects a private key. An example of a project that is examining interoperability issues at the cross-border level (Germany, Greece and Finland) is RESHEN, an EU funded activity for Regional Secure Healthcare Networks²⁵⁹.

Key factors in the take-up of biometrics in the health sector

Since the medical sector in Europe is funded to a significant extent by the state with drug costs and wages and salaries a visible part of the budget, there has been relatively little investment in IT and IT security. In the UK, this is being addressed as part of a major uplift in investment over the forthcoming budgetary period. However, there is little evidence of a concerted effort in any European country to consider more advanced non-medical technologies such as biometrics. Amongst the reasons that have been proposed are:

- Very limited awareness of the possibilities of biometrics
- Apparently high costs
- Identity theft not taken as seriously as it should be
- Security not a high priority
- Safety concerns
- Health services are not well integrated, so benefits of reuse across competing departments with access to different budgets are not appreciated.
- Quality concerns
- Potential integration with other services is unrecognised
- Power of the medical practitioner may be undermined

Possible roles for EBF

The European Biometric Forum could act as a catalyst to highlight the opportunities in this sector, offering an independent vision and source of reliable information. Lessons can be learnt from one application that is likely to be heavily promoted in the US: the security of hospital patient records. Although the HIPPA legislation does not mandate the use of

²⁵⁹ www.biomed.ntua.gr/RESHEN

biometric authentication, it is probable that many solutions will make use of these technologies.

Other activities that would contribute to the development of a stronger understanding of the options opened by biometrics include:

- Promotion of initial awareness of the range of opportunities
- Dissemination of publicly available information
- Database of deployed systems
- Encouragement of partnerships that will run pilot and demonstration projects
- Integration of the Electronic Patient Record and smart cards
- Monitoring the status of relevant regulation

6.5 Use of biometrics by the financial sector

Key opportunities for the use of these methods by this sector include:

- Customer-facing systems: Point of Sale (POS), Automatic Teller Machines (ATM), on line retail transactions, cashing of cheques for people without bank accounts, signing of insurance claims, etc
- Call-centre applications secured by speaker verification of callers, possibly supplemented by confirmation of knowledge-based authentication
- Notarisation systems. Authenticated signatures of financial transactions, e.g. a written signature biometric of a salesman used in combination with a digital signature to a document confirming that a client has seen the information provided in that document
- Security of high value back-office applications such as treasury, dealer rooms and interbank transfers
- Network logon, especially where accountability is required and separation of duties needs to be enforced (reducing the possibilities of a recurrence of the Barings Bank fraud).
- Time and attendance applications, and monitoring of employee activity to reduce all forms of insider fraud
- Protection of customers' financial data to permit only authorised viewing or alteration
- Physical access control to data centres and other high risk areas
- Automation of workflow through the replacement of paper-based systems. Since written signatures underpin many of the legal transactions in this sector, the use of a signature biometric may offer a legally acceptable alternative to the written version.

Note that a major application already in place in the USA - screening of employees for criminal records, by comparison of their fingerprints with FBI databases - is less likely to find acceptance in Europe.

Two key factors appear to be prominent in the discussion of the deployment of biometric systems by these organisations - in particular to their customers.. Firstly, it appears that in spite of their wide experience with managing risk, banks employ IT specialists who demand very high performance of biometric systems, often in excess of those implied by conventional PINs or passwords²⁶⁰. Secondly, the larger banks in Europe are generally conservative in their use of public-facing security technologies. They recognise the risk of a premature introduction of untested systems and the impact on trust in them by the public should the security of these systems be broken. A third factor, acceptance by the public, is likely to be offered as yet another reason for delaying a decision, even once these technical concerns have been resolved.

²⁶⁰ Examples of these stringent performance requirements were noted in the European collaborative BANCA project, <http://falbala.ibermatica.com/banca/index.html>

Credit and debit card fraud continues to rise inexorably, and it is therefore not surprising that banks, financial institutions and their associations (such as APCAS in the UK and TeleTrusT in Germany) continue to examine the commercial potential of biometrics in reducing fraud at the Point of Sale. Section 3.4 examined two scenarios for the future application of biometrics in this sector. In this section, the focus changes to the assessment of possibilities for their use in the near term (2003-2005), concluding that customer-facing applications are unlikely to be introduced widely over this period in Europe. Nevertheless, operations in the back offices of the financial institutions may begin to see the use of these systems in larger numbers in the early stages of the following period (2006-10).

Many of the issues that are discussed in this Roadmap have held back the widespread deployment of biometrics, although numerous trials have been undertaken and many reports issued. For example, in the early 1990's, the UK's Midland Bank undertook a Dynamic Signature verification trial, and in the mid 1990's the Nationwide Building Society led a major investigation into their use, with headline making trials of ATMs using Iris Recognition. They were also part of PICASSO, a European project. Other ATM manufacturers such as Oki have also trialled the use of biometrics, but the additional expense and need for customer training has curtailed this work. In the early 1990's, Barclays Bank in the UK suggested performance requirements for biometrics in terms of FAR, FRR and time for transaction, based upon typical POS operations. In the US, the Financial Services Technology Consortium (an industry body representing many leading financial institutions) continues to sponsor studies on biometrics. Most recently, a study into the application of speaker verification has been completed²⁶¹.

However, studies by Germany's TeleTrusT organisation and its working group on biometrics, BioTrusT, have been far from favourable when it considered the use of these methods for ATMs. Issues of unacceptably high error rates for mass market services, the large infrastructural changes required in the 'back end' systems, lack of all of the required standards in the financial service sector, and legal and regulatory uncertainties contributed to the negative tone of the report. This is backed by an appraisal of the opportunities by a respected UK sector journal published some time after September 11th²⁶². A roll call of the prime financial institutions repeated the same message, 'we have looked at biometrics, but we have no immediate plans - we have to look at the business case'. However, it was not only the costs that worried the head of policy card services at APACS, the association representing these institutions in the UK. Both the problems generated by false rejects on the daily number of 11 million bank transactions, and lack of a biometric that would have extensive acceptability amongst its customers were cited as causes for concern. Indeed, one unnamed source went as far as saying that it would take as much as a decade before the banking community would consider the introduction of biometrics. Before that, the UK programme of introducing a PIN to the credit card has to be completed²⁶³.

Alternative approaches to biometrics are possible. For example, in the first half of the 1990's, cards with small photographs of the holder were issued by the Royal Bank of Scotland and the National and Provincial Building Society in the UK. The claim was that fraud on two of the RBS's card had dropped by 99% and 85% respectively, saving the bank nearly £1m²⁶⁴. It was not clear whether this was as the result of displacement of crime to cards issued by other vendors, since trials by the University of Westminster in 1996 seemed to demonstrate its low value as a security device when offered to supermarket checkout operators²⁶⁵.

²⁶¹ www.ftsc.org/projects/voice-authentication

²⁶² Sean Jackson, *Stand and deliver*, Banking Technology **19** (1) 44 (February 2002)

²⁶³ *Traders gear up for chip-and Pin future*, Computer Weekly 27 March 2003. By the end of 2005, most of UK's 110m credit and debit cards will be chip-and PIN enabled at a cost of over £1bn.

²⁶⁴ *Guardian, Photocards slash fraud and save bank £1m*, (13 August 1996)

²⁶⁵ Richard Kemp *et al*, *When seeing should not be believing: photographs, credit cards and fraud*, Applied Cognitive Psychology (1996)

In the autumn of 2002, the Nationwide Building Society announced the rollout of a biometric solution whose business case was based upon savings in costs (by moving from paper-based processes to an all-electronic system) and responsiveness to the customer, with security only a secondary aim. In fact, this deployment would replace the need for frequent faxing of images of signatures between the 681 branches of this organisation²⁶⁶. Dynamic Signature Verification software from CIC and tablets supplied by MotionTouch are being integrated by Florentis. Only in the third phase of the deployment will automated signatures be verified. Extensive work on the user aspects of the hardware and software should improve its chances of success, and template ageing is used to take account of changes in signature. Nearly 60 subjects took part in four centres, and one of the developments was to change the feel of the surface of the signing pad towards that of paper.

Up to seven signatures are stored with a decision function determining which of the signatures will be dropped at the time of verification. Legal admissibility issues had to be considered, bringing in experts from Australia and Canada. Among the lessons learnt was the long process of obtaining agreement at all levels in the organisation, helped both by the involvement of many stakeholders, as well as by small and frequent deliveries of results, which kept a continuing interest in the project.

In summary, the outlook for the use of biometrics in the financial sector over the study period looks far from promising. Nevertheless, a number of banks have shown interest in using biometric authentication in the 'back office' applications, where they can learn about the challenges of introducing these methods under controllable conditions, and not risk the possibility of an expensive failure by premature use amongst their customers. There is a strong base for standards in this application, through the development of standard X9.84 by the American Bankers Association.

The use of biometrics by EU governments in passports will, no doubt, be followed with interest by the banking community - especially if this moves to electronically-enabled identity cards. In some countries, such a move may be the cue for involvement by financial institutions, since many of the deployments will rely for part of their business case on participation by the private sector. The experience of Finland in not getting sufficient take-up for its non-biometric card should be studied by any country planning to follow suit. Such considerations would appear to rule out extensive use of biometrics, either for cash transfers, ATM use or Point of Sale before 2008. The analysis of scenarios in Section 3.4 lists some opportunities and challenges. One advantage for this sector is the availability of a security standard for the use of biometrics: X9.84 (see section 5.6)

One factor that could bring forward the use of better authentication is the rising incidence of identity theft. In the US, this is seen as a major - and escalating - hazard of life in the 21st century. Its incidence is quoted variously as 750,000 people victimised annually (by US government agencies), through to Gartner's estimate of 7 million in 2002²⁶⁷. The UK government's consultation paper on Entitlement Cards quoted a figure of £1.3bn as the minimum cost to the economy. These figures do not reflect the misery that victims of such identity fraud suffer over long periods (up to several years) as they attempt to rebuild their credit records. In many cases, the financial institutions appear to be unable to remove all traces of these transactions, and the problem recurs even though the individual has been assured of its solution. Biometric methods of authentication could have a role to play in reducing the level of fraud, although insecure operation of such biometric-enabled systems could paradoxically increase the damage to individuals. Criminal entities would inevitably target such systems, either to ensure that their own identities were not compromised, or to commit more sophisticated frauds. Assuring the security of such systems over the lifetime of individuals will be a challenging objective.

²⁶⁶ *E-signatures win over iris scans*, IEE Review p.14 (January 2003)

²⁶⁷ Robert O'Harrow, *Identity Crisis*, Washington Post (10 August 2003). See also a review of policies, technologies and procedures from a US standpoint in John Vacca, *Identity theft*, Prentice Hall PTR (2003)

6.6 Physical access control and 'time and attendance' applications

In section 3.3 we examined the long term outlook for the use of biometric methods for physical access control, identifying two scenarios for their future wide scale application. Currently, most of the access control market for corporate government use consists of visible identity cards and security staff to check that the photograph of the individual matches that on the cardkey. Further restriction of access to individual parts of a site or office usually relies on keys and door locks. As organisations review their physical security, swipe cards or proximity cards replace keys, often integrated with the corporate identity card. Relatively few biometric systems have been installed, as testified by the need of suppliers to issue press releases every time a larger campus is converted to these technologies. In the past few years, a number of integrators have started to offer tailored solutions for improved 'time and attendance'.

The T&A proposition centres on a number of benefits:

- reduced 'buddy punching' fraud in which employees sign out on behalf of workers who have left the premises earlier - or even failed to turn up at work at all;
- improved quality control in industries with large workforces of semi-skilled labour; especially in developed countries, well-suited individuals can be recruited and trained, only to be replaced soon afterwards by less suitable friends and relatives;
- more accurate completion of timesheets by the staff, as the incidence of human errors is reduced;
- improved physical access control, so that only authorised staff are allowed on the premises.

Taken together, these benefits should ensure that this type of application should be attractive to employers of large groups of unskilled and semi-skilled staff - provided that the cost is kept low and that the workforce accepts its use. Much of the \$100m market in 2002 represented deployments outside of Europe, since (especially outside the UK), the attitude of employees towards the introduction of new technologies is uncertain. Even in the UK, these issues need to be handled with care, as witnessed by the strike by British Airways ground staff at Heathrow in 2003 following proposals to introduce swipe cards for T&A.

Kronos - one of the leaders in T&A applications - have developed biometric solutions; they appreciate the need for employers to consider the acceptance issues through the preparation of education material²⁶⁸. The reassurance focuses on three factors:

- the storage of mathematical representation of fingerprints - not the fingerprints themselves
- incompatibility with AFIS devices and systems
- speed and accuracy of operation, eliminating false readings.

For many years, hand geometry systems were synonymous with access control, and even though the PAC/T&A sector accounts for over 80% of sales of hand geometry biometrics, revenue from systems using fingerprints actually exceeds that of hand geometry sales. Iris systems come a distant third - mainly deployed where perceived security requirements demand this approach. Taken together, these three technologies account for over 90% of this sector. Growth of acceptance and widescale use in Europe will depend upon the resolution of acceptance, cost and robustness issues.

²⁶⁸ Kronos Inc, *Ease employees' privacy concerns about biometric technology*, www.kronos.com (2003)

6.7 Car personalisation and security

The use of keys to secure cars represents a considerable overhead for many fleet operators and rental companies. Keys are often mislaid, lost or stolen. It is not surprising, therefore that moves towards keyless, card-based systems are already underway - with Mercedes and Renault offering these options. An additional benefit of a biometric system would be in personalisation of the settings for seating and other user-adjustable controls in modern cars. This second opportunity has been seized by Audi in its recently introduced A8 model²⁶⁹. Addition of personalisation for up to four drivers is available at an additional 2% on the price of this top of the range model. Gartner has estimated that by 2010 approximately 8m new cars would be fitted with biometric identifiers (early 2002 estimate, worldwide). Relatively few cars would be equipped before the take-off in the second half of the decade, an assessment shared by other consultants. Before widespread adoption can take place, a number of issues have to be successfully addressed: cost, reliability, robustness in the electrical environment and resilience against dirt, dust and chemical cleaners.

6.8 Applications in the Criminal Justice Sector

The law enforcement community has an interest in the development of robust methods of identification to reduce the opportunities for identity theft²⁷⁰, to apprehend criminals with improved detection based upon scene-of crime evidence (including that obtained by CCTV systems) and to deter potential criminals from engaging in antisocial activities. In the UK, PITO, the Police IT Organisation are helping to define the research agenda and preparing a parallel roadmap that will help long term planning by solution suppliers and individual police forces. Databases of face and fingerprints are already well established in the police forces of all countries. In addition, there is a standard for distinguishing scars and tattoos. We have also mentioned the work on the use of external ear shape and there is extensive development in capturing palmprints from the scene of crime. DNA profiles are now routinely collected in the UK, and retained on computer even if the individual is released without charge by the police²⁷¹. If iris recognition becomes a widely accepted biometric, there is no doubt that databases of iris images will also be developed. As the UK's NAFIS²⁷² contract is in the process of re-negotiation, PITO is looking towards a new vision for an integrated identification service.

The aggregation of data can be used to increase the rate of crime detection, and reduce the likelihood of miscarriages of justice, provided that the probabilistic nature of the evidence from biometric systems is recognised and end-to-end traceability is maintained. The legal admissibility of biometric data will remain to be confirmed in the courts, but every stage in the process of data collection, through template formation and update, processing, linkage to the application and independent assignment of identity needs to be secured. The dangers of aggregation need to be recognised, though, especially if governments choose to misuse the systems to coerce their citizens or to manipulate electronic data in support of otherwise lawful aims. A fingerprint reader in every policeman's pocket linked over the mobile phone network to a database may exclude possible suspects in a quick and efficient manner. In another environment, it can be viewed as a symbol of the power that the policeman has over a minority exercising their human rights. Suppliers of biometric systems may need to consider the extent to which their technologies can be

²⁶⁹ www.audiworld.com/news/02/a8launch/content6.shtml

²⁷⁰ APACS claims that identity theft cost £20.6m in 2002, up from nearly £15m the previous year. *Ways to beat the identity thieves*, Financial Times 25 March 2003. A much wider definition suggests that, worldwide, the problem could amount to \$221bn www.aberdeen.com/2001/research/05030013.asp (Aberdeen group paper: *Identity theft: a \$2 trillion criminal industry in 2005*)

²⁷¹ As of June 2003, in the UK, police hold nearly 5m sets of fingerprints and over 2m DNA profiles.

²⁷² National Automatic Fingerprint Identification System (UK)

misused and the impact that the resultant adverse publicity will have on the likelihood of acceptance of their products in the EU.

Other opportunities that developments in biometrics offers include improvements in 3-dimensional rendition of suspect's faces which may in due course support the identification of potential suspects by victims of crime and similar use in the video identity parades of suspects²⁷³. Effective biometric systems could be used to enforce court orders to restrict the movement of individuals away from key witnesses or family members.

It appears very likely that the use of biometrics by the Criminal Justice sector will increase dramatically, from securing access to the increasingly rich data sources in the identification databases, through to supporting the police officer requiring a fast verification of a citizen's identity. However, deployment of new technologies requires a public debate on the checks and balances that should be in place for the protection of the citizen. The complexities of biometric systems, and the impact of many years of Hollywood films and television series, can be balanced by an impartial source of trustworthy data to allow society to establish a level playing field for such discussions.

Recently, a facial recognition system from Imagis has been configured for use in clustering Internet images of victims of child abuse. The ChildBase application developed for the UK police checks whether images obtained from the PCs of individuals accused of downloading relate to previously known victims²⁷⁴. Nearly 1m images were stored in the initial database which opened for operation in the Summer of 2003. Initial testing of the system has proved very successful as a support tool for the criminal justice system, even reputedly identifying siblings. This is one example of a biometric system that operates outside of the normal range of identification and verification.

Other applications of facial recognition, especially in the context of CCTV enhancement, are discussed by Michael Bromby, who provides a first view onto some of the legal issues that may accompany these innovations²⁷⁵.

RC/Sec3 RC - SYSTEMS AND DESIGN: SECURITY 3: Development of design methodologies that support the secure integration of biometric data in applications such as the Criminal Justice Sector, while limiting the opportunity for misuse and 'function creep'

6.9 Online authentication for consumers and employees

The EC funded BEE project addressed many of the issues in the application of biometrics to online transactions, especially for e-commerce²⁷⁶. To support the existing knowledge on the technical aspects, an ongoing 4m euro project, COST275, aims to investigate effective methods for the identification of individuals over the Internet using speaker verification and facial recognition²⁷⁷. The results of this COST Action project will be disseminated into the technical literature and through the organisation of specialist workshops.

²⁷³ In the UK, the current system for video identification parades, VIPER, has enjoyed considerable success.

²⁷⁴ Lisa Kelly, *Police invest in ChildBase system*, Computing 16 July 2003

²⁷⁵ Michael Bromby, *Computerised facial recognition systems; the surrounding legal problems*, cbs1.gcal.ac.uk/law/users/~mbro/documents/LLMDissertation.pdf (September 2000)

²⁷⁶ Business Environment of Biometrics involved in electronic commerce <http://www.expertnet.net.gr/bee/> (IST-1999-20078, completed June 2002). Specifically, document, D7.1 *Conclusions and Recommendations* (June 2002)

²⁷⁷ COST Action 275, *Biometrics-based recognition of people over the Internet*, www.fub.it/cost275

In its concluding report of June 2002, the BEE consortium noted that there were no major 'showstoppers' in the application of biometrics in this segment of the market for authentication. However, it did recognise that improved - and secure - performance was a prerequisite to assuring users that the technologies would address their requirements. Also of primary importance was the need to form a working group that would co-ordinate standards activities (particularly for interoperability) and best practices, especially in areas such as privacy protection. This is a role that the European Biometric Forum is aiming to fulfil, and the publication of the *Best Practices in Privacy in Biometrics*²⁷⁸ as part of the BIOVISION project will form one of the strands of work that the EBF will continue. Certification services will also be needed to provide an external monitoring of compliance with such best practices. Finally, it noted that very little work had been undertaken in establishing whether ethnicity could be deduced from biometric measures. In passing, we note that not timescales were offered for incorporation into the present Roadmap.

Developments continue in a number of areas that should ensure that future mass market systems are both cost effective and easy to install and operate. Microsoft has indicated that it will include a proprietary biometrics API ('BAPI') in a future release of the Windows operating system, thereby facilitating the integration of compatible biometric sensors into PCs and laptops. Sensors are continuing to fall in price, with suppliers offering even smaller devices to reduce the cost of the silicon in fingerprint systems. Even full scale sensors integrated into standard peripherals are now affordable; a standard Siemens computer mouse is now available in the UK at £36 in unit quantities. In a recent move that demonstrates the acceptability of fingerprint biometrics as a security device, Intel has issued guidelines for the use of fingerprint biometric sensors in notebook PCs²⁷⁹ and evaluated three commercial sensors against these guidelines, the Atmel Fingerchip, AuthenTec's TruePrint AES 3400 and the TCRU1 from ST Microelectronics²⁸⁰. Suggested performance targets are FAR of less than 0.01% and FRR of less than 2%, with the individual cost for such devices (inclusive of software costs) not exceeding \$10 in 100,000 up quantities - demanding goals that may represent performance which is difficult to attain, and maintain, with current devices operating under conventional conditions.

Although the focus of the study was on e-commerce applications, it foresaw the need for government to prepare roadmaps for the use of biometrics in on-line access to its services, national ID cards and the provision of secure services in the health sector. However, it could not have foreseen the impetus that the US Enhanced Border Security Act would give towards the demonstration of the feasibility of large-scale systems.

In view of their critical dependence on IT systems, large organisations continue to reassess the security of their operations. In the past, the view of the place of biometrics in these organisations was as 'drop in' replacements for passwords. The high cost of maintaining a help desk for resetting forgotten passwords and the proliferation passwords seemed to justify investment in novel technologies. Nevertheless, some organisations decided to consolidate legacy computer systems behind a single user interface, in the form of a Single Sign On solution (SSO). The pressure to introduce biometric authentication lessened.

The next stage was often to consider the introduction of PKIs (Public Key Infrastructures), offering non-repudiation (and often confidentiality of emails messages

²⁷⁸ Astrid Albrecht, *Privacy Best Practices in deployment of biometric systems*, Issue 1 (2003), available at the <http://www.eubiometricforum.com> website.

²⁷⁹ *Biometric User Authentication: Fingerprint Sensor Product Guidelines*
<http://www.intel.com/design/mobile/platform/downloads/FingerprintSensorProductGuidelines.pdf>
 (15 September 2003)

²⁸⁰ *Biometric User Authentication: Fingerprint Sensor Product Evaluation*
<http://www.intel.com/design/mobile/platform/downloads/FingerprintDeviceProductEvaluationSummary.pdf>
 (September 2003)

and electronic transactions). However, the complexity of integration with other applications and the consequent high costs resulted in lower take-up rates than were predicted in the late 1990's. Had PKIs been adopted widely, it is likely that the use of fingerprint verifiers to protect the user's private key would have followed soon afterwards. Since then, another paradigm has arrived: **Identity Management**²⁸¹. Through the years of restructuring and takeovers, many organisations have complex directories of their employees and customers. The same individual or role appears in many places in an organisation's databases, leading to customers and employees having to logon many times for similar services. For example, in the financial sector²⁸², banks and insurance companies see the prospect of account aggregation as a way of cutting costs and increasing their reach. Identity management (IdM) solutions offer the vision of a single integrated access to this information, with a set of business processes to support authentication and access management (policies and rules that govern access to applications), working within the Web Services and federated database frameworks. An emerging collection of standards is supporting this initiative, with SAML (Security Assertion Markup Language) one of the critical glues. Again, the use of biometrics would appear to complement the vision, although many suppliers are still to adjust their promotion of biometrics in this context. The opportunity is there, but cost, security and user interface issues will determine whether IdM is the breakthrough for biometrics in the mass market – or just another grand design that will fade as another acronym takes its place.

²⁸¹ RSA Security, *Identity and Access Management: Transforming e-security into a catalyst for competitive advantage*,
https://www.rsasecurity.com/solutions/idmgt/whitepapers/IAMBUS_WP_0403.pdf

²⁸² FSTC, *Identity management in financial services* (8 July 2003)
<http://www.fstc.org/projects/liberty/executive-overview.pdf>

7. Addressing the critical issues

This selection of applications of biometrics illustrates some of the issues that come into play when the technology is integrated as part of a complete service. Perhaps one of the key areas which has received little or no consideration is in developing the *credibility* of both the biometric proposition and individual technologies. To a large extent, the adoption of these methods in the identity document and aviation security field is a tribute to the lobbying of the technology suppliers immediately after 9/11. Many commentators have questioned whether more secure verification of the identity of visitors to the USA would have prevented these tragedies. Nevertheless, it is accepted that there is a role for improvements in security throughout the transport infrastructure, from the large hubs, such as railway stations and airports, through to the vehicles themselves. However, other forms of security are required, especially if the current mode of suicide terrorism by individuals with no previous history of such activity increases worldwide.

7.1 Crossing the 'Technology Chasm'

The classical view of a sigmoid curve in the take-up of new technologies is being questioned. If this were so, the early adopters would have given way in a ever-increasing way to the pragmatists, leaving only the conservatives to remain with the old technology²⁸³. At least some of the biometric technologies would have been used in large numbers, leading to major cost reductions. In point of fact, there have been considerable price drops for silicon fingerprint verifiers, but this has not stimulated a corresponding growth in the market.

A more recent reading of the diffusion and adoption of novel technologies by Geoffrey Moore notes this drop in the take-up rates after the *early adopters* have explored the new technology, but before the early majority feels confident enough to begin to buy into the new paradigm²⁸⁴. Of course, the initial group of enthusiasts and visionaries is a pre-requisite for the follow-through; their demand for novelty and performance, and their opinions are taken into account by those who will follow. These are the leaders who ensure the visibility of the new technology. However, they also willing to bear the risks which accompany any new developments. The following group, the *early majority* are pragmatists who have different concerns; they seek industry standards, complete solutions and the experience offered by reference sites. Between the early adopters and the early majority there may be a hiatus in the sales of novel systems, the *chasm*, which can lead commentators to doubt that the technology will ever be taken up. Some will attribute this lack of take-up to a lack of credibility of the technology and prescribe measures to address this deficiency²⁸⁵.

In Moore's analysis, the credibility issues must be addressed by targeting marketing efforts at the leading edge of this early majority. It is the *bowling alley* (in his phraseology) who will provide those reference sites. The challenge for suppliers and integrators is to convince this separate niche group in large enough numbers, thereby addressing the fears of the main majority who are waiting for sufficient momentum to build up in the market. However, once the bowling alley group is convinced, the take-up can rise spectacularly, with the majority demanding to be supplied quickly, leading to temporary shortages as the suppliers fail to meet the demand (Moore's *tornado effect*).

²⁸³ Everett Rogers, *Diffusion of innovations*, The Free Press (4th edition, 1995). This discussion is based on a review by Werner Mulder and Richard Simpson, *Supplement to 'DoCoMo's I-mode: strategies for success*, University of Cape Town Graduate School of Business paper 501-050-4 (2001). See also *Biometrics Market Intelligence*, a newsletter that addresses this model for the biometrics market www.acuity-mi.com and the discussion in Chapter 2 of D A Norman's *The Invisible Computer* MIT Press (1998) at <http://mitpress.mit.edu/books/NORVH/chapter2.html>

²⁸⁴ Geoffrey Moore, *Inside the tornado*, Harper Business (1995)

²⁸⁵ Kate Curtis, *All IT needs is credibility*, The Journal of the Communications Network 2(1) pp 4-8 (January - March 2003)

For the biometrics industry, the market may still exhibit the characteristics of the chasm, and requires standards to be in place (ICAO, ISO, X9.84) and the experience offered by trusted leaders (in this case, this could be the acceptance by governments of their use).

The increasing number of new entrants may also be confusing potential buyers, as these entrants may continue to aim their products at the early adopters, not learning from the mistakes of previous innovators²⁸⁶.

The successful deployment in non-governmental services may depend on numbers of successful, user-friendly implementations of biometrics in national ID and cross-border systems. Returning to the question posed in Section 2.1, there appears to be no clear cut 'best' application for which biometrics can be advocated in order to reassure the early majority. However, the situation could change due to wild card developments (a major disruption of the e-commerce market) or a radical reduction in the 'whole life' cost of a particular service that makes use of a biometric.

In the meantime, it is important to track the large-scale deployments and encourage the designers to follow the precepts that have been discussed in this roadmap. However, there are worrying indications that in the haste to deploy systems that meet the deadlines mandated by Congress, security and privacy issues have not been accorded the priority that we have identified in this report. Perhaps the GAO report will alert systems integrators to their importance once the contracts have been signed.

Use by commercial organisations is likely to start in internal applications such as access control and logon to enterprise wide applications. These can be simply as standalone replacements for existing non-biometric systems. However, the introduction of new mechanisms such as biometrics may be more sensibly approached as part of a review of the security infrastructure of organisations. One indicator that gives us concern is the slow take-up of PKI and applications using them. After the legislative activity worldwide that confirmed the role of electronic signatures, it was assumed that rapid uptake of Public Key Infrastructures would follow in their wake, with biometric signatures succeeding not long afterwards as corporate security officers recognised the weak link inherent in the use of passwords and passphrases. The evidence to date is that without a wild card event, corporates will continue to rely on well-established security mechanisms and not seriously review their exposure to external and internal threats.

If it is not a re-evaluation of the security that acts as a spur to the corporate use of biometrics, it may be the recent interest in integrated identity management systems that causes management to consider these new technologies. With information about employees and customers distributed across many databases, and with little co-ordination in updating these, forward-looking organisations are recognising the need to consolidate their schemas around LDAP directories and XML standards. Whether this provokes a reconsideration of the use of biometrics, with templates stored alongside the newly integrated systems remains an open question.

7.2 Future applications

While business ponders on the way in which biometric methods could be used in organisations, research projects should address some of the challenges in other fields of commerce. Two of the main areas of concern to the security community will be Digital Rights Management and Web Services, delivering current and future types of application to the consumer in novel ways, and requiring authentication in novel environments. It remains to be seen whether biometric verification of identity is required or can be justified on the grounds of cost and security. Once the range of applications widens significantly beyond transaction verification, PC logon and physical access control, robust

²⁸⁶ Jon Tullett, *Face facts, technology isn't always foolproof*, SC Magazine, Editorial of June 2003 issue, describing his experience of visiting biometrics vendors at the Infosecurity Europe exhibition.

middleware should be developed that allows simple, yet secure, integration of authentication across a variety of applications.

Analysis of typical biometric applications has shown that people costs dominate deployments, whether at enrolment or at helpdesks when users forget which finger they used at enrolment or find difficulty in adjusting the incident light in a simple face recognition system. Innovative strategies in both these people-dominated facets of the operation of authentication systems should be encouraged as the savings will be made directly on the cost of complete systems.

Looking further into the future, we can foresee a time when biometrics will be part of a 'fit and forget' culture, with cheap embedded systems forming part of the fabric of a world where computer processing is transparent and users expect systems to operate without the need for explicit intervention. In this scenario of ambient intelligence, the biometric will have a smart sensor and be significantly smaller than current models (even though the new range of silicon fingerprint devices approaches the limit of the human interface). The timescale for this type of environment is likely to be at least at the far end of the study period (2010), but an early demonstration of the functionality that could be achieved as part of an intelligent device fabricated using state of the art technologies would stimulate interest.

Summarising the longer term research issues for biometrics, we add the following research challenge:

RC/C10 RC - COMPONENTS 10 (LONG TERM): Among the longer term challenges for biometrics is the development of very cheap lightweight micro-sensors with integrated intelligence and context-awareness obtained by close integration with the application. In some instances these sensors will be embedded into the fabric of a service in a manner that will be transparent to the end user.

7.3 What are the critical issues?

On the basis of the studies undertaken in the BIOVISION Roadmap (and reviewed in Section 5), a large number of issues have been tabled (Appendix 1). The consortium has generally not looked at the challenges posed by individual technologies, nor considered the economic arguments for take-up²⁸⁷.

The consortium has noted that biometric technologies should be viewed as mechanisms that address one aspect of an application. Whether the use of biometrics enhances or reduces personal privacy, improves or worsens security, makes authentication more or less convenient, will depend on other features of the application. This is no different from many other technologies. It follows, therefore, that discussion of biometric performance, legality or usability should be in the context of a specific application. Moreover, the value of biometric methods - in improving security, convenience, etc - should be judged from the perspective of operators of services using these methods, and from the experience of the end users of such services.

For the early majority to consider investment in systems that are bought primarily to improve the **security** of systems, it is axiomatic that the systems themselves be warranted as secure. Some of the present lack of security in stand-alone devices themselves can be addressed in the secure design of integrated systems, but a new generation of devices and software is anticipated that will offer a higher level of intrinsic security, resistant to the spoofing attempts of college students. Although few suppliers will be able to pay for full accreditation to Common Criteria at EAL4, more informal testing by independent test

²⁸⁷ For an overview of the fundamental approaches to the economics of information security investments see Lawrence Gordon and Martin Loeb, *Economic Aspects of Information Security*, Rainbow Technologies White Paper (August 2001)

houses could provide a measure of reassurance. Governments acknowledge that the security of large-scale, government deployments is critical to their introduction, whereas many other operators may not recognise its importance.

Systems and services with biometric authentication must be **usable** by the end users. Not only must they be able to enrol large numbers of diverse people at the start of a deployment, but the performance must remain satisfactory over periods of years. In some applications, the system may be used only very infrequently by some individuals (e.g. in cross-border checks against an identity document), while others will be accessed on a daily basis. Strategies for fall back to an alternative method often appear to degrade the overall security; if frequent recourse to human intervention is called for, overall security may suffer, as well as cause others in the user community to question the viability of the solution. For some services, even small numbers of failures can have severe repercussions (e.g. at a supermarket checkout or immigration control). It is inevitable that some sections of the population will find it very difficult to use specific systems. These may be **disabled**²⁸⁸, lack the requisite feature in their body or just fail to meet the fundamental requirements for a particular way in which a specific method is implemented. Without extensive testing before the final commissioning of systems, the operator risks considerable annoyance to groups of customers and the consequent bad publicity that this can bring both to his service and to the use of biometrics in general.

Services that incorporate a biometric must also be operated in ways that respect the **legal requirements** with respect to data privacy, health and safety, etc. In spite of the moves towards harmonisation of these laws in the European Union, initial rulings point to a diversity of culturally-determined interpretations, which will cause difficulties for suppliers aiming to offer Europe-wide services. Although there are many exemptions for governments in these laws, society will require evidence of the need to take advantage of them.

The diversity of biometric methods, and the variety of ways in which a method is implemented by a supplier, should work in favour of the end user who is concerned about the possible sharing of biometric data across different applications. The arguments for interoperability of systems should be examined carefully lest users are disadvantaged. Although the existence of a multiply faceted identity for many people may disturb some commentators, it is difficult to justify the imposition of uniformity where there is no criminal intent to deceive or defraud. **User perceptions** of the introduction of biometrics could be adversely affected by an overbearing attitude. Preliminary evidence from the BIOVISION project appears to confirm the willingness to take part in biometric projects for the benefit of society, even though some of the citizens may still have concerns about the technology itself, whether about the **inference of medical conditions** or the potential of 'function creep'.

Operators of systems that will use a biometric, and suppliers of technology need usable **standards** that can simplify the procurement process and reassure operators that they will not be locked into a proprietary solution. Currently, the development of standards is being accelerated to meet the deadlines for the introduction of these methods into machine readable travel documents. Such standards could be too prescriptive for less demanding applications, even though customers - in their ignorance of the significance of a standard - may require supply of systems in conformance with an inappropriate standard.

Research projects should be designed to explore not only incremental improvement in the algorithms, but the impact of any improvements on the commercial viability of a product. There are numerous uncertainties about performance at the system level, which are not addressed by current programmes, and may require joint programmes with systems integrators and potential operators.

²⁸⁸ William Lawson, *Enhancing assistive technologies: through the theoretical adaptation of biometric technologies to people of variable abilities*, www.icdri.org/biometrics/enasstech.htm (19 February 2003)

7.4 The European Biometric Forum

Co-ordination of activities across the European Union has been identified as a key issue. Whether in sharing an understanding amongst national standards bodies; informing potential operators about the performance they may expect of a specific method; alerting a research team to similar work already being undertaken in another country; or bringing a sales opportunity to the notice of a potential partner in the same member state, the BIOVISION consortium has clearly identified the need for a European Biometric Forum. This will inform, share knowledge, offer impartial advice and act as a networking organisation. With the launch of the EBF in Dublin on 21 July 2003, the community of developers and users of biometric technologies has a common voice representing the vibrant diversity of all facets of the development of biometrics in Europe.

In support of this aim, the EBF's key tasks - as defined in the Consultation Document - include:

- the setting up of a demonstration centre to act as a showcase for technologies, applications and projects
- the initiation of Special Interest Groups that will work in specific areas of interest to the European biometrics community
- the organisation of a European Media Centre
- the facilitation of the formation of consortia to work together in research, development, deployment and promotion of awareness of biometric technologies
- the establishment of communication channels
- the organisation of annual conferences and workshops
- the encouragement of participation in national and international standards organisations

Further information is available at the website of the EBF:

<http://www.eubiometricforum.com>

APPENDIX 1: Research Challenges

A considerable investment in research has been made around the world. Examples of projects undertaken in Europe are listed in Appendix 3, and many others are still underway in the US and the Far East. As the world moves towards major deployments of biometric enabled systems, it is timely to consider where the scarce resources (of well-trained and motivated people, as well as financial resources) should be focussed. One of the aims of the BIOVISION project was to prepare a prioritised list of challenges, based upon a number of workshops that were held and the discussions and analysis that followed. A decision was taken to exclude consideration of the *individual* biometric technologies, thereby concentrating on issues that were common to many of the biometric methods.

A1.1 US Initiatives in determining a biometrics Research Agenda

In the USA, two initiatives with a similar aim have started with formal reports due in the Autumn of 2003. Firstly, the **National Science Foundation** sponsored a workshop in West Virginia in April with 55 participants, addressing four key questions in a cross-cutting way similar to the BIOVISION approach²⁸⁹ (parallel challenges identified by the BIOVISION consortium are noted in brackets):

- Biometric technologies: which are deployed now, available but not deployed, and under development with the prospect of being deployed in the foreseeable future?
Issues that were considered included:
 - template aging, (RC/C5)
 - multimodal fusion, (RC/C3)
 - operational performance modelling from test results
 - quality measures including distinctiveness (RC/C5)
 - overall system performance, including usability, comparison with other authentication system performance, optimising the performance of systems, impact of error, modelling of throughput, fallback using other biometric modalities (RC/Sec2) (RC/PS2) (RC/C1)
 - individual aspects of work on face recognition, fingerprint matching, iris recognition and speaker verification
- What measures of effectiveness are required to ensure that these aid higher levels of security?
 - fundamental limits of performance (RC/C2) (RC/C4)
 - assessment of performance of the methods under technology, scenario and operational evaluations, statistical method development, limits of accuracies and stability of the metrics,
 - effectiveness of fusion
 - scalability of large scale systems
 - large scale multimodal databases (RC/TTL4)
 - modelling of throughputs
 - impact of public understanding, habituation and use of incentives on the performance of systems
- What are the societal and political implications of these for personal security and preservation of individual liberties, and for lifestyles?
 - how does a biometric have a positive or negative impact on privacy, should privacy policies be encouraged and what should be in them? (RC/TTL7)
 - human factors and usability (RC/PS1) (RC/C8)
 - security of applications and systems, including measurement of perceived costs and benefits (RC/Sec1)

²⁸⁹ Raud Bolle *et al*, *Biometric research agenda: report of the NSF workshop* (1 July 2003)
<http://biometrics.cse.msu.edu/BiometricResearchAgenda.pdf>

- enrolment – security using breeder documentation, issues of unsupervised enrolment
 - differences between social acceptability of identification and verification (RC/TTL5)
 - impact on cost, usability and acceptance of factors such as mandatory use, standards, public or private use, data interchange between agencies
- What are cost-effectiveness tradeoffs in their implementation, the impact on productivity, and how is the workforce created?
 - modelling methodologies
 - how do you value the avoidance of very rare events such as 9/11?
 - undesirable side effects of the deployment of biometric systems
 - measurement of deterrent effect of a biometric
 - total cost modelling, including upgrade against move to an alternative system

A key recommendation is that biometrics should be recognised as a highly interdisciplinary endeavour with technical, economic, social and political dimensions, requiring R&D programmes that acknowledge this view (see our RC/SD1 and the general approach of the BIOVISION project)

The second activity stems from a **US Government workshop** held in Washington on 6 March 2003 which developed an agenda for applied research relevant to the interests of government, targeting those areas that were considered to be key to national security and prosperity²⁹⁰. Of the 30 areas of work which were identified at the meeting, the following were noted as HIGH priority:

- authentication systems for firing armaments
- biometrics operating outdoors in glare and shadow
- authentication of personnel in suits that protect against nuclear, chemical and biological contamination and warfare
- development of an enterprise architecture and implementation scheme across the Department of Defense, permitting multiple enrolment applications, usage at multiple sites with template repositories of various types
- developing a search front end for the millions of images of faces on the IAFIS mugshot file
- methods of verification of an individual's identity prior to enrolment, and ensuring that the link to individuals and their identity claim are consistent across all biometric-enabled systems
- collection of biometric data from unco-operative individuals in jails
- optimisation of fusion of biometric measurements
- understanding the upper bounds of performance of biometrics (RC/C2)
- improvement in the usability to end users of the front end of systems (RC/PS1)
- capture of facial images in a crowd, and then zooming in to obtain a high resolution image of the individual face
- faster throughput of individuals through systems using a biometric, specifically for school safety systems and jails
- understanding the limitations and capabilities of biometrics applied on the large scale (nationwide enrolment and use)
- defining standards for exchanging of 'watch lists'
- wireless transmission of biometric data in remote locations (cities or harsh environments) and return of results within minutes
- specific enrolment and verification of individuals in ships at port
- understanding the acceptance of biometrics by the public in an international context (RC/TTL5)

²⁹⁰ Duane Blackburn *et al*, 2003 *US government biometrics workshop: overview and summary* www.biometricscatalog.org, (9 April 2003)

- collection and searching iris images by law enforcement agencies (extension to IAFIS)
- long term stability of the biometric measures to determine frequency of re-enrolment of individuals. (RC/C5)

A1.2 The BIOVISION Research Agenda

During the 14 months of the BIOVISION project, a number of opportunities were sought to identify these key challenges. Individual study areas (security, legal, standards, medical aspects and applications) contributed insights from their research. Further inputs were gained from comments by participants to the BIOVISION Rome workshop in January 2003. The list (of which this is a part) was then formed into a questionnaire that was mailed to a group of key opinion formers in the biometrics community. Based on the results of this limited study, those aspects that were judged to be particularly important research areas have been labelled as **KEY PRIORITY AREAS**. Others that were considered important have been labelled as **IMPORTANT AREA**. Note that the first two challenges were not included in the questionnaire and that some of the challenges have been clustered together in this summary.

These research topics should not be taken individually in isolation. Addressing one (or even a few) in isolation will not progress the development of successful deployments. More specifically, in any research proposals, the proposers should consider justifying the selection of specific research topic areas by the impact that a successful resolution will have on increase in the wider acceptability of biometrics, either for all uses, or in the specific application are under consideration. This information may not be available at the outset of a project, but should be considered during its development

Research Activities

RC/RA: RC - RESEARCH ACTIVITIES: Following the initial phase of establishing research teams throughout European organisations, funding bodies should now ensure that new research projects are based upon a solid appreciation of both the current status of the research as well as the realities of commercially viable deployments. If the European biometrics sector is to flourish, timely sharing of knowledge between the research and commercial sector is vital.

FUNDAMENTAL (Not assessed)

Systems and Design

RC/SD1: RC - SYSTEMS and DESIGN 1: Successful implementation of systems using biometric methods requires an inter-disciplinary design approach. There are few specialist designers able to put together an integrated design that addresses the already documented issues and concerns.

FUNDAMENTAL (Not assessed)

RC/Sec1: RC - SYSTEMS AND DESIGN: SECURITY 1: Methods are required to evaluate and compare the security of biometric systems. Schemes other than the Common Criteria framework should be investigated for their suitability. The level of security should appropriate to the application and the risks involved. In particular the binding of the application to the result of the biometric authentication has to be secure. In view of the value of databases of biometric identifiers to other people and organisations, these may need to be secured against both internal and external threats using state-of-the-art techniques. Appropriate security is also required for the templates during their transmission between database and application. All security measures subject should be periodically subject to a review.

KEY PRIORITY AREA

(except for alternatives to Common Criteria and transmission of templates; database security is viewed as an **IMPORTANT AREA**)

RC/Sec2: RC - SYSTEMS AND DESIGN: SECURITY 2: Methods for the design and secure implementation of appropriately secondary systems that cope with both false match and false non-match errors. Such strategies may be required to operate in a gradual manner.

KEY PRIORITY AREA

RC/Sec3: RC - SYSTEMS AND DESIGN: SECURITY 3: Development of design methodologies that support the secure integration of biometric data in applications such as the Criminal Justice Sector, while limiting the opportunity for misuse and 'function creep'. These could make use of binding of the user's identity, the application, template and user's expression of consent as well as validation by external Trusted Third Parties.

KEY PRIORITY AREA

RC/Sec4: RC - SYSTEMS AND DESIGN: SECURITY 4: Biometric data for different applications (or held centrally and on-card) may require to be of different types (or held in incompatible formats) in order that centrally held information cannot be misused.

RC/Sec5: RC - SYSTEMS AND DESIGN: SECURITY 5: Provision of 'live and well' features in biometric systems is a high priority, especially when these are unattended or only intermittently attended by security personnel. Testing of the liveness of the biometric signal needs to be commensurate with other security aspects of the system

KEY PRIORITY AREA

RC/Med: RC - SYSTEMS AND DESIGN: MEDICAL ASPECTS: Further development of the BIOVISION methodologies for ensuring health and safety in systems using biometrics and the non-disclosure of medical conditions.

Deployments

RC/Dep: RC - DEPLOYMENTS 1: The impact of a high profile failure in the application of a biometric method could impact on the willingness of other customers to specify such methods, and adverse media comment could increase the resistance to their use by individuals and groups.

Trials, Testing, Legal, etc

RC/TTL1: RC - TRIALS, TESTING, LEGAL, etc 1: There is no clear ethical framework for the development and use of biometrics. To some extent this will be determined by individual societies and cultures. However, currently, the agenda is set by cost-benefit analysis for improved security, without reference to a more fundamental assessment of the advisability of cross-application unique identification of individual citizens and consumers.

IMPORTANT AREA

RC/TTL2: RC - TRIALS, TESTING, LEGAL, etc 2: Social and socio-psychological research should be encouraged to understand how identities and personas are used at present, and the implication of the use of biometrics on legitimate expression of such multiple identities.

RC/TTL3: RC - TRIALS, TESTING, LEGAL, etc 3: The impact of long term exclusion of those unable to make use of certain biometrics.

IMPORTANT AREA

RC/TTL4: RC - TRIALS, TESTING, LEGAL, etc 4: A programme of database construction and testing should be initiated especially for those biometric methods for which such large scale databases are still not collected or publicly available. Certain biometric methods (e.g. multimodal biometrics) will require specific algorithm testing schemes and research may be required to devise the most appropriate methods.

KEY PRIORITY AREA

RC/TTL5: RC - TRIALS, TESTING, LEGAL, etc 5: Further research is needed, based upon the initial proposals in the BIOVISION project, that will test perceptions by end users and the social groups of which they are members. This should also examine the evolution of such perceptions and whether different techniques apply to other social groups and cultures.

IMPORTANT AREA

RC/TTL6: RC - TRIALS, TESTING, LEGAL, etc 6: Tools and methods for the forensic investigation of the abuse of biometric methods.

RC/TTL7: RC - TRIALS, TESTING, LEGAL, etc 7: Further development of the Best Practices, based upon experience of similar codes in other fields. One specific application could be in the integration with Privacy Impact Assessments, together with advice to auditors confirming the adherence to such a Code.

IMPORTANT AREA

RC/TTL8: RC - TRIALS, TESTING, LEGAL, etc 8: Further studies should continue to monitor the progress towards a uniform interpretation of the privacy issues surrounding the use of biometrics in the countries of the EU (including the Newly Accessioning States), and support the activity of the Article 29 Working Party with impartial information about developments in biometrics. Users' experience in the application of biometrics should be collated and interpreted with the aim of either lobbying for a revision in the legal regime or for retention of the *status quo*.

RC/TTL9: RC - TRIALS, TESTING, LEGAL, etc 9: The status of those unable to use the preferred biometric solutions should be recognised, whether these are in the private or in the public sector. Solutions are required that will limit the long term exclusion of such individuals from the opportunities offered by uniform secure authentication.

RC/TTL10: RC - TRIALS, TESTING, LEGAL, etc 10: Work is required to develop a framework for the legal admissibility of biometric data. This should build upon the existing procedures for scene of crime fingerprints and handwritten signatures.

Products and Solutions

RC/PS1: RC - PRODUCTS AND SOLUTIONS 1: Transparent - yet not covert - systems with excellent adaptive user interfaces, delivering apparently 'instantaneous' authentication for end users

KEY PRIORITY AREA

RC/PS2: RC - PRODUCTS AND SOLUTIONS 2: Systems that are easy to install securely, with useful and appropriate feedback if they fail

KEY PRIORITY AREA**Components**

RC/C1: RC - COMPONENTS 1: R&D effort is required to improve the *operational* performance of existing biometric systems. In some cases, the error rates are substantially below what is required for the applications for which they are sold, and 'quantum' improvements in their performance may be required.

IMPORTANT AREA

(Not for quantum improvements in performance)

RC/C2: RC - COMPONENTS 2: There is little understanding of the fundamental limits to the performance that could be attained using a specific biometric

RC/C3: RC - COMPONENTS 3: In view of the limitations of individual biometric methods, further research is needed to optimise the performance of multi-modal biometrics. This should focus on improvements in the approach to fusion of measures, as well as to address the requirements of specific applications and services

RC/C4: RC - COMPONENTS 4: Research into the ultimate limits of performance with various methods of implementing specific biometric techniques

RC/C5: RC - COMPONENTS 5: Research into the 'uniqueness' of a template, and the extent to which it depends upon demographic factors such as gender, age, ethnicity, etc. Do such templates exhibit stability over extended periods of time (> 5 years)?

RC/C6: RC - COMPONENTS 6: A methodology to determine whether novel methods of using the human body for secure authentication are worth supporting

RC/C7: RC - COMPONENTS 7: Use of DNA as a biometric, including the development of protection mechanisms.

RC/C8: RC - COMPONENTS 8: Systems that minimise the mental and physical load on the end user, particularly if that end user is physically or mentally disabled.

RC/C9: RC - COMPONENTS 9: Performance improvements are needed to reduce the possibility of chance matches between different people, and for identification of non-cooperative users in negative identification applications

RC/C10: RC - COMPONENTS 10 (LONG TERM): Among the longer term challenges for biometrics is the development of very cheap lightweight micro-sensors with integrated intelligence and context-awareness obtained by close integration with the application. In some instances these sensors will be embedded into the fabric of a service in a manner that will be transparent to the end user.

RC/Csupp: RC - COMPONENTS (Supplementary): Smart sensor development to improve performance, scalability, functionality, etc

KEY PRIORITY AREA

Standards

RC/S1: RC - STANDARDS 1: Interface standards are needed for all aspects of the operation of systems using a biometric. These should be in a form that is easily used by the design community and readily applicable to the variety of applications that are described in this roadmap.

KEY PRIORITY AREA

RC/S2: RC - STANDARDS 2: The prime driver of standardisation appears to be early application to border security and towards improvements in the physical security of transportation systems (especially in airports). Will this impact upon the usefulness of such standards in other application areas?

RC/S3: RC - STANDARDS 3: Standards should be appropriate for specific application areas (including the legal and societal context). Work on 'profiles' should be grounded in case studies of existing and proposed systems


KEY PRIORITY AREA

RC/S4: RC - STANDARDS 4: Work to support the standards activities in testing, validating, accrediting and accepting deployed systems at the hardware, algorithm and user acceptance levels.

KEY PRIORITY AREA

RC/C5: RC - STANDARDS 5: Although a study group (SG6) has been formed to examine legal and societal aspects of standardisation, historically, standards bodies have been reluctant to develop international standards in this area. At present, the usefulness (and acceptability to some national bodies) of such a standard remains to be proven.

RC/C6: RC - STANDARDS 6: Relatively few players are taking an active role in the development of standards, even though standardisation initiatives are being accelerated to meet the requirements of border control applications. Other national bodies (including many in the EU) are unaware of the implications of such standards. Sharing of knowledge should be encouraged through the formation of a European special interest group.



APPENDIX 2: Current biometric R&D and innovation in Europe

This incomplete list provides a first attempt at an inventory of the institutions that undertake research and development into biometrics and biometric-related fields in the European Union, or have a significant involvement in sponsoring or driving the research agenda in Europe. This list will be updated in future issues of this roadmap. Any specific expertise is identified by the abbreviation of the technology, although many institutions conduct research in a number of methods and applications.

AFR: Automatic Face Recognition

DEPL: Innovative deployments (with subsidiaries of non-European companies)

DNA: DNA analysis for biometrics

DSV: Dynamic Signature Verification

E: Ear shape analysis

FV: Fingerprint Verification

G: Gait Recognition

HG: Hand Geometry

HV: Hand vein systems

KD: Keystroke Dynamics

IA/PR: Image Analysis and/or Pattern Recognition

ID: Identification systems

INT: integration

IR: Iris recognition

L: Lip movement analysis

MM: multimodal biometrics

RR: Retinal recognition

SV: Speaker verification

Organisation	Activity	Contact	Website
Austria			
Joanneum Research, Graz	FV, IA/PR		
Belgium			
Keyware Technologies	Identity management solutions	Christian Halet	http://www.keyware.com
Louvain, Universite catholique de			
RMA/SIC Brussels			
SITA (international services organisation)	Air security applications	Michel Saunier	www.sita.int
Denmark			
Open Business Innovation	Privacy	Stephan Engberg	
Finland			
Joensuu, University of			
Lappeenranta University of Technology			
Nokia Research and Technology Access, Oulu			
France			
Atmel	FV		www.atmel.com
Avignon, Univerisite d' et des Pays de Vaucluse			
ENST, TSI (Paris)			
Eurecom Institut,			

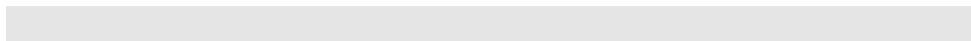
Sophia Antipolis			
Evry, University			
GET, Groupe des Ecoles de Telecommunication	DSV, MM		
INT	MM	Prof. Bernadette Dorizzi	www.int-evry.fr
IRISA (CNRS & INRIA), Rennes			
LIS, Grenoble			
Sagem	FV, ID, AFIS		www.sagem.com
Thales Research and Technology			
Germany			
Bergdata	FV		www.bergdata.com
Berlin, Fraunhofer IPK	Systems	Katrin Franke	
BSI	Security	Dr. Astrid Albrecht	www.bsi.de
B&L Management Consulting	Consultants	Veronika Nolde	www.bulmc.de
Bundesdruckerei	ID		www.bundesdruckerei.de/en/index.html
Cognitec	AFR	Alfredo Herrera	http://www.cognitec-systems.de/index.html
Darmstadt, Fraunhofer Institut Graphische Datenverarbeitung		Christoph Busch, Henning Daum	
Darmstadt, Fraunhofer Institute for Secure Telecooperation FhG-SIT		Dr Dirk Scheuermann	
Dermalog	FV		www.dermalog.de
Deutsche Bank	INT		
Erlangen, Fraunhofer-Institute for Integrated Circuits			
Giesecke & Devrient	FV, ID systems		
Giessen-Friedberg: University of Applied Sciences	Applied biometrics	Prof. Michael Behrens	
Guardeonic Solutions		Dr. Brigitte Wirtz	www.guardeonic.com
Hitex GmbH	FV	Dieter Baur	www.hitex.de
Infineon	FV		www.infineon.com
Magdeburg, University of	DSV		
Saarbrücken, Max-Planck-Institut			
Softpro	DSV	Dr Christiane Schmidt	www.softpro.de
ZN-Vision	AFR	Dr.-Ing. Stefan Gehlen	http://www.zn-ag.com/
Greece			
Expertnet SA	General	Christos Dimitriadis	http://www.expertnet.net.gr/bee/index2.html
ICCS-NTUA		Dr. Despina Polemi	http://secgroup.iccs.ntua.gr/home.htm
Net Smart		Lefteris	www.netsmart.gr

		Leondaridis	
Thessaloniki, Aristotle University of	AFR		
Ireland			
Daon	INT	Martin Walsh	www.daon.com
Dublin, University College			
Voice vault	SV		www.buytel.com
Italy			
Bari, Istituto di Studi sui Sistemi Intelligente per l'Automazione, CNR			
Bologna, University of, Biometric Systems Laboratory	FV	Davide Maltoni	http://bias.csr.unibo.it/research/biolab/bio_tree.html
Cagliari, University of			
CNR	Medical Standards	Mario Savastano	
Milan, Università degli Studi di Milano			
Sassari, University of	AFR, MM		
Ugo Bordoni, Fondazione	SV		
Luxembourg			
The Netherlands			
CWI, Centre for Mathematics and Computer Science, Amsterdam	IA/PR	Ben Schouten	
Dartagnan Biometric solutions	INT		www.dartagnan-biometrics.com
Enschede/Sdu	ID systems		www.enschede-sdu.nl/eng/frmiid.html
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	ID systems		
Philips Research, Eindhoven			
TNO, Organisation for applied scientific research	Security, testing		
Twente, University of,	Hand grip	Professor Pieter Hartel	
Portugal			
Spain			
S.L. Barcelona			
Barcelona, Universitat Politècnica de Catalunya			
FNMT, Fabrica Nacional de Moneda y Timbre	Fingerprint, INT		http://www.fnmt.es/hta/taid/cc_taid_ta.html
Madrid, University Carlos III de	Ear		
Madrid, Universidad Politécnica de	SV, Ear		www.atvs.diac.upm.es

Murcia, Universidad de Telefonica	INT	Orestes Sanchez Benavente	www.tid.es
Valencia, Universidad Politecnica de			
Vigo, Universidad de	SV, IA/PR		
Zaragoza, Universidad de	G		
Sweden			
Fingerprint Cards AB	FV		www.fingerprint.se
Halmstad University	FV		
Precise Biometrics	FV		www.precisebiometrics.com
United Kingdom			
Aurora Computer Services	AFR		
AX-S Biometrics Ltd	INT	Richard Ashwell	www.ax-sbiometrics.com
Avanti	INT	Julian Ashbourn	homepage.ntlworld.com/avanti
BT Exact	System issues, privacy and social concerns, standards	Marek Rejman-Greene	www.btexact.com
BTG	HV, DSV	Peter Hawkes	www.btgplc.com
CESG	Security	Philip Statham	www.cesg.gov.uk/biometrics
De La Rue	ID systems	Bob Carter	www.delarue.com
Domain Dynamics	SV		www.ddl.co.uk
Edinburgh University	SV		
Forensic Science Service	SV, FV	dr. Didier Meuwly	http://www.forensic.gov.uk/forensic/entry.htm
Glasgow, University of, Department of Psychology			
Glasgow Caledonian University	Legal Admissibility, AFR, DNA	Michael Bromby	http://cbs1.gcal.ac.uk/law/users/~mbro/index.htm
Hertfordshire, University of		Aladdin Ariyaeinia	
HP Laboratories, Bristol	Security		http://www-uk.hpl.hp.com/mcs/
Huddersfield, University of			
IBM, Hursley Park	Various		www.ibm.com
Identix (US)	AFR, FV DEPL		
Imagis (Canada)	AFR DEPL		
Imperial College, University of London			
ISL	INT	Derek McDermott	www.informer.co.uk
Kingston University			
Kent at Canterbury, University of	DSV, others	Prof Mike Fairhurst	http://www.ee.kent.ac.uk/research/elecsys/image/image.html
Manchester University	AFR	Dr Tim Cootes	
National Physical	Testing	Dr Tony	www.npl.co.uk

Laboratory		Mansfield	
Nationwide Building Society	DSV, others	Will McMeechan	
Neurodynamics	AFR, FV		http://www.neurodynamics.com/BIOMETRICS/biometrics_home.htm
Nuance (US)	SV DEPL		
OmniPerception Ltd	AFR	Dave McIntosh	www.omniperception.com
Plymouth University	KD		
Police IT Organisation (PITO)	Criminal Justice apps	Clive Reedman	www.pito.org.uk
Queen Mary College, University of London			
QinetiQ	INT		www.qinetiq.com
Securivox	SV		securivox.co.uk
Sharp Laboratories of Europe	Smart card		www.sle.sharp.co.uk
Sheffield University	DNA	Martin Evison	
Stirling University	AFR, Recognition of faces by people	Prof Vicky Bruce	
Southampton University	G, Ear, SV	Prof Mark Nixon	http://www.isis.ecs.soton.ac.uk/image/gait/
Surrey, University of: Centre for Vision Speech and Signal Processing	AFR, MM, L	Prof Josef Kittler	www.ee.surrey.ac.uk/CVSSP
TSSI	FV, INT	Pat Oldcorn	www.tssi.co.uk
University College London	User and privacy concerns	Dr Angela Sasse	
Wales, University of (at Swansea)	SV	Dr J S Mason	
Other European Countries			
Croatia			
Zagreb, University of	HG, Palm	Dr S Ribaric	www.zemris.fer.hr
Hungary			
Guardware Systems	FV		www.guardware.com
Lithuania			
Neurotechnologija	FV, Iris		www.neurotechnologija.com
Poland			
Warsaw University of Technology	DSV, IR, HG	Andrzej Pacut, Adam Czajka	www.ia.pw.edu.pl/en/research/projects/biometrics
Russia			
A4Vision			
Slovenia			
Ljubljana, University of			
Switzerland			
Bern, University of			
Biomet Partners	HG		www.biomet.ch
EPFL, STI-ITS, Lausanne			
Fribourg, University of	SV		
IDIAP (Institute for Perceptual Artificial			

Intelligence), Martigny			
Idencom AG	FV	Qiu-Ping Zeng	www.idencom.com
Iridian (US)	Iris DEPL		
Swiss Federal Institute of Technology, Lausanne			www.epfl.ch



APPENDIX 3: Research Projects in Biometrics

Research projects that include some elements of a biometric include (unless otherwise stated these are, or were, EU funded):

Acronym	Name	Completion Date	Website	Comments
ASPeCT		Aug 1998	http://www.cordis.lu/info-win/acts/rus/projects/ac095.htm	Telecommunications
BANCA	Biometric Access Control for Networked and e-Commerce Applications	Jan 2003	http://falbala.ibermatica.com/banca/index.html	
BEE	Business Environment of Biometrics involved in Electronic Commerce	Feb 2002	http://www.expnet.gr/bee/index2.html	
BIOTEST	Biometric testing services	Oct 1998	http://www.cordis.lu/esprit/src/21978.htm	Testing biometrics
BVN	BIOVISION-Roadmap for Biometrics in Europe to 2010	July 2003	http://www.eubiometricforum.com	The present project
CAVE	European Caller Verification Project	Apr 1997	http://www.kpn-telecom.nl/cave	Speaker verification for phone applications
COST 275	Biometric-based recognition of people over the Internet	Jun 2005	http://www.fub.it/cost275	Application of voice and face; 4m euro project
E-POLL	Electronic polling system for remote voting operations	Aug 2002	http://www.e-poll-project.net/innovations.htm	Fingerprint verification for electronic voting
EUCLID	European Initiative for a Citizen digital ID solution	Nov 2003	http://www.electronic-identity.org	Provides resources for the eEurope Smart Card Trailblazer 1 <i>Public Identity</i>
FINGER_CARD		Jun 2002	http://www.hsb.nl/finger_card.html	Integrated fingerprint sensor on smart card, and applications
FG-net	European group on face and gesture recognition	ongoing	http://www-prima.inrialpes.fr/FGnet/html/home.html	Foresight reports and development of data sets. Improvement in interpretation of CCTV images.
HISCORE	Hi-speed 3D	2000?	http://uranus.ee.auth.gr/h	Enhanced CCTV

	and colour interface to the real world		iscore	with colour and 3D
IAMBIC	Intelligent Agents for multimodal biometric identification and control	2003	http://www.iambic-project.org/	(UK) Online secure access control for health sector using multimodal biometrics
M2VTS	Multimodal verification for Teleservices and Security Applications	Sep 1998	http://www.cordis.lu/info/win/acts/rus/projects/ac102.htm	Face and speech fusion
PAIDFAIR	Protecting Accumulated Intellectual Data for Accounting in Real Time	Nov 2002	http://virtualgoods.tu-ilmenau.de/2003/VG_Co-demeter.pdf	Fingerprint verification for digital rights management
PICASSO	Pioneering caller authentication for secure service operation	Jul 2000		Speaker verification for secure telematics transaction services by voice
PUMA	Personalised User interfaces for information Management and Authorisation	ongoing	http://www.dti-mi.org.uk/newweb/puma.htm	(UK) Fraud resistance of mobile phone and data services using SV
RETRIEVE	Realtime Tagging and Retrieval of Images Eligible for use as Video Evidence	Nov 2002	http://www.retrieve-project.org/	Aim was to enhance CCTV surveillance systems by providing effective search and retrieval mechanisms for archived digital material.
SABRINA	Secure Authentication by a Biometric Rationale and Integration into Network Applications	ongoing	http://www.sabrina.uni-karlsruhe.de/publicdescription.html	Miniature ultrasonic fingerprint sensor
SCID	Secure Customer Identification for Drive-in Retailing	ongoing	http://www.dti-mi.org.uk/newweb/scid.htm	(UK) Face recognition for 'drive in' retail applications
s-Travel	Secure-Travel	Apr 2004	FP5 dataabse search at http://dbs.cordis.lu/fep/FP5/FP5_PROJ1_search.html	Use of biometrics, smart cards and digital certificates to improve travel security; trial between Athens and

				Milan in late 2003; business model, privacy and user issues considered
TASS	Smart cards with fingerprint biometrics to allow employee access to data about their social security entitlements	1995 - Ongoing	http://www.fnmt.es/html/taid/cc_taid_ta.html	Spain. 7m cards issued to date. Project started in 1995 in Cordoba and aim is to complete nationwide deployment.
TSWG Task T-1595	Statistical Analysis of Forensic Friction Ridge Matching Criteria	Ongoing		UK Forensic Science Service and Switzerland
TVID	Speaker verification over the telephone network		http://www.speech.kth.se/~melin/proj/spver.html	(Sweden)
U-FACE	User friendly face access control system for physical access and healthcare applications	Oct 2002	http://www.uface.org	Face Recognition
ViPBoB	Virtual PIN Based on Biometrics	Feb 2004	http://vipbob.gi-de.com/vipbob/index.html	Encryption to support privacy and security
VIRSBS	Visual intelligent recognition for secure banking services	Feb 1999	http://www.cordis.lu/ist/98vienna/xvirsbs.htm ; http://www.aramis-research.ch/e/6165.html	Facial recognition at ATM machines
Waby	Integration of face image capture and recognition systems for real time use			(NL) Aiming for high security with high speed and a good user experience
ZAVIR	Ascribability of Actions in the virtual world	Dec 2003	http://www.sit.fhg.de/ZAVIR/ZAVIReng.html	(Germany) DSV biometrics applied to electronic signature use

Glossary: acronyms and vocabulary

Acronyms

AFIS	Automated Fingerprint Identification System
AFNOR	Association française de normalisation, French national standards body
AFR	Automatic Face Recognition
ANSI	American National Standards Institute http://www.ansi.org/
APACS	(UK) Association for Payment Clearing Services
API	Application Programming Interface
ATM	Automatic Cash Dispenser used by banks
BANTAM	Biometric and Token Technology Application Modelling Language
BEE	A European Commission funded Biometrics project examining the economic, technical and social context for the adoption of biometrics in Europe
B-SAD*	Biometric Standard Application Description methodology as applied to requirements capture
BSI	Bundesamt für Sicherheit in der Informationstechnik, the German federal security agency, www.bsi.bund.de
BVN	An abbreviation for the BIOVISION project
BWG	Biometric Working Group, funded by the UK government, http://www.cesg.gov.uk/technology/biometrics/
CC	Common Criteria (for security accreditation)
CCTV	Closed Circuit Television systems (generally used in security surveillance)
CESG	Communications-Electronic Security Group (UK)
CRM	Customer Relationship Management system
DSV / DSR	Dynamic Signature Verification or Recognition
EBF	European Biometric Forum, a new European organisation for all stakeholders in the biometric community in Europe, formed in July 2003 www.eubiometricforum.com
EC	European Commission
EoI	Expression of Interest (for Sixth Framework)
EU	European Union (of 15 member states)
FAR	False Accept Rate
FRR	False Reject rate
FTE	Failure to Enrol in a biometric
HCI	Human Computer Interaction
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technologies
ID	Identity (as in identity card)
IEC	International Electrotechnical Commission http://www.iec.ch
ISO	International Standards Organisation http://www.iso.org
IST	Information Society Technologies
LED	Light Emitting Diode, a semiconductor light source
NIST	(US) National Institute of Standards and Technology http://www.nist.gov/public_affairs/factsheet/biometrics.htm
NHS	National Health Service (the UK's public medical service)
NPL	National Physical Laboratory (UK) http://www.npl.co.uk/
PET	Privacy-Enhancing Technology
PIN, pin	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point of Sale
PR	Public Relations
R&D	Research and Development
RSPCA	Royal Society for the Prevention of Cruelty to Animals (UK)
SIA	Semiconductor Industry Association (US) http://www.semichips.org
TRM	Technology Roadmap
UCD	User Centred Design
UPI	User Psychology Index
WP	Workpackage

Vocabulary

A number of glossaries of terms have been produced, some of which have gained greater acceptance by the biometrics community. Working Group 1 of the SC 37 standards subcommittee is charged with developing a harmonised vocabulary. In the interim, the Roadmap document bases its usage on that of the 1999 Glossary of Biometric Terms produced by the Association for Biometrics and the International Computer Security Association²⁹¹. Where there is a divergence from the AfB/ICSA definitions in the following table, this is indicated by a star (*).

AFIS (Automated Fingerprint Identification System)	A highly specialised biometric system that compares a single finger image with a database of finger images. AFIS is predominantly used for law enforcement, but is also being put to use in civil applications. For law enforcement, finger images are collected from crime scenes, known as latents, or are taken from criminal suspects when they are arrested. In civilian applications, finger images may be captured by placing a finger on a scanner or by electronically scanning inked impressions on paper.
Algorithm	A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match.
API	Application Programme Interface. An API is computer code used by an application developer. Any biometric system that is compatible with the API can be added or interchanged by the application developer. APIs are often described by the degree to which they are high level or low level. High level means that the interface is close to the application and low level means that the interface is close to the device.
Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.
Authentication	Alternative term for Verification . See also section 1.2.2
Behavioural biometric	A biometric that is characterised by a behavioural trait that is learnt and acquired over time rather than a physiological characteristic.
Binning	Binning is the process of classifying biometric data.
Biometric	A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee.
Biometric application	The use to which a biometric system is put.
Biometric data	The information extracted taken from the biometric sample and used either to build a reference template or to compare against a previously created reference template.
Biometric engine	The software element of the biometric system which processes biometric data during the stages of enrolment and capture, extraction, comparison and matching.
Biometric device	The part of a biometric system containing the sensor that captures a biometric sample from an individual.
Biometric sample	Data representing a biometric characteristic of an end-user as captured by a biometric system.
Biometric system	An automated system capable of: <ul style="list-style-type: none"> - capturing a biometric sample from an end user; - extracting biometric data from that sample; - comparing the biometric data with that contained in one or more reference templates; - deciding how well they match; and - indicating whether or not an identification or verification of identity has been achieved.

²⁹¹ The full glossary is available at www.afb.org.uk/docs/glossary.htm (used with permission)

Biometric technology	A classification of a biometric system by the type of biometric.
Capture	The method of taking a biometric sample from the end user.
Certification	The process of testing a biometric system to ensure that it meets certain performance criteria. Systems that meet the testing criteria are said to have passed and are certified by the testing organisation.
Comparison	The process of comparing a biometric sample with a previously stored reference template or templates. See also One-To-Many and One-To-One .
Claim of identity	When a biometric sample is submitted to a biometric system to verify a claimed identity.
Claimant	A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.
Closed-set identification	When an unidentified end-user is known to be enrolled in the biometric system. Opposite of Open-Set Identification .
* Credentials	Documents, tokens, information or data that establish or confirm an individual person's rights and privileges. (Note that the production of adequate credentials need not involve disclosure of identity. Proof of Class Membership may be necessary and sufficient.)
Database	Any storage of biometric templates and related end user information.
* Disruptor	A person who disrupts (or attempts to disrupt) the correct operation of a biometric system for human identification. Successful disruption leads to the system providing false decisions or scores to the application or failing to operate at all.
Eigenface	A method of representing a human face as a linear deviation from a mean or average face
End user	A person who interacts with a biometric system to enrol or have his/her identity checked.
Encryption	The act of converting biometric data into a code so that people will be unable to read it. A key or a password is used to decrypt (decode) the encrypted biometric data
Enrollee	A person who has a biometric reference template on file.
Enrolment	The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
Enrolment time	The time period a person must spend to have his/her biometric reference template successfully created.
Equal error rate	The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.
Extraction	The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Failure to acquire rate	The frequency of failure of a biometric system to capture and extract biometric data (comparison data).
Failure to enrol	Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).
False acceptance rate	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts.
False match rate	Alternative to False Acceptance Rate . Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of 'False Acceptance' and 'False Rejection'.
False non-match rate	Alternative to False Rejection Rate . Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of False Acceptance and False Rejection
False rejection rate	The probability that a biometric system will fail to identify an enrollee, or

	verify the legitimate claimed identity of an enrollee.
Field test or trial	A trial of a biometric application in 'real world' as opposed to laboratory conditions.
*Function creep	Extension of the use of biometric data to secondary applications and services that were not initially envisaged in the specification of the primary service.
Goats	Biometric system end users whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.
Identification	The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with Verification . (See also section 1.2.2)
Impostor	A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee.
Iris recognition	A physical biometric that analyses iris features, found in the coloured ring of tissue that surrounds the pupil
Matching	The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.
Minutiae	Small details found in finger images such as endings of ridges (the raised markings found across the fingertip) or bifurcations (branches made by more than one finger image ridge).
Multiple biometric	A biometric system that includes more than one biometric system or biometric technology.
One-to-many	Synonym for Identification .
One-to-one	Synonym for Verification .
Open set identification	Identification, when it is possible that the individual is not enrolled in the biometric system. Opposite of Closed-Set Identification .
Physical/physiological biometric	A biometric which is characterised by a physical characteristic rather than a behavioural trait. However, behavioural elements may influence the biometric sample captured
PIN (Personal Identification Number)	A security method whereby a (usually) four digit number is entered by an individual to gain access to a particular system or area.
Recognition	The preferred term is Identification .
Response time	The time period for a biometric system to return a decision on identification or verification of a biometric sample.
Score	The level of similarity from comparing a biometric sample against a previously stored template.
(Dynamic) signature verification	A behavioural biometric that analyses the way an end user signs his/her name. The signing features such as speed, velocity and pressure exerted by a hand holding a pen are as important as the static shape of the finished signature
Template	Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.
Template ageing	The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.
Threshold	The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.
Throughput rate	The number of end users that a biometric system can process within a stated time interval.
Type 1 error	In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the

	claimant is genuine, in which case this error corresponds to a False Rejection .
Type 2 error	In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a False Acceptance .
User	The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system
Verification	The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with Identification
Zero effort forgery	Where an impostor uses his or her own biometric sample and claims the identity of a different enrollee

Diagrammatic Form of a Roadmap

Roadmap: Diagrammatic Representation of an Idealised Roadmap (partly based on Groenvald (1997))

