AMTEC Consulting plc
Excalibur House
2 The Millennium Centre
Crosby Way, Farnham
Surrey GU9 7XX

Tel 01252 737866
Fax 01252 737855
Email post@amtec.co.uk
Web www.amtec.co.uk

AMTEC
CONSULTING GROUP

REPORT TO

IMMIGRATION & NATIONALITY DIRECTORATE

ON

CO-ORDINATION & MANAGEMENT OF BIOMETRICS

A company within the
AMTEC Consulting Group

Registered in England and Wales
No 2991335

Registered Office Excalibur House
2 The Millennium Centre Crosby Way
Farnham Surrey GU9 7XX

This report, reference AM/4599/R V1.0e, is in response to a requirement from the Immigration and Nationality Directorate to provide consultancy on the Co-ordination and Management of Biometrics.

Reference:	AM/4599/R V1.0
Prepared by:	John Elliott Neil Garner Bill Perry
Reviewed by:	Andrew Chapman Tony Mansfield (NPL)
Issue Date:	13 May 2003

AMTEC CONSULTING GROUP

CONTENTS

1 MANAGEMENT SUMMARY

AMTEC Consulting undertook this study for the Immigration and Nationality Directorate to provide consultancy on the Co-ordination and Management of Biometrics. This study was conducted in order to establish a governance framework for the co-ordinated planning, development and implementation of biometrics in support of IND's policy objectives. The duration of this study was five weeks.

1.1 Objectives

This study was conducted in order to establish a governance framework for the co-ordinated planning, development and implementation of biometrics in support of IND's policy objectives.

The study is specifically aimed at the use of biometrics to meet IND requirements for identity and verification of persons. Whilst the requirements of bodies outside IND are touched upon, as are more generic identity and verification techniques, such information should be seen as background, provided to establish the context within which this study sits, and not as part of the core deliverable.

1.2 Approach

We approached this work by performing a number of tasks in parallel in order to complete the work on time.

- **Stage 1 - Review current position**.
- **Stage 2 – Conduct interviews**. Around 30 interviews were performed with internal and external stakeholders
- **Stage 3 – Define requirements and produce model.**
- **Stage 4 – Review external influences.**
- **Stage 5 – Assess policy implications and develop framework.**
- **Stage 6 – Present and report.** This document is a draft of the final report.

1.3 Key findings

1.3.1 Co-ordination within IND

- There is some detailed experience of biometrics within IND. Most of this is concentrated within a very small number of staff within IAFP and specialises in fingerprint technology. There are other pockets of experience but not in the same detail in the areas of specification, procurement, benchmarking/evaluating, roll-out and management of live biometrics systems.
- There is no agreed clear IND-wide biometric strategy for all parts of IND to align with. This is not surprising, since this is the main reason for this study, but is worth stating.

- As technology matures, projects wishing to use biometrics are appearing more and more frequently. There appears to be no mandatory central control for approving these technology projects.
- Co-ordination of internal communications relating to biometrics would benefit from some improvement. Progress towards a common goal may be improved if the apparent technology 'camps' could co-operate more closely.
- Co-ordination of biometrics research and planning is further advanced in some other UK government organisation, in particular PITO.
- Co-ordination of external communications relating to biometrics would benefit from improvement. Mixed messages about IND's biometrics plans are being received outside of IND and IND may not be aware of significant external activities ongoing which could influence IND operations. Opportunities to share the benefits of research and to influence external initiatives at an early stage may be lost if action to improve communication co-ordination is not taken soon.

1.3.2 Compliance with the framework

- The framework is presented which puts the current IND biometrics in context and allows the consideration of other areas where biometric technology is not currently being used.
- As many already know within IND, there is no single biometric appropriate for all applications. The choice of most appropriate biometric requires analysis of the requirements and constraints of each individual application.
- There is no mechanical way of determining which biometric is most appropriate for any new application since there are so many variable factors and the technology and external influences are changing apace. We believe that new project evaluation can only be fully achieved by experts who are up to date with both biometric technologies and IND activities and aims.

1.4 Key recommendations

1.4.1 Co-ordination of biometrics within IND

- The IND high-level strategy for biometrics needs to be agreed at senior management level taking into account legislation, policy, operational aims and the technical framework presented in this document.
- IND needs to consider the relevance of all the disparate standards groups to their business and determine in which they need to be involved. Some standards will emerge by themselves, but these should be tracked by IND to determine whether and when they become relevant.
- Agree the IND-wide centre of technology provision from where expertise can be concentrated and shared. IND senior management should agree the role of BISTD as the IND central IT provider. To distribute IT provision will lead to inefficient use of resources and increased costs. The model of central IT Service provision is a sound one and has been seen to work in other organisations such as PITO.
- Establish a central body of expert advice that is available to all IND departments on demand.

1.4.2 Biometric project planning

- Put in place a mandatory project initiation process that ensures that project requirements are evaluated against IND-wide goals and available biometric technology options before being allowed to progress.

In the interim period before new procedures are put in place, all parts of IND as a whole needs to decide how to act on existing plans for biometrics.

- Initiate the next steps as quickly as possible to minimise this 'limbo' period.
- Projects which offer 'quick wins' to the business should be allowed to proceed so long as they can be shown to be of low risk to the business.
- Preparations should be made to capture and feedback experience gained from new projects/trials to the central body once it is established.
- For further new projects arising, ensure that, where possible, consideration is given to the need for data sharing in the future as well as now. Take into account the impact of known likely biometrics initiatives such as biometrics travel documents.
- No new biometrics projects should be initiated without being brought to the attention of the PSG first.

1.4.3 Implementation

It is not possible for a study of this brevity to make detailed implementation recommendations. However, these key recommendations have been identified:

- It is necessary to determine the best match between the individual application requirements and the characteristics of any given implementation. It is expected that each of the three key Biometrics (Finger, Iris and Face) has a role to play in the business of IND.
- Wherever possible in day-to-day operations, *verification* (1:1 matching against a token) should be preferred to *identification* (1:n matching), since this will provide best accuracy and speed of response. In might still be necessary to carry out a 1:n check at the point of enrolment to spot duplicate enrolments.
- Where 1:n matching is used and where appropriate, database sizes should be constrained by any other known factors to minimise the search domain. The means of constraint would be application specific, but the general idea would be to segment the database based on known person attributes, e.g. additional data contained in a machine-readable travel document.
- Technologies should not be used at their limits. Any technology considered for introduction must have an upgrade path.
- Use standards to maximise the possibilities for data sharing and sources of supply where possible and permitted under the Data Protection Act.

1.5 Next steps

This study has been extremely brief and so it has not been possible to address all areas in sufficient depth. Several areas that deserve further consideration have been identified as follows:

- Further detailed assessment of the projects identified within this report to determine key success/failure criteria and summarise lessons learned.

- Further, more detailed evaluation of the framework of Biometric requirements is required to produce a road map for Biometrics within IND. This is similar to work which PITO is about to undertake and perhaps experiences could be shared here.
- Further consideration needs to be given to the implications of biometric data sharing from technical and policy angles and how this feeds into strategy.
- Further consideration needs to be given to the implications of the use or absence of tokens in biometrics systems and this fed into the overall strategy.
- Define exactly the technology initiation process and how it will be made mandatory.
- Consider the 'straw man' Terms of Reference for the central expert body provided in section 4.2.1 and flesh out the exact appropriate powers of the above central expert body and how it can be ensured that it will not be another "talking shop".
- Consider where this body should be established. This might be within IND, in which case it would be appropriate to be housed within BISTD, or perhaps could be Home Office-wide. This is a matter for IND to decide based upon their detailed understanding of government operations.
- Consider whether this body should cover only biometric technologies or all electronic ID technologies such as hardware tokens (smart cards, optical cards, etc), cryptography, PKI, etc.

2 INTRODUCTION

2.1 Background

The Home Office Immigration and Nationality Directorate's (IND) responsibilities include processing applications from foreign nationals to enter the UK and for enforcement of immigration policy. Three important aspects of this role are the processing of increasing number of asylum seekers, the deterrence and detection of rule breakers, and admitting 90 million legitimate travellers annually with as little delay and inconvenience as possible. There are also objectives defined within Aim 6, shared jointly with the Passport Office, which need to be achieved by the IND.

In the past two years projects have been undertaken of an AFIS system for checking fingerprints of Asylum seekers and others for border control purposes – however there is currently no co-ordinated plan for use of biometric technology and management of biometric information.

2.2 Scope and Terms of Reference

This study was conducted in order to establish a governance framework for the co-ordinated planning, development and implementation of biometrics in support of IND's policy objectives. The key tasks to be performed to achieve this goal include:

- identify business areas suitable for biometrics use,
- conduct interviews with key personnel and stakeholders in various departments to identify criteria for use of, and needs for, biometric information,
- assess the fit of three identified biometric technologies (fingerprint, iris and face) against these criteria and needs,
- understand and assess the external environmental factors affecting IND's biometrics approach,
- understand and assess policy implications for use of biometrics and how work should be co-ordinated with other domestic and international bodies,
- present findings to the Project Steering Group and produce report on requirements and proposed framework.

The study is specifically aimed at the use of biometrics to meet IND requirements for identity and verification of persons. Whilst the requirements of bodies outside IND are touched upon, as are more generic identity and verification techniques, such information should be seen as background, provided to establish the context within which this study sits, and not as part of the core deliverable.

2.3 Acknowledgements

Our thanks are due to all who have contributed to the study by giving their time to interviews, answering follow up questions and providing documentation to enable the rapid completion of this study.

2.4 The AMTEC Team

In order to complete the work within a five week period, a consultancy team of three, one consultant dedicated to the project full time, with consultative and review input to the work on a part time basis from two additional consultants.

- **Dr John Elliott - Lead Consultant.** John was responsible for the management and day-to-day project work for this assignment. John has worked for various government and financial services organisations analysing and defining requirements for identity management and security systems.
- **Dr Neil Garner – Consultant/Reviewer** Neil was responsible for review and quality of the deliverables and provided technical advice on biometric systems and input into the development of the biometric framework. Neil has extensive technical knowledge of biometric, authentication and communication systems.
- **Mr William (Bill) Perry – Specialist Consultant.** Bill acted as a specialist consultant, providing background information on work being undertaken by other Home Office departments and specialist biometric technical input. He reviewed critical working documentation.

2.5 References

[UKISBP] *UK Immigration Service Business Plan 2002-2003*

[eBPB] *e-Borders Programme Brief*, Version 1, 27th January 2003

[IGC] Inter-Governmental Consultations on Asylum, Refugee and Immigration Policies in Europe, North America and Australia, *Workshop on Technology*, Geneva, November 2002.

[FSES] Tony Mansfield (NPL) and Mark Rejman-Greene (BTExact), *Feasibility Study on the Use of Biometrics in an Entitlement Scheme*, For UKPS, DVLA and the Home Office, IMSC/H07/D2, Version 3, February 2003.

[BPT] Tony Mansfield (NPL) and ,J.L. Wayman, *Best Practice in Testing and Reporting Performance of Biometric Devices*, NPL Report CMSC 14/02, v2.01, August 2002. http://www.cesg.gov.uk/technology/biometrics/media/Best%20Practice.pdf

2.6 Terms and abbreviations

Term	Definition
AfB	Association for Biometrics

Term	Definition
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
ARC	Application Registration Card
ATC	Authority to Carry
BAA	British Airports Authority
BCMP	Border Control Modernisation Programme (IND)
BISTD	Business IT Sytems and Technology Directorate
BFT	Biometric Facial Template (BCMP)
BSI	British Standards Institution
CBEFF	Common Biometric Exchange File Format
CCRA	Canada Customs and Revenue Agency
CEN	Comité Européen de Normalisation
DfT	Department for Transport
DPA	Data Protection Act
DVLA	Driver and Vehicle Licensing Agency (executive agency of DfT)
ECAC	European Civil Aviation Conference
EDE	EURODAC Data Exchange
e-ID	Electronic Identity
ES	Enrolment Searches
ETA	Electronic Travel Authority
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROPOL	European Police
FBI	Federal Bureau of Investigation (US)
FCO	Foreign and Commonwealth Office
G8	Group of 8. Heads of state or government of the major industrial democracies meet annually to deal with the major economic and political issues facing their domestic societies and the international community as a whole. These countries are currently: France, United States, United Kingdom, Russia, Germany, Japan, Italy and Canada
IAFP	Immigration and Asylum Fingerprint Programme
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
IAFS	Immigration and Asylum Fingerprint System
IC	Identity Confirmation
ICAO	International Civil Aviation Organization
ICD	Integrated Casework Directorate
ID	Identity
IGC	Inter-Governmental Consultations
IMO	International Migration Organisation

Term	Definition
IND	Immigration and Nationality Directorate
IPR	Intellectual Property Rights
IRIS	Iris Recognition Immigration System
ISO	International Organization for Standardization
IT	Information Technology
MRTD	Machine-Readable Travel Documents
NAFIS	National Automatic Fingerprint Identification System
NAIR	National Asylum Intake Reduction (temporary name given to Peter Wales' new project which currently has no name).
NCITS	National Committee for Information Technology Standards (USA)
NASS	National Asylum Support Service
NIST	National Institute of Standards and Technology
NTWG	New Technology Working Group (ICAO)
PIFE	Police/Immigration Fingerprint Exchange
PITO	Police Information Technology Organisation
PKI	Public Key Infrastructure
PSG	Project Steering Group (within IND)
PNC	Police National Computer system
RANS	Restricted Access to NASS Support
SIS	Schengen Information System
UK	United Kingdom
UKIS	UK Immigration Service
UKPS	UK Passport Service
UNHCR	United Nations High Commissioner for Refugees
US	United States (of America)
US	United States of America
VAT	Value Added Tax
WI	Warnings Index
WS	Watch-list Searches

3 WORK CARRIED OUT

3.1 Approach/Methodology

We approached this work by performing a number of tasks in parallel in order to complete the work on time.

- **Stage 1 - Review current position**. Firstly we reviewed IND's current position, through access to documentation and IND staff, as well as team knowledge of existing initiatives in common with the passport office through Bill Perry.
- **Stage 2 – Conduct interviews**. Around 30 interviews were performed with internal and external stakeholders to ensure that needs and requirements were identified throughout IND's entire operation.
- **Stage 3 – Define requirements and produce model.** The result of these interviews were used to define the business needs and requirements presented within this document
- **Stage 4 – Review external influences.** An assessment was made of the external Biometric technology market and international initiatives which may affect the work of IND. This assessment was used to formulate the key constraints on the emergent biometrics framework.
- **Stage 5 – Assess policy implications and develop framework.** A 'straw man' framework for biometric planning, development and implementation was produced.
- **Stage 6 – Present and report.** This document is a draft of the final report that will be presented to the Project Steering Group (PSG)after which we will incorporate feedback into the final deliverable report.

3.2 Current Position on Biometrics within IND

This section provides an overview of IND and current biometrics activities within IND.

3.2.1 IND key activities

The aim of IND is to meet the Home Office's Aim 6 jointly with the UK Passport Service (UKPS). Aim 6 is:

> *To regulate entry to and settlement in the UK effectively in the interests of sustainable growth and social inclusion.*
> *To provide an efficient and effective work permit system to meet economic skill requirements and fair, fast and effective programmes for dealing with visitors, citizenship and long-term immigration applications and those seeking refuge and asylum.*
> *To facilitate travel by UK citizens.*

More specifically, IND and the Lord Chancellor's Department are drafting an Asylum and Immigration Joint Delivery Plan that sets out the Government's asylum and immigration plans for the next three years. The current position can be summarised as follows:

- Asylum intake is high

- Backlog of undecided asylum cases and appeals
- Asylum support costs are high
- Removals are well short of target
- Rising volumes of applications in all areas (work permits, nationality and after entry)
- Long waiting times for nationality and after entry
- Insufficient resources

The Joint Delivery Plan vision for three years' time can be summarised as follows:

- Border controls outside the UK using advance passenger information processing
- Reduced level of unfounded asylum applications
- Capacity to produce prompt decisions
- Increased proportion of failed asylum seekers removed
- Low asylum support costs
- Capacity to process rising volumes of applications business
- Very fast turn-around for routine applications
- Control immigration while inconveniencing as little as possible those entitled or qualified to enter

Actions within the Joint Delivery action plan that are significant to this study include:

- Tighten border control
- Develop e-Borders
- Re-engineering to reduce end-to-end time in the asylum system
- Work with other countries to improve documentation and open up removals routes
- Manage asylum support more tightly
- Cease payments promptly for those no longer entitled to them
- Create more joint operations schemes
- Expand intelligence capabilities
- Strengthen programme and project management skills
- Improve communication
- Reduce delays to *bona fide* passengers

3.2.1.1 Home Office organisation

IND sits within the Home Office and is a large and complex organisation. Therefore, we have been guided by IND to the relevant parts of the organisation from which to gather input to this study. The figure below presents a simplified organisational chart that includes only those parts of IND with which we have come into contact during this study and where they sit within the Home Office.

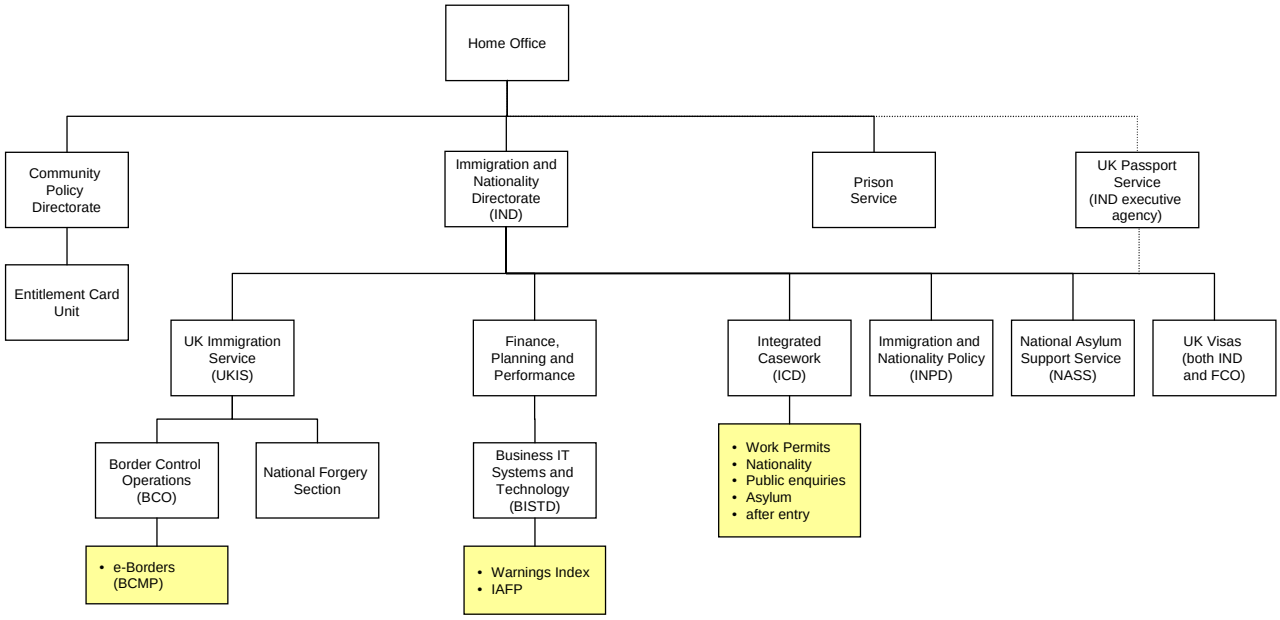


Figure 1: Simplified Home Office Overview

The interviews that were conducted during the requirements gathering phase of this study are listed in Annex A.

3.2.2 IND functions

For the purposes of this study, we have broken down IND activities as follows:

- Policy
- Controlling admissions
- Asylum, After-Entry Casework and Nationality
- Asylum support
- Enforcement

Each of these areas is described briefly below.

3.2.2.1 Policy

Policy provides the narrative that makes sense of events and INDs operational response to them. Issues of particular concern to IND are:

- International policy making and harmonisation, working with the EU, the G8 and the UN amongst others.
- Pushing forward measures to tackle illegal immigration and people trafficking
- Preventing 'asylum shopping' where claimants move around Europe looking for 'the best deal'.
- Legal changes such as various relevant Acts introduced including the Immigration and Asylum Act 1999, the Human Rights Act 2000 and Race Relations (Amendment) Act 2000.

3.2.2.2 Controlling admissions

IND works with the Foreign and Commonwealth Office (FCO) and UKvisas, clearing people abroad to enter the UK. IND also operates the immigration control at UK ports. UKvisas is a joint IND and FCO department, staffed by both IND and FCO.

3.2.2.3 Asylum, After-Entry Casework and Nationality

IND's Integrated Casework Directorate (ICD) decides how to respond to applications from asylum seekers and other overseas nationals who want to remain in the UK. This includes applications within the UK from those who wish to extend their stay or change its basis.

IND's ICD (North) in Liverpool makes decisions on applications for British citizenship from those who have the right to stay permanently.

3.2.2.4 Asylum support

While asylum claims are being considered, IND's National Asylum Support Service (NASS) supports destitute asylum seekers. They also help to integrate those who are accepted as refugees.

3.2.2.5 Enforcement

IND enforces the immigration laws. They remove those who have no right to be here. They pursue those who profit from breaking the rules.

3.2.3 IND biometrics projects to date

There have been a number of biometrics projects within IND to date. The majority have been proof-of-concept trials. The one exception is the programme known as Immigration and Asylum Fingerprint Programme (IAFP) that now resides within BISTD. This programme contains a number of biometrics sub-projects:

- ***IAFS:*** The fingerprint system itself which allows matching against the database of past asylum seekers. (delivered in 2000)
- ***ARC:*** Application Registration Card. A smart card currently used for asylum seekers but which could be used to track any kind of applicants. The card stores two fingerprints allowing spot checks to made
- ***PIFE:*** Police/Immigration Fingerprint Exchange. Currently, cross-checking with the national Police fingerprint database, NAFIS, is a manual process. This project will automate this process from September 2003. The aim is to provide real-time cross-checking.
- ***EDE:*** EURODAC Data Exchange. EURODAC is the European Union asylum seeker fingerprint database. The Dublin Convention states that asylum seekers must apply for asylum in first EU state in which they arrive. EURODAC went live in January 2003 and is being used to speed their return to that EU state.

Another activity involving biometrics within IND is the e-Borders Programme that resides within UKIS. This is a programme bringing together a number of different projects aimed at establishing a modernised, intelligence-led immigration control framework, based on the electronic processing of information relating to passengers on declared routes to the UK and providing expedited entry for certain categories of passengers using biometric technology.

The core project incorporates a number of other projects as defined in [eBPB] including:

- ***IRIS:*** Iris Recognition Immigration System. An expedited clearance scheme for selected categories of passenger, typically those with existing rights of entry, or frequent visitors. Upon enrolment in the scheme passengers will be

screened for suitability for automated clearance, and their irises will be scanned and stored. A scheme member will then be free to enter the UK as often as desired via automatic iris-controlled gates at arrival ports, without any contact with immigration officers. Note that iris recognition is the currently favoured biometric, but other biometrics may be supported if required (e.g. a biometric in a UK passport).

- ***BFT:*** The Biometric Facial Template (project Verlaine) is a research project into applications for facial recognition techniques, aimed at ensuring that the person who was granted certain approvals or privileges at an early stage in the travel process is the same person who seeks to use those privileges at a later stage. For example, it could check that a passenger presenting a boarding card at a boarding gate is the person to whom the card was issued.

A list of biometrics projects discussed during interviews both within IND and with relevant external partners is presented in Annex B.

3.3 Overview of Biometrics Technologies

3.3.1 Introduction

Biometric identification can be defined as the "*automated identification, or verification of human identity through measurable, repeatable physiological and behavioural characteristics*".

Example biometrics are: face, fingerprints, hand and finger geometry, handwriting, iris, retina, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming more and more apparent.

There are two different ways to authenticate a person:

1. Verification (*Am I whom I claim I am?*) involves confirming or denying a person's *claimed identity*.
2. Identification (*Who am I?*) involves searching for an identity. This might be a positive case of identification, or a negative case of spotting duplicate enrolments.

IND requested that this study focus on three biometric types, namely facial recognition, iris recognition and fingerprint recognition. There are a number of reasons behind this decision, including interoperability between UK government organisations and international interoperability at immigration facilities. However, it should be noted that many airports and travel operators have trialed, piloted and implemented other solutions, especially using hand geometry. Examples of live installations are: airside security doors, staff entrances/exits and frequent traveller fast-track stations.

Even within the three biometric types selected by IND, there is much variation in acquisition systems and algorithms in the supplied systems. There is also a wide performance gap between the best and worst systems.

IND's core business is to regulate and control border activity and, as such, this is where the focus of biometric choice should be. There are numerous biometric systems (other than the three nominated technologies) that, individually, or in combination, could provide adequate accuracy and functionality within specific IND projects. However, our aim in this study is to encourage the building of a biometric strategy that encompasses all aspects of IND business and relative interaction and interoperability. To achieve this it is pertinent that IND restricts the choice of biometrics available for IND use. Interoperability and data exchange between other UK Government departments is also extremely important, especially areas such as PITO, UKPS and FCO. All these departments have also, to a greater or lesser degree, restricted the overarching use of biometric techniques.

However, it should be noted that each application/business requirement is unique and there may be the need to utilise a biometric technique other than the three recommended. This choice should be strictly controlled from a centralised function to ensure that a common approach is adopted wherever practical. Data sharing requirements are key to IND's business.

ICAO (International Civil Aviation Organisation) recently undertook a large and wide-ranging evaluation and scoping study into the use of biometrics in travel documents, the culmination of which is a "Technical Report on Biometrics". In this study common biometric types (around seven biometrics) were analysed and measured in numerous ways including operational impact (in areas such as enrolment and verification), compatibility with existing MRTDs (Machine Readable Travel Documents), redundancy, global public perception, storage requirements and performance. The study concluded that the top three contenders (in no particular order) were face image recognition, eye pattern recognition and fingerprint recognition.

Furthermore, in an ICAO meeting held in New Orleans during March 2003 it was recommended that on future MRTD face image recognition be used as the primary biometric supported by iris recognition and/or fingerprint recognition. The following is a copy of the resolution passed at the March conference:

"New Orleans Resolution

In order to clarify NTWG resolution N001/02 (commonly referred to as the "Berlin Resolution"), and taking into account recent developments in data storage technologies, the NTWG hereby resolves:

ICAO TAG-MRTD/NTWG recognises that Member States currently and will continue to utilise the facial image as the primary identifier for MRTDs and as such endorses the use of standardised digitally stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.

ICAO TAG-MRTD/NTWG further recognises that in addition to the use of a digitally stored facial image, Member States can use standardised digitally stored fingerprint and/or iris images as additional globally interoperable biometrics in support of machine assisted verification and/or identification.*

Member States, in their initial deployment of MRTDs with biometric identifiers, are encouraged to adopt contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers.

**subject to the resolution of intellectual property issues."*

3.3.2 General Considerations when implementing biometrics systems

3.3.2.1 No panacea

Biometrics are not a panacea. No biometric system can ever be 100% accurate and each new project needs to remain aware of this when considering the use of biometrics and how their security will integrate with the security of any other systems to which they need to interface.

3.3.2.2 User perception

User attitudes to biometric technology can be a key influence on the choice of biometric deployed. Some biometric systems can seem to be intrusive and thus alienate the very people who would benefit from it. This is particularly pertinent when attempting to implement an optional system that has joint benefits both to the User and Operator/Implementer.

3.3.2.3 Acceptance

The choice of a biometric should take account of the enrolee population acceptance of the enrolment procedure. Acceptance rate might be lowered due to the following:

- The fear from intrusive acquiring devices that might annoy or injure enrollees.
- Devices that require physical contacts could raise hygiene concerns
- Some religious or cultural peculiarities.
- Privacy concerns according to uses broader than intended purposes like law enforcement or surveillance.

All biometrics will face some acceptance problems to a certain degree.

3.3.2.4 Suitability

Some of the general population do not have the body part (or sufficient quality of the body part) required for measuring any one biometric except face.

A fallback system should always be considered for people who cannot enrol through the system's biometric. This fallback system could be the current procedure or another biometric identifier.

Only facial recognition might be applied to all individuals and could serve as a general enrolment fallback biometric. However, it will not serve all applications' requirements due to its generally low accuracy.

3.3.2.5 Uniqueness

The purpose of biometrics is to uniquely identify individuals. Where large databases are to be used (e.g. millions) one needs to use a biometric identifier that has proved to be unique inside large populations.

3.3.2.6 Stability

The biometric should be stable (constant) during the period of its usage by the system. Unstable biometric traits will lead to increasing false non-match rates over time.

Some face recognition techniques are exposed to instability, in particular because of some people's voluntary change of appearance, the effects of ageing, and differences in illumination between environments.

3.3.2.7 Robustness to spoofing

Secure systems need to defend against counterfeit input data. Electronic attacks are a growing phenomenon and have gained much attention since the Internet growth. Some specific cryptographic techniques can be carefully applied to avoid such a risk. Generally, no one biometric is more exposed than another to electronic attacks.

The use of spoof biometrics such as holding up a large photograph of the face to the camera, or using latex fingerprint pad copies is sometimes dealt with through counter-measures predominantly in the scanning devices and associated software systems which are designed to detect the 'liveness' of the presented biometric. Often a human supervisor at enrolments or recognition attempts will be the main means to prevent such spoof attempts.

3.3.2.8 Enrolment

Acquisition conditions (scanning device, temperature, humidity, light, enrolee attitude, age, etc.) are crucial for the quality of the templates and then the accuracy of the system, in particular for improving the false non-match rate.

Biometric identifiers sensitivity to acquisition conditions should be assessed in the context of the system (e.g. cross- border checkpoints).

As some biometrics require complex acquisition procedures, supervision will be needed, especially in an AFIS type environment where ten rolled prints are collected. Operational impacts of supervision have to be considered:

a) The acquisition **time,** in particular when several attempts are necessary to get an acceptable sample, will directly translate into personnel costs and additional investments to cope with queues.
b) The level of required **technical expertise** from the personnel should be reasonable in order not to increase training costs too much.

3.3.2.9 Failure-to-enrol rate

In order to improve the quality of the biometric database some systems perform a quality check during the acquisition procedure and possibly reject people with poor biometrics. This results in improved accuracy on the one hand but also results in a fraction of the population not being able to enrol with the system (e.g. if their fingerprints are worn down through manual labour and cannot be captured, or if they have a disease resulting in their having no iris). Accordingly the accuracy of a system should be considered jointly with its failure-to-enrol rate.

It should be noted that the failure-to-enrol rate will not have the same importance in a voluntary system where accuracy might be the main driver.

3.3.2.10 Using Biometrics in conjunction with secure tokens

As described previously in section 3.3.1, biometrics can be used to authenticate a person using either identification (1:n matching) or verification (1:1 matching) techniques.

Identifying which of these two authentication modes is most applicable for meeting a particular requirement is not as straightforward as it may first appear. Some applications are truly about ‘identification’, e.g. covert monitoring of crowds. However, for many requirements, whether an individual is authenticated based on a 1:n search against a database, or a 1:1 verification against a token is purely an implementation decision. Many requirements that are initially assumed to be met using the ‘identification’ mode can, in fact be turned into ‘verification’ applications through the use a secure token.

For the purposes of this study we define a secure token as a token carried by someone for claiming an identity or privileges. This will be built from tamper-resistant hardware and is likely to be in the form of a smart card or a travel document containing a contactless smart card chip.

Each application requirement needs to be individually assessed in order to decide on the best implementation to meet it, however there are a number of generic advantages gained from using biometrics in conjunction with tokens:

- A greater number of biometrics can be feasibly considered – biometrics unsuitable for ‘identification’ can be considered for an application by performing ‘verification’ against a secure token.
- A 1:n (identification) system that is well received may find itself with a rapidly growing user base and a subsequently unacceptable drop in performance, damaging the good reputation built by the early success. Using secure tokens for ‘verification’ helps to mitigate this risk.

A number of factors need to be considered before deciding if token based (1:1) or database (1:n) type search is most appropriate for meeting the authentication requirements of a particular application. For instance:

- What are the performance criteria? (the lower the acceptable failure rate, the faster the process, the more likely it is that 1:1 matching is more appropriate)
- Is the system on or offline? (verification against a biometric stored on the token may be more suitable for offline applications such as door access)
- Are staff already familiar with carrying tokens for physical / logical access?
- Token cost vs database / network bandwidth cost.
- Closed or open user group? (1:n more suitable for a static sized user base, otherwise risk performance degradation as user base grows.)
- Data storage needs – what additional data need to be used by the application and is it more appropriate to store them in a back-end database than on a token that may be lost?
- Data update needs – how frequently do the data used for the application change and what are the practicalities of updating those data on distributed tokens as opposed to maintaining the data centrally?
- Cost of secure transport and storage of cards plus audit and management.

It should be noted that there is potential for the use of tokens to make a system less secure. For example, a criminal has all the time in the world to attack the token in private. Therefore system security must take this into account and ensure that appropriate risk analyses are performed and countermeasures put in place such as the use of cryptographic mutual authentication between the token and the reader, encryption of data and tamper-resistant hardware.

3.3.3 Detail on the three technologies

3.3.3.1 Face Image Recognition (Facial recognition)

Facial recognition is the most familiar biometric; we identify people every day of our lives by their faces. Immigration officers currently utilise this feature for face-to-face verification of travel documents.

Facial recognition does not usually require complex co-operation on the part of the subject in order to perform identification and verification tasks. They simply walk up to a system that uses a video camera — such cameras vary from standard camcorders, to special purpose cameras.

There are general problems when using this technology in that systems are sensitive to lighting conditions, facial expression, etc. This technology cannot, at present, be used in the identification mode where extremely large databases are concerned (i.e. it is not accurate enough for large databases with millions of records).

For 1:n checks, facial recognition systems often return a range of possible matches which then require human intervention in order to select the ‘best’ match.

There are current standards for collecting ‘mugshots’ and standards for facial image exchange are in development.

3.3.3.2 Iris Recognition

Iris recognition is theoretically proven, user-safe and operationally reliable. However there are few large-scale implementations in the world today and none known with more than a 150,000 records. The iris pattern, once stable, does not change with age, and rarely suffers damage.

Iris recongition generally uses standard video cameras — the same kind used in video camcorders — to take a picture of the iris of your eye. It does not require physical contact but current systems typically require the user to move forward into the camera’s narrow field of vision. Most systems work from a distance of around 30 – 60 cm.

One drawback of this technology is that the use of iris images as a biometric has been patented by a single company (Iridian) who rigorously defend their patents and prosecute all offenders. Standards bodies should not recommend proprietary technologies and therefore ICAO may well decide not to recommend iris scanning as a biometric for travel documents unless detail of the technology enters the public domain. The concept patent expires Feb 2005 (US), 2006 (elsewhere).

There are several suppliers of iris recognition technology. The best performing all use Iridian algorithms (in addition to some of their own) – but there are others marketed in countries not covered by Iridians concept patent. Iridian is cooperating all the other suppliers of the technology on an iris image interchange format so that there might be wider interoperability.

3.3.3.3 Fingerprint Recognition

Among all the biometric techniques, fingerprint-based identification is the longest standing and has been successfully used in many applications. Evidence over many years suggests that every person has unique, immutable fingerprints.

A fingerprint is made of a series of ridges and furrows (patterns) on the surface of the finger including basic patterns (whorls, arches etc.) and complex patterns (edges, line endings, islands etc.). The uniqueness of a fingerprint is determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprints are known to change over time, they may become thinner and less well defined.

Fingerprint systems often return a range of likely matches in 1:n mode and then a human expert is required to decide which it the ‘best’ match.

Traditional criminal and justice Automated Fingerprint Identification Systems (AFIS) use rolled prints of all ten fingers and have been used for some time. This is because rolled prints help when matching with partial prints collected from a crime scene. This legacy constraint can cause difficulties since it means that enrolment needs to be supervised and that the person being enrolled has to be “man-handled” by a supervisor.

Other fingerprint biometric systems might use only flat prints and might only record one or two fingerprints. Thus, with fingerprint systems it is vital to know exactly which kind of system is implemented before sensible comparisons can be made.

AFIS is the only biometric used today in identification-based applications where database sizes exceed one million records. Indeed the UK Police NAFIS system and the FBI IAFIS system far exceed these figures whilst maintaining an excellent degree of accuracy.

3.3.4 Examining the options for IND

In order to understand the three primary biometrics chosen it is necessary that we examine areas such as history, techniques, key features and usability. This study is not intended to be an exhaustive and fully documented account of these entities, however, an overview is provided in the table below.

	Fingerprint	**Iris**	**Facial**
History	1. > 100 years old 2. Used in international Criminal Justice Systems for > 10 years 3. Founded on manual ink print collection techniques.	1. < 20 years old 2. Until recently only used in physical access control, now in other application areas. 3. Founded on concept patent – expires Feb 2005.	1. Used as primary means of human identification for as long as mankind has walked the earth. 2. Electronic usage < 20 years old 3. Primarily aimed at CCTV, surveillance and access control.
Suppliers	1. < 10 AFIS suppliers 2. 100+ verification suppliers 3. 1000s of systems installed worldwide (largest FBI 40M+ users)	1. Founded on concept patent owned by Iridian – expires Feb 2005. 2. Currently 4 suppliers using Iridian licences (though many more have partnership licenses); 5 using other algorithms. 3. Relatively few installations (largest approx 100,000 users)	1. 4+ major suppliers
Techniques	1. Pattern matching 2. Minutiae 3. 1 & 2 Combined	Commercial systems use 3 different techniques. 1. Daugman, 2. Lim et al, 3. Noh et al	1. Eigen faces -MIT 2. Vector analysis 3. Base model analysis

	Fingerprint	**Iris**	**Facial**
Operator assistance required	1. AFIS – Yes owing to the need to acquire rolled prints. 2. Others – No, however some people do have difficulty in using the technology	No, however some people do find difficulty using this technology.	Sometimes required to correctly locate landmark points on the face.
Usability for subject	Easy for both frequent and infrequent users.	Easy for both frequent and infrequent users.	Easy for both frequent and infrequent users .
Usability for operator	Low-level training required	Low-level training required	Highly dependant upon the application. One-to-one is easy to use, spotting a face in a crowd is difficult
Information used to establish 'uniqueness' of an individual	Ten fingers, with approx 30-50 minutiae points per finger. The ring and small fingers provide less information content, and there is some correlation between data from separate fingers.	Two eyes, with over 240 binary degrees of freedom in each 512-byte template. There is no evidence of correlation between a person's two iris patterns.	Two-dimensional characteristics of the face. Features such as eyes, nose, mouth and ears provide much of the vital information.
Maturity of the technology	Extensive experience in its application to criminal AFIS systems. UK NAFIS and FBI databases have multi-million records each. Over 20 years of development.	Over 15 years of development of the method, almost exclusively by the one supplier. Several small scale deployments. Large-scale starting to appear: e.g. UNHCR, Canada CCRA.	Over 10 years of development with most of the products building on university research.
Hardware	Many optical and electronic sensors available. Large area platen sensors for 'slap' fingerprint capture of all fingers. Portable fingerprint units for remote data capture.	Specialised cameras. Portable units for remote data capture Improved user interfaces under development. The camera system can often capture a face image at the same time	Range from standard cameras, to more sophisticated cameras which track face images, or capture 3D information
Maturity of '1-to-1' verification	Hundreds of deployments.	A small number of deployments; handheld systems still under development	Numerous deployments.

	Fingerprint	Iris	Facial
Performance in '1-to-1' verification	Very good	Very good	Fair-Good
IPR considerations	Suppliers have proprietary algorithms and matching hardware.	Concept patent owned by Iridian. Suppliers have proprietary algorithms.	Suppliers have proprietary algorithms.
Privacy implications.	Concerns about access and cross-matching with criminal justice systems. Data are considered personal under the Data Protection Act (and so must be used for a specific purpose only and stored securely).	Data are considered personal under DPA.	Data are considered personal under DPA.
Social concerns	Some cultures have hygiene concerns associated with touching sensors used by others.	Health and safety fears over putting eye close to camera.	Religious headgear can conceal face

A summary table of the pros and cons of the three technologies is given in section 3.7.2.

3.4 External Influences on Biometrics in IND

The figure below shows IND in the context of the organisations with which it currently shares, or is likely to share, information relating to biometrics. These are briefly described in turn in this section.

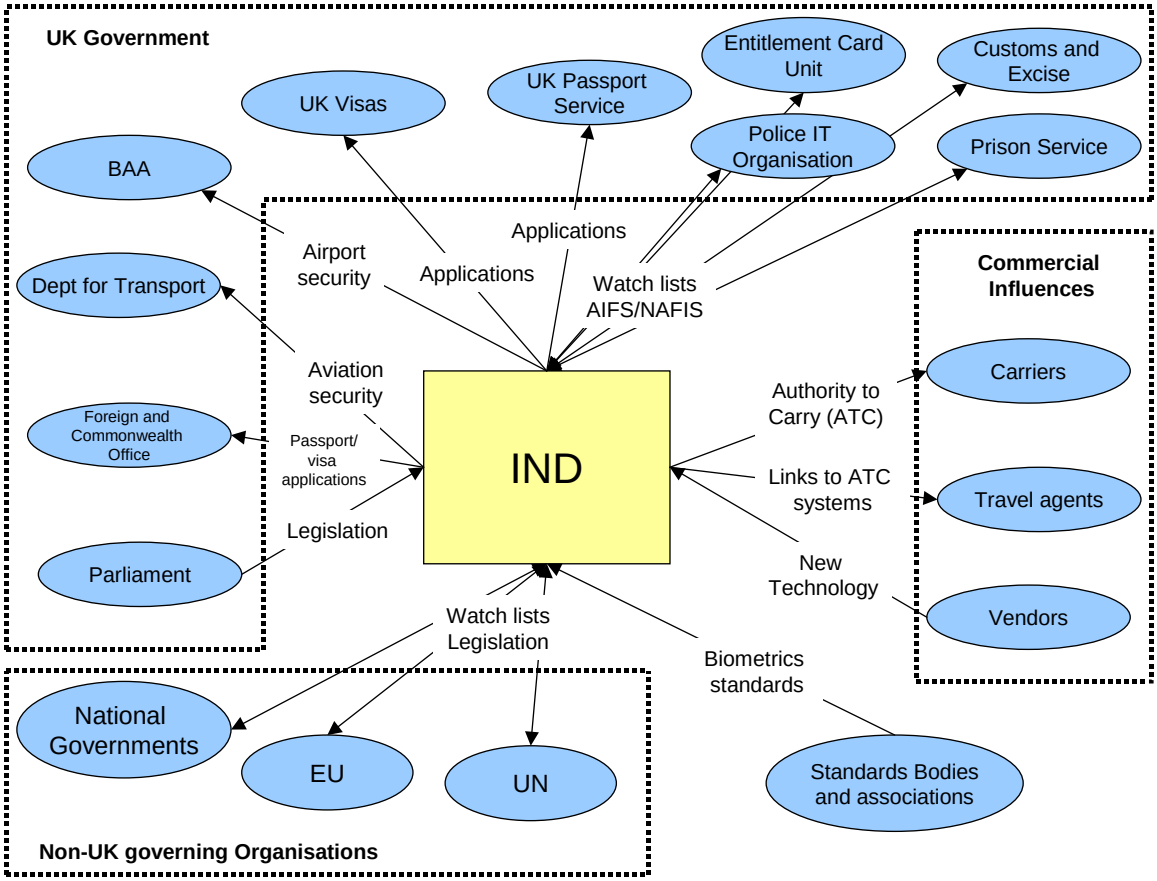


Figure 2: IND Biometric external influences

3.4.1 UK government organisations

Within UK government there are various organisation outside of IND with which IND might benefit from sharing information relating to biometrics.

3.4.1.1 Foreign and Commonwealth Office

The Foreign and Commonwealth Office's purpose is:

> *To work for the United Kingdom's interests in a safe, just and prosperous world*

During this study we have interviewed FCO staff involved with UKvisas and passports. UKvisas was established in June 2000 jointly by the Foreign and Commonwealth Office and the Home Office to manage the UK's entry clearance (visa) operation.

Also applications for UK passports from abroad are dealt with by the FCO. Their views can be summarised as follows:

- Biometrics in passports will be consistent with ICAO policy and standards
- Biometrics must be implementable overseas in operations ranging widely in scale in circa 140 overseas missions (cost and complexity of technology which may not work in less than ideal conditions)
- Any decisions on biometrics should not preclude applications by mail because passport operations are centralised for security and efficiency.

'Applications in person only' would hit those e.g. on US West Coast (passports issued in Washington), in Perth (passports issued in Canberra).

3.4.1.2 Department for Transport

The Department for Transport (DfT) has a legal responsibility for physical and procedural access control at airports. There exist legal directives on over 150 sites made up of 53 airports and approximately 100 other recently inherited green-field sites from which flights might be made.

ECAC, the European Civil Aviation Conference will mandate the access control requirements eventually, but it is not clear when. They will defer to EU legislation. Currently, the DfT seems to be leading on airport access control in the EU and so it is likely that ECAC will adopt whatever the UK implements.

DfT is initiating an Access Control project and, as the first stage, is drawing up a single requirements specification for all their sites to comply with. Initially this will be for DfT staff only but could then roll out to passengers for baggage control over 3-5 years.

The vision is that biometrics are used to identify travellers on arrival at the airport. Check in would be no longer required. Baggage will be linked to their owners and dropped down a shoot. Eventually the redundant check-in desks will become valuable shopping real estate.

DVLA is an executive agency of DfT and is significant because they issue driving licenses that are likely to contain biometrics in the future and could be part of the Entitlement Card scheme if it goes ahead.

3.4.1.3 British Airports Authority

The British Airports Authority (BAA) is responsible for buildings security in airports. By contrast, the airlines are responsible for airplane security. BAA is looking to effectively increase capacity in terminal buildings by minimising queues at flight boarding when leaving and immigration control on arrival. Expedited passage in effect saves space. Also, passengers are happier if they clear border control faster: “passenger delight” is one of their aims.

If ticket-less travel is introduced, BAA would be responsible for implementing it.

3.4.1.4 UK visas

Visa (or entry clearance) applications are processed by entry clearance officers in UK embassies, high commissions and consulates abroad, collectively known as UK Missions. UKvisas works closely with other parts of IND responsible for immigration policy and who also deals with applications by people already in the UK to extend their stay or to change their immigration status.

UKvisas is a joint Home Office and FCO Department. It reports to a joint management board of senior Foreign and Commonwealth Office and Home Office officers and to Ministers in both departments.

3.4.1.5 Entitlement Card Unit

The Home Secretary wants all lawful residents to have a card to meet the Home Office agenda of fighting ID fraud and illegal working. This will:

1. Help control illegal immigration/work permits (reduce attractiveness of UK to undesirables)
2. Reduce general ID fraud (e.g. bank accounts, passports, driver's licences)
3. Simplify access to government services through single unique ID

A survey [FSES] by NPL and BTExact, commissioned by the Entitlement Scheme, concluded that for 1:n matching there are currently only two biometrics technologies that could be used (fingerprint or iris).

If the scheme goes ahead, all UK residents will have a card and there will be three Entitlement Card types:

1. Passport
2. Driving License
3. Other (for those with neither of the above)

3.4.1.6 UK Passport Service

The United Kingdom Passport Service is an executive agency of the Home Office that issues UK passports to British Nationals living in the UK. Applications from abroad are dealt with by the Foreign and Commonwealth Office.

The UKPS operates seven issuance offices nationwide. Each office can issue passports via post or by the applicant attending the office directly.

The format of passport documents is determined by EU directives, which in turn are largely derived from ICAO recommendations. A good example of this is the machine-readable format that allows the biographical data contained within a passport to be "swiped" using a suitable reader. Note that "bio data" is shorthand for biographical data such as the document holder's name and does not include biometric data.

The UK has a visa waiver agreement with the US which means that UK passport holders do not need to apply for a visa to visit the US. However, the US has been tightening security since 9/11 and has announced that from October 2004 all such visa waiver agreements will only be valid if the participating country's passports contain biometrics or there is a programme in place to introduce them.

It is not clear what will happen in this regard since it is generally agreed that this deadline will be hard to meet and, in any case, the majority of existing UK passports without biometrics are valid for 10 years. UKPS is expecting to start issuing passport books with biometrics in 2005 and passport cards would follow after that.

Biometric collection is likely to be an issue since they currently accept many passport applications by post. FCO (the other UK passport issuer) has also raised this point and have said that it is more extreme in some of the countries that they operate. It is possible that UKPS might move towards the Continental

model where the registry offices are used for registering important events (marriage, death, births) and this could include passport applications.

UKPS is heavily involved with the Entitlement Card consultation since it is proposed that a passport card is one of the three Entitlement card types. UKPS is proud of their issuance infrastructure (checking whether applications should be allowed and preventing duplicate passports for one person) and will be seeking to keep this at the forefront of secure processes by using biometrics where appropriate, whether or not the Entitlement Card scheme goes ahead. They advised DVLA on the setting up of their Card issuance process.

3.4.1.7 Police IT Organisation

PITO aims to support the UK police and other criminal justice organisations in reducing crime and in administering justice more effectively by providing information and communication technology solutions, either directly or through contracts with suppliers.

The UK is unusual when compared to most other EU governments in that Police and Immigration functions are carried out by separate organisations (Police and UKIS within the Home Office). Whilst the Home Secretary oversees the Police Forces, they each have a high degree of autonomy.

PITO systems of particular interest to this study are:

- ***PNC:*** The Police National Computer system that has been running for many years now and is typically used to support person and vehicle spot checks.
- ***NAFIS:*** The National Automatic Fingerprint Identification System is the Police criminal fingerprint database that holds fingerprint biometrics and other information. It is estimated that 10% of the UK adult population have records on this database.
- ***IDENT1:*** This is the next generation system after NAFIS that will be launched in September 2003. The high level aim is to collect facial and iris biometrics. An example use might be to deliver a photo of a suspect to a policeman on the beat with a portable fingerprinting device.

PITO is actively involved in looking at biometrics and has a dedicated unit internal to PITO. They are conducting trials and initiating research into key biometrics areas.

3.4.1.8 Prison Service

The Prison Service is part of the Home Office. Each prison is run by its own Governor in a largely autonomous way. Some prisons have independently implemented biometric systems based on hand geometry or fingerprint. It has been suggested that prisons would benefit from a co-ordinated approach to biometrics to help with roll-call functions and prisoner location within the prison buildings.

3.4.1.9 Customs and Excise

UK Customs & Excise is a Government department with responsibility for collecting billions of pounds in revenue each year in VAT, other taxes and customs duties. They also have a front-line role in preventing illegal imports of drugs, alcohol and tobacco smuggling and tax fraud. They use Police systems for prosecution work, including NAFIS.

It has been mentioned that Customs would like to use biometrics (perhaps facial recognition) to spot who comes in and out of ports and intercept targets.

3.4.1.10 Parliament

A number of government policy decisions outside of IND impact on the use of biometrics within IND. For example, regulations relating to areas such as:

- Human Rights
- Race Relations
- Privacy and Data Protection

There are many government decisions that may constrain the usage of biometric technology by IND. IND policy (see section 3.2.2.1) is responsible for assessing IND functions within the context of external legislation and advising IND on any such constraints on proposed applications.

3.4.2 Non-UK Governing Organisations

In 1999 Finland launched a national electronic ID card combining Schengen travel document functionality and digital signature. Since then the vast majority of European countries and New Associate States are in the process of implementing or planning extensive national roll-outs of some form of electronic ID and signature card with a bundle of specific functions designed to simplify life for citizens in the information society and help accelerate provision of cost-effective e-Government services.

The UK is well connected with major international governments and has been co-operating for some years on the subject of immigration control, both through international assemblies such as the EU, and through more direct inter-governmental co-operation.

3.4.2.1 European Union

The European Commission is harmonising co-operation, border control and expanding the field of exchange of information [IGC].

There are EU directives in several areas that influence IND operations including:

- Travel document and ID card standards
- EU Residents permit

Data are currently being exchanged with the following databases:

- EURODAC database for asylum seeker tracking in EU countries.
- SIS: Schengen Information System
- EUROPOL: European Policing.

In addition, the EU is in the process of forming a Biometric co-ordination group that will be represented at the national level. The official linkage will be via the Home Office but in reality IND may be best placed to provide the co-ordination function from the UK perspective. Other departments interested in this group would include UKPS and FCO.

3.4.2.2 United Nations

The UNHCR and the responsibility it takes for refugees worldwide, is likely to have international influence of the use of biometrics for the management of this people group.

3.4.2.3 National governments

As well as working through governmental organisations such as G8, the EU and the UN, the UK government also co-operates directly with other national governments. For example the “Four Countries Group” (US, Canada, Australia, UK) is working closely together on the concept of Advanced Passenger Processing and some standards have been agreed in this area.

Discussions of a similar nature are also underway with like-minded European Governments such as Germany and Holland. This proactive approach means the UK is likely to be among those leading the EU in decisions about biometric standardisation.

It should not be forgotten that national governments that are not co-operative with the UK are also an external influence on the management and application of biometrics for immigration functions. For instance, any practical measure that goes towards proving the true origin of an individual is going to assist the removal process to countries that are reluctant to take back residents without significant proof of citizenship.

3.4.3 Commercial influences

3.4.3.1 Carriers

Carriers bringing passengers to the UK are responsible for ensuring that they each have valid travel documents. The carrier is fined £2,000 for each passenger they bring who is found to not have valid travel documents for entry into the UK.

3.4.3.2 Travel agents

One means by which Carriers can seek to ensure that they only carry legitimate passengers is via the travel agents who sell places on their flights. Many of these travel agents already have direct access to the carrier booking systems and, as such, provide the first point of contact between the carrier and the passenger. By enabling the collection of data from machine readable travel documents, which will, in time include biometric, as well as biographical information, the process of assessing the validity of a passenger, and providing the carrier with the associated authority to carry that passenger could begin at the earliest opportunity.

There is currently no proposal for travel agents to have biometric readers.

3.4.3.3 Vendors

Commercial Vendors of biometric technologies are always looking to develop and present their unique selling point within the market. Because such activities drive innovation and performance upwards, this will influence the viability of the usage of biometrics for the various IND identification and identity verification requirements.

3.4.4 Biometrics standards

There are numerous standards activities currently being progressed around the world. These include work being performed by NIST (National Institute of Standards and Technology – USA), ICAO (International Civil Aviation Organisations), ISO (International Standards Organisation), CEN (Comité Européen de Normalisation) and numerous others. The good news is that most, especially the larger organisations, are co-ordinating their approach and work items. The gateway or controlling organisation is ISO, which again is the correct decision.

At a local and regional level there are a number of organisations actively pushing and leading the standards activities whilst co-ordinating their work again at an international level (through ISO). These include BSI (British Standards Institution), which shadows ISO, AfB (Association for Biometrics) representing 50+ member companies, numerous commercial organisations and numerous UK government departments (e.g. PITO, UKPS, Home Office).

There are a number of standards relevant to biometric security. These include ISO 17799 and ANSI X9.84 [FSES]. CEN and ETSI (European Telecommunications Standards Institute) currently have a Joint Group on Network and Information Security standardization, which is preparing an overview of standardization requirements in the whole security area, including biometrics. The draft report of this Group (which is open to any interested party) is likely to be made public within a month or so for comment and discussion at an Open Meeting scheduled at present for 13 June in Brussels. The draft report addresses biometric standardization issues and includes a list of current standards initiatives in this field. The group started its activity on 4 July 2002 under the Chairmanship of John Phillips (Nortel Networks and ETSI Board member). Secretariat support is provided by ETSI.

The main thrust of standards activities is now through ISO. The ISO initiatives are based upon a large amount of work that took place within the biometric industry over the last five years, primarily in two areas: BioAPI (Biometric Application Programming Interface) and CBEFF (Common Biometric Exchange File Format).

In early 2002 NCITS (National Committee for Information Technology Standards - USA) under the auspices of the Patriot Act and Homeland Security Bill brought these two initiatives together under a new technical group called M1. This was the real beginning of the international standards process and the feeder organisation to a great deal of work currently being conducted under the ISO banner. The UK developed Best Practices in Testing and Reporting Performance of Biometric Devices [BPT] and the Biometric Evaluation Methodology supplement to the Common Criteria is also being progressed to ISO standards.

The activities of ISO SC37 are summarised in Annex C.

IND is already represented, for example, at ICAO from the travel document forgery perspective. IND needs to consider the relevance of all these disparate standards groups to their business and determine in which they need to be involved. Some standards will emerge by themselves, but these should be tracked by IND to determine whether and when they become relevant.

3.4.5 Sharing biometrics data implications and benefits

The following table contains a discussion on the practicalities of IND sharing biometric data with a number of the external entities shown in Figure 2. We have only included those external entities that have been identified as needing to exchange biometric information with IND either now or possibly in the future.

Where appropriate to the application constraints, fingerprint should be considered as the first choice of biometric. Not doing so leads to two immediate issues:

- Advantage cannot be taken of large existing databases of fingerprints such as PITO's NAFIS and the EU EURODAC for background checking. This is particularly significant in the light of the fact that most of IND applications are concerned with fraud and other criminal activities.
- A person could have multiple identities on multiple systems.

It should be noted that this recommendation is in line with the IGC recommendations for a "comprehensive migration management strategy" [IGC].

This is not to say that other biometrics should not be used where appropriate. The nature of this constraint might change as other databases (e.g. PITO's IDENT1, UKPS and UKvisas start to collect other biometric data). For example, the possibility of passports containing biometrics from 2004/5 will be significant, though it is likely to take several years before all passport holders carry these new passports.

Technical interoperability rules for IND biometrics projects should be drawn up in line with existing biometrics data standards such as CBEFF. For all new projects, consideration should be given to the storage of raw image biometric data, rather than just templates, for future-proofing purposes.

Consideration should be given to acquiring two, or even all three, of the biometrics types at the points of enrolment. This would provide for maximal future-proofing, but the cost implication would need to be considered. The capture of more than one biometric would also help address problems associated with those individuals who cannot provide certain biometrics (e.g. not having all required fingers).

This would also build up the databases for deploying multi-modal biometrics systems where matching is performed on more than one biometric at the same time. This can have advantages so long as manual intervention is available to arbitrate when the match results disagree. The research being carried out by PITO in Integrated Intelligent ID systems will be relevant here and IND should make every effort to work closely with PITO so as not to duplicate effort.

External entity	Biometric sharing discussion
PITO	IND sharing data with PITO helps criminal investigations in areas such as benefits fraud and 'watch-lists' of those individuals considered to be an immigration threat. PITO is researching an Integrated Intelligent ID Project. They are sponsoring research at University of Kent on multi-classified systems where results of searches on multiple systems are interpreted. PITO would like to share information from many other agencies and extract metadata. Subsequently, Intelligent Agents could be used to guide the user through the data complexities based on the task in hand. Intelligent Interfaces could know the user and present relevant simplified interfaces. There is already co-operation between PITO and IND in sharing fingerprint records for the IND IAF Programme (PIFEprojects linking IAFS database to NAFIS)
FCO	FCO and UKPS need to spot duplicates so could share common list of all current UK passport holders
UKvisas	There is interest in detecting UK visa applicants who subsequently claim asylum in the UK. Visa refusals biometric data will be useful for watch-lists to identify those trying to claim asylum on arrival in the UK. A biometric collected from visa applicants could be used to expedite the clearance of visa holders whose visa already grants them leave to enter: but there are no plans for this yet
DfT	No plans for sharing with IND since only looking at staff access control within closed systems at airports. Might be possible to agree a common staff access control method for IND UKIS immigration officers working in airports. In the future, DVLA might share biometric information for Entitlement Card multiple enrolment checking.
Entitlement Card Unit	Same need as for DVLA and UKPS if the Entitlement Card scheme goes ahead.
UKPS	Sharing data with FCO and IND to combat fraud. Also, same need as for DfT (DVLA) if the Entitlement Card scheme goes ahead.
Carriers	Biometrics collected at check-in could link bogus asylum seekers (document flushers) to their arrival flights and their travel documents. This would speed up their return to where they came from and allow the carrier to avoid being fined. Could also link biometric data to luggage streamline check-in process. Sharing such data with IND might enable linking of passengers to suspect packages for example.
Travel Agents	Machine Readable Data from travel documents can be provided to carriers, currently biographical, ICAO recommendations to include biometrics. International use of Biometric passports likely to start circa 2005.
National Governments	General criminal investigations like the sharing with PITO above. Could be used for speedy returns of illegal immigrants.

External entity	Biometric sharing discussion
EU	Asylum seeker fingerprint records have been shared with the EURODAC database since January 2003. There are two benefits to sharing this data with the EU: 1. Returning asylum seekers registering at 3rd countries to the EU state in which they first registered for asylum. The idea is to prevent asylum shopping in EU states. 2. Detecting benefits fraud where entry to the UK is gained on valid EU travel documents and then asylum is subsequently claimed without the documents. Other relevant databases identified are EUROPOL and SIS.
Biometrics association and standards bodies	Standards information for projects. Associations supply good information about what is coming next and what other relevant bodies are thinking.

3.5 IND Business Needs and Requirements

Biometric technologies are defined as automated identification, or verification of human identity through measurable, repeatable physiological and behavioural characteristics (see section 3.3).

This section identifies the business needs for person identification and verification within IND's current operations. IND operations are then further analysed to produce a list of practical requirements for which particular identity and verification functions can be used to meet.

The business needs and requirements detailed within this section have been collected from the interviews conducted and from documentation provided. A list of interviews carried out is provided in Annex A.

3.5.1 IND Business Needs

The business needs raised by IND staff and applicable external parties can be summarised as shown in the table below.

#	Business Need
1	Ensure documents are only issued to those entitled to hold them
2	Ensure that documents are only accepted when presented by the legitimate holder
3	When an individual deals with the UK government on multiple occasions the UK government should always be aware that it is dealing with the same person
4	Access to sensitive systems and information should be restricted to legitimate personnel
5	Reduce processing costs
6	Provide legitimate travellers with an excellent and timely service.
7	Ensure document integrity
8	Provide a means to identify persons attempting to enter the UK or already

#	**Business Need**
	present in the UK who may have illegal travel or visitation intentions. (e.g. terrorism suspect, deportation orders, visa refusals etc.)

Business needs 1-4 relate directly to the identification and verification of individuals, and can therefore be directly met by the introduction of biometric systems, where appropriate to an individual project's business requirements.

Business needs 5 and 6 are more general but have been included due to the specific opportunity presented by the introduction of biometric systems to enable the automation and streamlining of various processes to enable a reduction in operating costs. Such examples include expedited border control freeing up staff time and port real estate, or biometrics being used to enable issuance of paperless documents (e.g. Australian Electronic Travel Authority) saving on secure printing costs.

Business need 7 highlights the necessity of considering the application of biometrics within the wider realm of identity and credential management. Electronic document integrity (i.e. ensuring a document has not been tampered with since issuance, and ensuring the credentials attributed to a document were assigned by a legitimate member of staff) is a wider identity function bound up with non-repudiation services regarding the credentials of a presented document. Biometrics are not the answer to providing such services, but they are, when used in conjunction with other identity technologies such as secure tokens and digital signatures, a useful building block in the provision of a user-friendly and trustworthy document integrity system.

Business need 8 is closely related to needs 1 and 2. Whereas business needs 1 and 2 are about ensuring someone purporting to be a legitimate visitor or resident is indeed telling the truth, business need 8 is about proactive detection of illegitimate travellers who may well seek to bypass legitimate traveller checks entirely, or legitimate travellers who are suspected of illegal activities or intentions.

3.5.2 Summary of the IND Identity and Verification Requirements

The following table summarises the person identity and verification requirements, both now and in the future, identified by the interviewees listed in Annex A.

#	**Requirement**
R1	Expedited arrivals for low-risk travellers
R2	Matching asylum seeker applicants with people previously entering the UK
R3	Identifying under-5s already presented as dependents at asylum seeker units.
R4	Preventing boarding card swapping by ensuring that the people checking in are the same people who board flights
R5	Matching those arrivals claiming to have no travel documents with foreign-national UK visa applicants.
R6	Verify document ownership
R7	Real-time access to 'watch-list' data for preventing passage to UK in advance of boarding.

#	**Requirement**
R8	To allow IND biometric checks to be conducted anywhere (asylum seekers).
R9	To allow IND biometric check results to be obtained whilst the subject is still present, without causing undue inconvenience.
R10	Identification of asylum seeker reporting and/or collecting benefit.
R11	Physical and logical access control to buildings areas and systems.
R12	Proof that a member of staff with appropriate privileges executed certain security-related actions, e.g. document endorsement; database updates.
R13	Preventing an individual from successfully enrolling multiple times for the same IND documents using different identities.

3.5.3 Needs to Requirements cross-reference

In order to ensure the current and future identity and verification requirements identified cover the full remit of IND operations, the table below cross-references the requirements to the business needs.

#	**Business Need**	**Requirements**
1	Ensure documents are only issued to those entitled to hold them	R2, R3, R12
2	Ensure that documents are only accepted when presented by the legitimate holder	R1, R4, R6, R7, R10
3	When an individual deals with the UK government on multiple occasions the UK government should always be aware that it is dealing with the same person	R2, R3, R5, R7, R9, R10, R13
4	Access to sensitive systems and information should be restricted to legitimate personnel	R11, R12
5	Reduce processing costs	R1, R2, R3, R10
6	Provide legitimate travellers with an excellent and timely service.	R1, R9
7	Ensure document integrity	R6, R10, R13
8	Provide IND staff with an effective means to rapidly identify persons attempting to enter the UK or already present in the UK who may have illegal travel or visitation intentions. (e.g. terrorism suspect, deportation orders, visa refusals etc.)	R7, R8, R9

The above table is a clear indication that IND has effectively identified current and future requirements that tackle all of the identified business needs.

3.6 Proposed Framework for Biometrics

This section attempts to analyse (at a very high level) the appropriateness of the three types of biometrics in relation to:

- The Current and Future Person Identification & Verification Requirements of IND
- Categories of person or customer of IND
- High level functions performed by biometric systems.

3.6.1 Person-type Segmentation

In order to drive out all the potential uses of person identification and verification, we start by identifying the person-type categories that IND has to deal with in day-to-day business. We are aware that more detailed segmentation could be made (especially for foreign travellers), but we have decided to use this high level because of the brevity of this study.

Person type	Description
UK travellers	Travelling on a UK passport. Perhaps renewing a passport. Checked by carrier on exit from UK. Expect Expedited arrivals on return to UK.
Foreign Traveller	Non UK citizen entering the UK with or without legitimate travel documents. This includes non-UK EU travellers.
Asylum Seeker	asylum seekers often arrive by uncharted routes without documentation + suspects.
After entry casework subjects	Applicants for British Nationality, extended leave to stay, etc.
Staff	Staff of the Control Authority organisations and partner organisations including IND, PITO, BAA, DFT, etc. These staff have access to secure areas and systems. They also sometimes endorse certain actions electronically which might be useful to track back to them such as EU resident permit issuance.

3.6.2 Biometric Function Segmentation

Biometric technology enables two basic functions to be performed:

- *Identification*: Who is the subject? Have we met them before?
- *Verification*: Is the subject who they claim to be?

For the purpose of this study, two types of identification function are considered, due to the dual role IND performs in assisting legitimate travellers whilst protecting the integrity of UK borders. This approach leads to the identification of 3 biometric functions that are subsequently mapped to IND requirements within this framework

1. **Enrolment searches:** This is an *identification* function used to check against lists of legitimate UK visitors and temporary residents or previous applicants. Applications include ensuring a document applicant is not issued with documents under multiple identities.
2. **Biometric Watch-list searches:** This is an *identification* function for detecting those suspected of illegitimate activity, e.g. an applicant not present in a list of undesirables. Can be done for visa and passport applications. Much harder to do in real-time at point of entry.
3. **Identity confirmation:** bearer is person to whom document was issued. This is an *authentication* function.

3.6.2.1 Enrolment Searches (ES)

This is 1:n matching for both ‘positive’ cases (i.e. seeing if a traveller is previously registered for expedited travel, or if an asylum seeker has previously sought asylum) and ‘negative’ cases such as checking whether an applicant is previously enrolled under a different ID. Key characteristics:

- Databases could be very large.

- Collecting high-quality enrolment data in a controlled environment is very important in order to minimise false matches.
- Enrolment procedures for automated border entry must be robust to ensure the integrity of border control.

3.6.2.2 Watch-list Searches (WS)

3.6.2.3 Identity Confirmation (IC)

This is 1:1 matching of claimed Identity versus actual identity. Key characteristics:

- Throughput at points of entry should be not be hampered by this function.
- Could be used for:
- expedited clearance of low risk categories of passenger when combined with a security token or biometric passport.
- establishing individuals are true owners of travel documents (though this does not in itself grant a UK immigration entitlement).

3.6.3 Biometric Cross Reference matrix

The following table shows how the biometric functions identified above can be used to meet the identity and verification requirements defined in 3.5.2 for the person-types defined in 3.6.1.

Where existing IND projects exist to tackle a particular requirement for a particular people segment, the project name is shown on the table below in italics. More information about each named project can be found in Annex B.

A point to note in this table is that in many instances IC *or* ES may be appropriate depending upon whether a token or machine-readable travel document is presented by the person interacting with the service.

Person-Type **Requirement**	UK traveller	Foreign traveller	Asylum Seeker	Case work after entry	Staff
R1 Expedited arrivals for low-risk travellers	IC / ES	IC / ES *IRIS*	--	--	--
R2 Matching asylum seeker applicants with people previously entering the UK	--	WS *IAFS* *Hornet / NAIR*		--	--
R3 Identifying under-5s already presented as dependents at asylum seeker units.	--	--	ES *RANS* *IAFS*	--	--
R4 Preventing boarding card swapping by ensuring that the people checking in are the same people who board flights	IC / ES *Verlaine*	IC / ES	--	--	--
R5 Matching those arrivals claiming to have no travel documents with foreign-national UK visa applicants.	--	WS *UKvisas / IAFS*		--	--
R6 Verifying Document Ownership	IC *Entitlement Card* *UK Passport*	IC	IC *ARC*	IC	IC
R7 Realtime access to 'watch-list' data for preventing passage to UK in advance of boarding.	--	WS *e-borders*	--	--	--
R8 To allow IND biometric checks to be conducted anywhere	--	--	IC / ES *IAFS* *ARC*	IC / ES *ARC*	--
R9 To allow IND biometric check results to be obtained whilst the subject is still present, without causing undue inconvenience.	--	WS *Hornet / NAIR*	IC / ES *IAFS* *ARC* *Hornet / NAIR*	IC / ES *ARC*	--
R10 Identification of asylum seeker reporting and/or collecting benefit.	--	--	IC *VIAFS*	--	--
R11 Physical and logical access control to buildings areas and systems.	--	--	--	--	IC / ES / WS
R12 Proof that a member of staff with appropriate privileges executed certain security-related actions, e.g. document endorsement; database updates.	--	--	--	--	IC / ES
R13 Preventing an individual from successfully enrolling multiple times for the same IND documents using different identities.	ES	ES	ES *IAFS*	ES	ES

The following sections justify and expand each of the requirement cross references shown above, including a discussion as to the pros and cons of using particular biometric technologies to meet the requirement.

3.6.3.1 R1 - Expedited arrivals for low-risk travellers

There is potential that border control could make a resources saving at the same time as providing a faster and more efficient service to legitimate travellers through the use of biometrics for expedited travel. This could either be achieved through a 1:1 identity check alongside some sort of secure token (e.g. a biometric passport) or through a search against data gathered from those registered to use the service.

Biometric	Pros	Cons
Fingerprint	• Accuracy proven to work for large databases, • Interoperabilty with other existing systems for background checks.	• Association with criminality could reduce uptake and hence limit cost saving. • Current ES AFIS implementations unlikely to be fast enough for expedited processing. No business case where system requires operator to roll fingerprints.
Iris	• Not associated with criminality, potentially greater uptake and greater cost saving. • Good customer feedback & performance from SPT trial.	• Not previously implemented with databases in the millions, hence risk for ES approach. (not a problem if IC type system used in conjunction with secure token)
Face	• People used to providing photographs for travel documents	• Current inaccuracies mean that ES approach not viable, would have to be IC with token.

Currently, the IRIS project within the e-borders programme is looking into using Iris technology for this function via the ES approach (i.e. large database and no tokens).

Whilst the cost of tokens may be considered prohibitive, the move by the US government to look towards the issuance of biometric passports by the end of 2004 and subsequent ICAO recommendations (including optional iris template) should not be considered insignificant in this area, and is likely to be re-usable for expedited travel. The requirements, costing and business case for any separate initiative should be documented with this possibility of being superseded by wider international passport developments in the medium term.

As discussed in section 3.3.2.10, consideration of the use of tokens alongside biometrics, allowing 1:1 rather than 1:*n* matching would enable a greater choice of biometric types for expedited travel without taking on the risk of applying technologies to a scale of problem for which they are, as yet, unproven.

Another risk that use of tokens help to mitigate is that of the system becoming a victim of its own success. A 1:*n* system that is received well by travellers may find itself with a rapidly growing user base and a subsequently unacceptable drop in performance, damaging the good reputation built by the early success.

3.6.3.2 R2 - Matching asylum seeker applicants with people previously

entering the UK

One of the checks that should be able to be performed when a person applies for asylum is to do an enrolment search to ensure that they have not previously entered the UK using valid travel documents.

This applies to all travellers, not just EU travellers. However, the principle constraint in this area revolves around the right to 'freedom of travel' within the EU for all EU citizens. This makes it currently impossible to capture any biometric other than face (through the rapid scanning of travel documents) border crossing (until such a time as other biometric information is included in the EU passport).

Biometric	Pros	Cons
Fingerprint	• Large databases of fingerprints within Eurodac. • Used already by IAFS and ARC. • Good performance for 1:n matching with multiple fingers	• Cannot be gathered from EU citizens at time of border crossing
Iris	• Good performance for 1:n matching	• Unproven for largest databases. • Cannot be gathered from EU citizens at time of border crossing
Face	• Can be gathered from EU citizens at time of border crossing without delaying their journey unnecessarily	• Questionable whether the quality of photo gathered will be sufficient to provide credible results at subsequent asylum enrolment.

A limited trial, known as Hornet, was carried out at Dover, involving the capture of photographic images that were subsequently shipped to Croydon to search for matches during the asylum application process. The results of the trial were inconclusive, and the NAIR project is now underway to investigate this area further.

Whilst 'freedom of movement' means an EU citizen cannot be detained to gather biometric data at entry against their will (limiting the data that can be gathered at this point in time to facial image) many travellers will be willing to 'trade' biometric data in order to achieve a smoother passage. For instance, data voluntarily provided for an expedited travel system, as discussed in section 3.6.3.2 above could also be shared with IND in order to help prevent bogus asylum claims should a suitable biometrics data sharing infrastructure be in place.

As an aside, an expedited travel system could be a useful means of reducing the number of searches and the facial database size being searched for this requirement by simply moving pre-registered travellers to a different and potentially faster-moving queue.

Sharing biometric data gathered for different applications within IND, whereby multiple biometrics can be gathered on individuals to increase the quality of the system both in terms of the service provided to the individual, and as a whole, is likely to take a number of years before it returns significant benefits. Such an approach, however, is not without precedent, and IND must ensure that they

monitor closely the progress of the PITO IDENT1 initiative, where just such a joined up identification approach is being taken forward by the police.

3.6.3.3 R3 - Identifying under-5s already presented as dependents at asylum seeker units

It is common knowledge that asylum seekers with families receive preferential treatment, appropriate to the vulnerable nature of their young children. With this in mind, there is a potential for 'child sharing', where an individual child is used in the asylum application process by multiple 'parents'.

A biometric enrolment search to enable children to be checked against children already presented would close this loop-hole.

Biometric	Pros	Cons
Fingerprint	• Currently gathered from all asylum seekers over 5 as part of existing processes.	• Fingerprints of under 5s change (stretch) too frequently for this to provide an accurate *historical* record.
Iris	• Iris patterns are stable and usable a very young age • Database size should be within iris proven limits today.	• Not currently used in asylum seeker processing
Face		• Facial recognition of children not suitable for ES type searches.

The Restricted Access to NASS Support (RANS) project is currently working in this areas, and IND policy have recently made the appropriate changes to allow the collection of fingerprints from under 5s. It should be noted that, as with all projects, the complete requirements need to be fully analysed before a specific single biometrics can be recommended. For example, it might be possible to use fingerprints for this application if the requirement is to spot children in appearing again within just a few weeks or months.
There is very little data on under 5's regarding the stability of their biometrics, how easy it is to enrol and use their biometrics. Modified capture devices and algorithms might enhance performance for this particular age group compared to using the "adult" versions of the systems.

3.6.3.4 R4 - Preventing boarding card swapping by ensuring that the people checking in are the same people who board flights

Many airports worldwide have both domestic and international flights sharing the same 'airside' space. With this in mind, there is potential for someone checking in for an international flight with legitimate travel documents, and then allowing a person who checked in for a less stringently checked domestic flight to board in their place.

This not only effects IND, but also the Carriers who are fined for every illegal arrival that can be traced back to one of their flights.

One way to prevent this is for the carriers to register biometric information for every traveller at check-in, which is validated at boarding, either through an identity confirmation (in conjunction with a secure token, e.g. biometric passport

or other travel document/ticket) or through an enrolment search against a database.

Biometric	Pros	Cons
Fingerprint	• Good performance of IC and ES checks	• Association with criminality may offend legitimate travellers.
Iris	• Good performance for IC and ES checks	-
Face	• Can be collected from existing travel documents.	-

Currently the Verlaine project is looking at capturing facial biometric data at check-in for meeting this requirement, enabling ES type searches on one planeload of passengers at a time – database size of 3-400.

3.6.3.5 R5 - Matching those arrivals claiming to have no travel documents with foreign-national UK visa applicants

This is a subtle difference between this requirement and R2. R2 is concerned with matching legitimate travellers who have crossed UK borders. This requirement is about performing an ES type check for those who have been granted visas to enter the UK, to prevent them entering, destroying their visa and then claiming asylum.

Since this requirement relates to non-EU foreign travellers, it does not suffer from the same constraint 'freedom of movement' for EU citizens that is so important in R2. For this reason, biometrics other than face are worth greater immediate consideration.

Biometric	Pros	Cons
Fingerprint	• Compatible with existing Asylum processing • Fingerprint well proven for multi-finger ES • Compatible with EURODAC and Police records	• Association with criminality may cause offence to Visa applicants • Cannot be gather remotely (e.g. for postal applications)
Iris	• Iris promises excellent performance for ES	• Iris not currently collected as part of existing asylum processing • Risk in that Iris not yet implemented with very large databases for ES • Cannot be gathered remotely (e.g. for postal applications)
Face	• Visas can still be processed by post if required.	• Accuracy for ES type searches may not be acceptable.

Currently the UKvisas/IAFS project is looking at collecting fingerprint during the Visa application process within a pilot country by Q4 2003. This data will then be to IAFS for subsequent ES checking during Asylum registration.
Long-term issues include the sheer volume of data that would be gathered if this pilot was expanded. UKvisas currently process 2.2 million visa applications per year, where IAFS is currently dealing with numbers an order of magnitude smaller.

3.6.3.6 R6 - Verifying Document Ownership

A principle requirement throughout all of IND operations is the need to verify document ownership, be that document a passport, ARC, work permit, visa, or some other official document.

A biometric can be used to help meet this requirement, in conjunction with a secure token (which could be embedded in the document itself) or a document with machine-readable Biometric data on it, by means of an identity check.

Biometric	Pros	Cons
Fingerprint	• Good 1:1 matching • Fingerprint seems to be favoured by US govt.	• Cannot reliably be collected covertly • Associated with criminality • Inclusion on passport only optional in ICAO current recommendation
Iris	• Good 1:1 matching • No association with criminality yet.	• Cannot be collected covertly • Proprietary technology means ICAO cannot formally endorse • Inclusion on passport only optional in ICAO recommendation
Face	• Capable of 1:1 matching if photo quality is sufficient • Easy for a human being to manually cross check result • ICAO recommendation states a full face image as mandatory biometric.	• Need to ensure photo capture is under suitable conditions • Covertly collected images might not be high enough quality

Work is being undertaken in this area by both UK Passports and the entitlement card initiative (at consultation stage).

Fingerprint is being currently being used to ensure ownership of the ARC for asylum seekers.

3.6.3.7 R7 – Real-time access to 'watch-list' data

3.6.3.8 R8 - To allow IND biometric checks to be conducted anywhere

Timely access to ES and WS results are essential to the majority of IND operations, and in a number of disparate locations. The security of these locations, and cost requirements for hardware vary greatly, and it is a requirement of IND to be able to overcome such barriers for asylum seeker tracking. In addition, this requirement may also include the need for wireless/mobile accessed identity checks.

Biometric	Pros	Cons
Fingerprint	• Proven for 1:n matching • Fast capture if just 2 print • Capture devices can be low cost and highly portable	• Multiple fingerprints required to maintain accuracy over large databases
Iris	• Non-invasive, fast capture. • Good ES and WS performance	• Unproven scaling for largest databases (millions) 1:n matching
Face	• Capture devices are many and varied and hence low cost	• 1:n matching performance very limited without manual intervention

The portable QuickCheck stations provided under the IAFP meet this requirement for fingerprint, enabling a match against the IAFS database in around 4 minutes. A range of possible matches is often returned which would then resolved by a human 'operator' using biographical data.

3.6.3.9 R9 - To allow IND biometric check results to be obtained whilst the subject is still present

As mentioned previously, timely access to ES and WS results are essential to the majority of IND operations, as it is unacceptable to detain legitimate travellers unduly on the off chance of a match, and in any case, any time spend waiting around for results by IND staff is a waste of resource.

Biometric	Pros	Cons
Fingerprint	• Proven for 1:n matching	• Multiple fingerprints required to maintain accuracy over large databases
Iris	• Trials thus far indicate rapid processing of results	• unproven for large database 1:n matching
Face	• Capture of photograph of subject is a fast & simple process	• 1:n matching performance low, requiring manual supervision.

As with R8, the portable QuickCheck stations provided under the IAFP meet this requirement.

This requirement is also a driver for the NAIR project, where EU citizens cannot be held up, and therefore the only viable biometric at this point in time is a facial image obtained via CCTV or document scanning.

3.6.3.10 R10 - Identification of asylum seeker reporting and/or collecting benefit

One of the issues with preventing abuse of the asylum system is ensuring that those seeking asylum report when they are supposed to.

In addition to this, the ability to protect the integrity of benefit payments is key: Benefit should be paid to the appropriate person and should only be paid whilst the payee is still eligible to receive it. Thus, use of IC in conjunction with a secure Token is the logical way to control this process, providing card reading and Biometric infrastructure is present at point of interaction.

Biometric	Pros	Cons
Fingerprint	• Currently used within Asylum processes • • Cost of capture devices is fairly low	• Criminal association (although already acceptable through current system).
Iris	• Excellent performance for 1:1 IC checks: no scaling problems	• Not currently used within ARC system
Face	• Expected introduction of facial biometric into international travel documents commencing circa 2005 • Good performance for 1:1 IC. • Low cost of capture devices	• Not currently used within ARC system

The ARC enables a 1:1 IC to be performed based upon two fingerprint templates stored on the card (see section 3.3.2.10 for a general discussion of the use of secure tokens such as the ARC in conjunction with biometrics). The card also includes a 'next report datefield enabling the withdrawal of benefit should an asylum seeker not meet their reporting obligations. The card is presented for benefits collection, but currently the fingerprint biometric is not verified.

3.6.3.11 R11 - Physical and logical access control to buildings areas and systems

Access control for staff was a requirement across all of IND operations, for various reasons:

- Protecting access to sensitive information
- Protecting access to sensitive systems (e.g. secure document printing)
- Non-repudiation (linking actions to employees to ensure proper audit trail as a deterrent to corruption)
- Integrity of staff identification to make it as difficult as possible for impostors to pose as IND staff.

Biometric	Pros	Cons
Fingerprint	• Mature technology • Maybe used for IC or ES.	• Hardware performance issues – (e.g. coping with humid office environment) • Staff might dislike the use of fingerprints
Iris	• ES proven to work well for physical access with limited numbers. • Excellent performance of 1:1 IC.	-
Face	• Photos can be manually verified by humans as a cross check • Good for 1:1 IC in conjunction with a Token	• Poor for 1:n

One initiative in this area is being looked at for airports by DFT/BAA – to better manage staff access to 'airside'. In the twelve-month period between 15/10/00 and 15/10/01 there were no less than 6769 cases of people being found airside without appropriate documentation at Heathrow, or 18.5 per day. This includes legitimate passengers who have thrown away their travel documents to claim asylum. Better control of this area for both staff and travellers is being investigated.

A demonstration of iris technology was given with a view to tackling a specific problem of Immigration Staff access to a controlled area through an unmanned door, but this has yet to be taken any further, possibly due to BAA wide investigation work that is underway, to ensure a co-ordinated and consistent approach across all UK airports.

This is another area where the problems relating to 1:n type searches may be mitigated through the introduction of secure tokens, as with R1. See section 3.3.2.10 for further discussion on the use of secure tokens in conjunction with biometric technologies.

3.6.3.12 R12 - Proof that a member of staff with appropriate privileges executed certain security-related actions

This is not so much a requirement that can be met with biometrics, rather it is a function where the use of biometrics in conjunction with other technologies can help to provide the most trustworthy and user friendly system.

Biometric	Pros	Cons
Fingerprint / Iris / Face	• Can be used in conjunction with a secure token to authorise digital signing of an action	• Additional cost of biometric and integration with existing network hardware.

No existing initiatives currently meet this requirement, although access to the remote terminals for the warnings index currently uses secure tokens along with password to control staff access (See section 3.3.2.10 for further discussion on the use of secure tokens in conjunction with biometric technologies). It is areas like this where biometrics could enhance security and user experience.

3.6.3.13 R13 – Preventing multiple enrolments

This requirement is principally about the prevention of an individual from successfully enrolling multiple times for the same IND documents or privileges using different identities.

Another key requirement for IND is to ensure that they don't process the same person twice without knowing it.

Biometric	Pros	Cons
Fingerprint	• Fingerprints already held for all asylum seekers for the last 10 years. • High accuracy and allows cross-checks with Police systems. • Compatibility with EURODAC to check against other asylum requests throughout the EU.	• Criminal connotations may cause problems, particularly for applications where collection is voluntary.
Iris	• Hi accuracy in 1:n searches based on available data	• No legacy data available • Unproven for ES type actions on large databases (e.g. millions)
Face	• Can be gathered remotely, e.g. by post	• Poor technology for ES type actions without significant manual involvement

The IAFP currently sets out to meet this requirement using fingerprints for UK Asylum seekers, looking to prevent multiple enrolments both within the UK and throughout the EU (via EURODAC).

Which technology is appropriate depends upon the application for which enrolment is being attempted. For instance, fingerprint is ideal for asylum seekers, but for passport applications, a high proportion of which are processed by post, it is not practical without major changes to existing business processes and the associated expense.

3.6.4 Allocation of biometrics to requirements

In the table below, we take each IND requirement and allocate which biometrics we feel are appropriate currently and consider how this might change in the future. We are not making absolute recommendations since each cases requirements needs to be considered in detail which has not been possible during this short study. Clearly where the future biometric choice is different from the current one, serious consideration needs to be given to the potential wasted investment and migration costs.

We are expecting to see biometric travel documents emerging over the next 2-3 years. However, are not expected to be global and will take several years to roll out even in the countries which are early adopters.

Requirement	**Observations**
R1 Expedited arrivals for low-risk travellers	Today: **Fingerprint (with token)**, **Iris (with token)** • Fingerprint association with criminality means that an Iris-based system achieve greater uptake amongst frequent flyers from some countries • Fingerprint allows extensive background checking at enrolment stage. • Registering parties are low risk cases, and are unlikely to register if they intend any illegal activity; therefore the need for sharing data gathered via this system is minimal, making iris a good choice particularly if database size can be constrained by application context. • **Use of Token:** Secure Token or machine readable document could be used to mitigate very large database risks through reducing problem to 1:1 IC instead of 1:n ES. However, if token is used any Biometric may be suitable. Future: **Biometric Passport**
R2 Matching people entering UK with valid travel docs to subsequent asylum seeker applicants	Today: **Face (if at all)** • 70% of people entering the UK are EU citizens who have freedom of movement and as such cannot be delayed in order to gather biometric data. For this reason only facial data can practically be gathered at this time. • Whether this is of practical use right now is yet to be proved (NAIR project), Future: **Biometric Passport**
R3 Identifying under-5s already presented as dependents at asylum seeker units.	Today: **Fingerprint (if longer-term historical records not needed)** • IAFS system already in place, and IND policy now allows the collection of fingerprints from children Future: **Iris** if can be shown to match all current fingerprint functionality
R4 Preventing boarding card swapping by ensuring that the people checking in are the same people who board flights	Today: **Face** • Airline carriers already require the presentment of passports, enabling document scanning and the collection of facial biometric data. Only useful if checking limited to small databases (e.g. single flights) Future: **Biometric Passport, Iris?**
R5 Matching foreign-national UK visa applicants with those arrivals claiming to have no travel documents	Today: **Fingerprint** • As the current asylum system uses fingerprints, the most effective means of meeting this requirement would be the collection of fingerprints from visa applicants, if diplomatically achievable within target countries Future: **Iris? As a UK visa grants leave to enter the UK, an iris biometric taken at the time of visa issue could grant automated border entry also.**

Requirement	**Observations**
R6 Verifying Document Ownership	Today: **Fingerprint/Face** for IC • ICAO recommendation for machine-readable travel documents cater for the inclusion of all three biometric technologies. • Looks like only facial image will be the mandatory ICAO biometric (image) stored in travel docs • Full endorsement of iris pending release of patent Future: **Fingerprint, Biometric passport/visa**, **Iris?**
R7 Realtime access to 'watch-list' data for preventing passage to UK in advance of boarding.	Today: **Face/Fingerprint** • Currently facial image the only biometric that it is practical to collect from presumed legitimate travellers prior to boarding Future: **Iris, others** • Collection of multiple Biometrics will allow future searches against this data.
R8 To allow IND biometric checks to be conducted anywhere	Today: **Fingerprint** • Currently able to match fingerprint • **Use of Token:** Reducing problem to 1:1 IC allows other Biometrics to be considered. Future: **Iris** •
R9 To allow IND biometric check results to be obtained whilst the subject is still present, without causing undue inconvenience.	Today: **Fingerprint** • Face not appropriate for ES due to delay in manual processing required. • **Use of Token:** Verification against a token/document will give better speed/performance/convenience. Future: **Biometric passport/visa, Iris (**likely to provide fast checking when databases exist.)
R10 Identification of asylum seeker reporting and/or collecting benefit.	Today: **Fingerprint** • ARC in place and producing results. Future technologies: **Fingerprint** until other databases allow checking with other biometrics
R11 Physical and logical access control to buildings areas and systems.	Today: **Iris for ES** • Iris performance statistics good for staff user base. **Fingerprint or other for IC** • Any biometric may be appropriate in conjunction with a token.
R12 Proof that a member of staff with appropriate privileges executed certain security-related actions, e.g. document endorsement; database updates.	Future: **Fingerprint** • **Use of Token:** Any biometric appropriate in conjunction with a token and wider identification system (e.g. non repudiation provided by PKI)

Requirement	Observations
R13 Preventing an individual from successfully enrolling multiple times for the same IND documents using different identities.	Today: **Fingerprint** allows widest background checks • Fingerprint already used within asylum system. • Face most convenient for other documents, as it does not exclude postal applications Future: **Combination** of Biometrics

3.7 Findings

This section describes the key themes we have identified relating to Co-ordination of biometrics within IND during this study before recommendations are made in the following section.

3.7.1 Observations on current status

While all parties interviewed were co-operative and happy to talk to us, we detected a tension between UKIS and the rest of IND. This is perhaps not surprising when the nature of the work of the two is compared.

What is important is that all of IND's work is co-ordinated through a common overarching coherent strategy and that communication channels remain open at all times.

Without prejudice, the current status within IND gathered from our interviews can be summarised using the following observations:

- It is BISTD's role to deliver IT to all projects within IND but some projects keep IT to themselves if it is new and interesting (e.g. a biometrics system as opposed to a help desk system).
- At the same time, some other parts of IND say they do not have confidence in BISTD's track record to deliver efficiently and on time and so are inclined to not share their plans for projects with IT elements, especially where they are under heavy time pressure from Ministers to deliver results.
- There are pockets of specific biometric technology experience within various part of IND. There is a danger that departments are each growing their own narrow expertise, 're-inventing the wheel' and not benefiting from each other's biometric project experience.
- There are several potential biometrics projects starting up within IND and new ones seem to be appearing fairly regularly. There is no common channel through which these projects are funnelled to share experience and get best advice.
- Internal communication and co-ordination in respect of biometrics technology projects within IND is poor. There was an IND biometrics group chaired by Dave Roberts (UKIS) that used to meet by teleconference. However, co-ordination of this group has stopped and so meeting are no longer being held.
- There seem to be examples of IND policy constraining further than the constraints placed on IND by external legislation. This can give rise to frustration in IND powers of operation being unnecessarily limited. E.g. not being allowed to collect fingerprints under certain conditions.

- There is poor co-ordination of representation at relevant external biometrics standardisation meetings. In the time available for this study we have identified the following attendees:
    - An official from IND attends the UK Government Biometrics Working Group (BWG);
    - An official from UKIS represents IND at ICAO NTWG meetings along with a representative from UKPS;
    - An official from UKIS leads the UK delegation to the EU Commission Article 6 visa security committee as well as representing IND at the European Forum for Travel Documents.
    - BISTD attends the Inter-Governmental Consultancy (Technical Group) meetings;
    - A consultant currently employed by BISTD was, until recently, was Chairman of AfB and attends the meetings. However, he has not been asked to represent IND at AfB. It seems significant that PITO are heavily involved in AfB and yet IND are not.
- Within the timescales of this study, we cannot be sure that we have had sight of all of IND's liaison activities. There seems to be poorly co-ordinated IND representation and liaison with:
    - international governments
    - the EU and
    - UK Government agencies such as Police, UKPS, UKvisas, DfT and FCO.

  This is important not only from the data sharing point of view, but also because there are potentially huge opportunities to share biometrics research and strategy between UK Government departments (e.g. the research programmes being initiated by PITO and DfT). If IND is not involved strategically at an early stage then the later individual project choices for appropriate biometrics might be limited purely by data-sharing requirements rather than business area requirements.

3.7.2 Co-ordination of Biometrics within IND for compliance with the framework

The list of IND identity and verification requirements (see section 3.5.2) for biometrics we have drawn up in the time available will certainly not be exhaustive and even if it were, new ones will arise as IND's business changes over time. Therefore, it is vitally important that as new business needs arise, they can be rapidly and methodically assessed as to their suitability for the application of biometrics.

Maximising the appropriate use of biometrics technology within IND is highly desirable since person identification/verification is core to IND business. The framework is designed to assist identifying which technologies are appropriate for which applications. As we have seen 'pros and cons' in the table below, there is no single biometric which is suitable for all applications. Therefore the choice of biometric technology must be application driven.

Furthermore, biometric technologies are extremely difficult to compare since a lot depends on any given implementation. It is not possible to give accurate meaningful performance figures for each technology since so much depends upon the implementation and particular integration requirements. Before an individual technology is selected for a given application, supplier systems should ideally be benchmarked in the locations in which they will be used in order to see compare how they perform under realistic constraints.

The best we can provide at this stage is a high-level comparison of the pros and cons of each of the three targeted biometric technologies:

Biometric	Pros	Cons
Fingerprint	• Established Technology • Easy to use • Understood in court of law (experts can corroborate) • Technology challenges now well known • Number of competing solutions • Exception cases understood and documented • Proven to work for large databases • Compatible with existing Asylum processing • Good 1:1 matching • Primary identity used for most immigration procedures for the last 10 years. • Extensive existing legacy of data relating to 'negative' individuals e.g. criminals. • Proven for 1:n matching with multiple fingers • Capture devices can be low cost and easily integrated	• Operator assistance required for AFIS technique enrolment (rolled prints) • Associated with criminality a deterrent to usage for some customer groups • Contact required – perceived hygiene concerns in some people groups • Human element in quality control • Cannot be gathered from EU citizens at time of border crossing • Fingerprints of under-5s change (stretch) too frequently for this to provide an accurate historical record. • Difficult to gather covertly • Multiple fingerprints required to maintain accuracy over large databases • Often returns a list of possible matches requiring human follow up inspection. • Slow data capture in Large-scale 10 rolled print AFIS systems

Biometric	Pros	Cons
Iris	• Facial images can be captured at same time providing multiple biometrics with no additional inconvenience • Automated quality control • Not associated with criminality, potentially greater uptake and greater cost saving. • No “man handling” necessary at enrolment • No contact with machine necessary – relatively easy to use. • Good 1:1 matching • Highly effective 1:n matching on database sizes tried thus far. • Systems designed to return automated absolute match/no match responses rather than lists of possibles.	• Unproven for large scale applications (millions) Largest application currently approx(> 100,000) 1:n matching. Little known about integration into different application environments. • Relatively bulky and expensive hardware • Concept patent situation must be resolved before it is likely to be recommended by standards bodies. • Extent and nature of exception cases needs to be addressed. • Cannot be gathered from EU citizens at time of border crossing • Cannot be gathered covertly • • Operator assistance required for some enrolments • Requires user co-operation, therefore unsuitable for young children or unco-operative adults
Face	• The biometric used by humans to naturally identify each other enabling manual crosscheck with minimal expertise • Possible to gather biometric remotely (e.g. by post) • No specialist hardware required • People used to providing photographs for travel documents • Can be gathered from EU citizens at time of border crossing without delaying their journey unnecessarily • Can be collected from existing travel documents. • Good to for 1:1 matching • ICAO recommendation currently states a full facial image as mandatory biometric, but this might change. • Can be gathered covertly	• Least effective technology of the three for 1:n matching. Current performance levels unacceptable for many applications • Facial image needs to be captured in correct lighting and aspect for good performance. • Least effective technology for 1:1 verification, even though performance is good.

3.7.2.1 Communication and independent advice

There are currently barriers to information sharing within IND:

- There are perceived to be 'camps' which prefer one biometric technology over others. While this turns out not to be true from our interview feedback, the perception is what matters.
- Advice is not being sought from experienced departments within IND because of perceived bias and information is not being freely shared.
- Departments attending important biometrics meetings are disseminating information gathered on a good-will basis to interested parties they are aware of. This means that it is not necessarily being disseminated effectively and it is not clear where such information should be sought within IND.
- Foreign contingents are seeking advice from IAFP

3.7.3 Strategic approach to new ID/verification projects

For a coherent biometrics strategy to be successful, it is vital that new biometrics projects do not continue to appear in pockets of isolation without all relevant departments being aware and having the opportunity to share their relevant experiences.

At the same time, any project vetting procedures must be signed up to by all departments in order to avoid them being side-stepped. There is often considerable pressure to find a solution to an identified problem in just a few months. Therefore, any vetting process must be set up to be and be seen to be extremely efficient and rapid in execution.

3.8 Recommendations

This section summarises the recommendations we are making as a consequence of the information gathered during this study and the biometrics framework proposed.

3.8.1 Co-ordination of biometrics within IND

There is clearly an urgent need to co-ordinate biometrics activities within IND. It can also be argued that this co-ordination would be most beneficial and cost-effective at a higher level such as the Home Office.

BISTD has been in place for only two years and has a track record of providing biometrics IT programmes such as IAFP. IND senior management should agree the role of BISTD as the IND central IT provider. To distribute IT provision will lead to inefficient use of resources and increased costs. The model of central IT Service provision is a sound one and has been seen to work in other organisations such as PITO.

Since each application tends to have very specific requirements, it is not possible to present an evaluation framework against which to mechanically evaluate new projects. Therefore, instead we provide some high-level recommendations here followed by a set of recommendations around establishing an independent expert body to co-ordinate all biometrics activities within IND.

We make the following recommendations regarding co-ordination of biometrics:

- ***Technology provision.*** It makes sense for IT project expertise and experience to be built up in one service department serving all other departments within IND.

BISTD's role should be clarified within IND as regards technology provision. Measures should be put in place to ensure that technology provision is centralised including the appropriate level of resourcing and skills and that it is not possible to procure technology via other routes.

- ***Biometric Focus***. We endorse IND's decision to concentrate their efforts on the three biometrics already identified: face, fingerprint and iris. These are the most mature in the application areas relevant to IND. Concentrating effort on this small number of technologies will lead to a better understanding than if many were being considered.
- ***Policy issues.*** Policy personnel should be aware of the IND biometrics strategy and closely involved in its implementation. The overall goals must be clear so that appropriate regulations can be formed and that timely opportunities are taken for removing illogical barriers to IND operations.
- ***External communication.*** Clear assignment of IND representatives should be made for attendance of meetings and communication with the important external bodies identified (Ministers; PITO; Entitlement Card Unit; etc).
- ***Cohesive Message.*** These representatives should be thoroughly up to speed with the latest IND biometrics strategy so that a uniform message appears outside of IND and should therefore be part of or briefed by the central expert body mentioned below.
- ***Linkage with other departments.*** It is recommended that IND takes a proactive approach to remaining in touch with key UK government organisations such as PITO and UKPS so as to understand and influence their initiatives as early as possible, as well as feeding back into ongoing maintenance of IND biometrics strategy.
- ***Internal communication.*** Internal representatives of each department within IND should be identified. The use of e-communications technologies such as bulletin boards, news groups and email lists should be considered for the timely dissemination of biometrics-related information.
- ***IND systems architecture***. IND should plan for the provision of biometrics storage where this is likely to be shared. If possible, lessons should be learned from PITO's experience with the new IDENT1 multiple biometric architecture as it is rolled out.
- ***Requirements Driven.*** Within the IND biometrics framework, the choice of biometric technology should be driven by the individual application requirements. There is no single biometric technology that will best fit all applications.
- ***Background checks.*** It is recommended that, *where appropriate to the application constraints*, fingerprint is considered as the first choice of biometric. Without doing this, advantage cannot be taken of large existing databases of fingerprints such as PITO's NAFIS and the EU EURODAC. This is particularly significant in the light of the fact that most of IND applications are concerned with fraud and other criminal activities.

  It should be noted that this recommendation is in line with the IGC recommendations for a "comprehensive migration management strategy" [IGC].

  This is not to say that other biometrics should not be used where appropriate. Indeed, fingerprint might be used (at the point of enrolment)

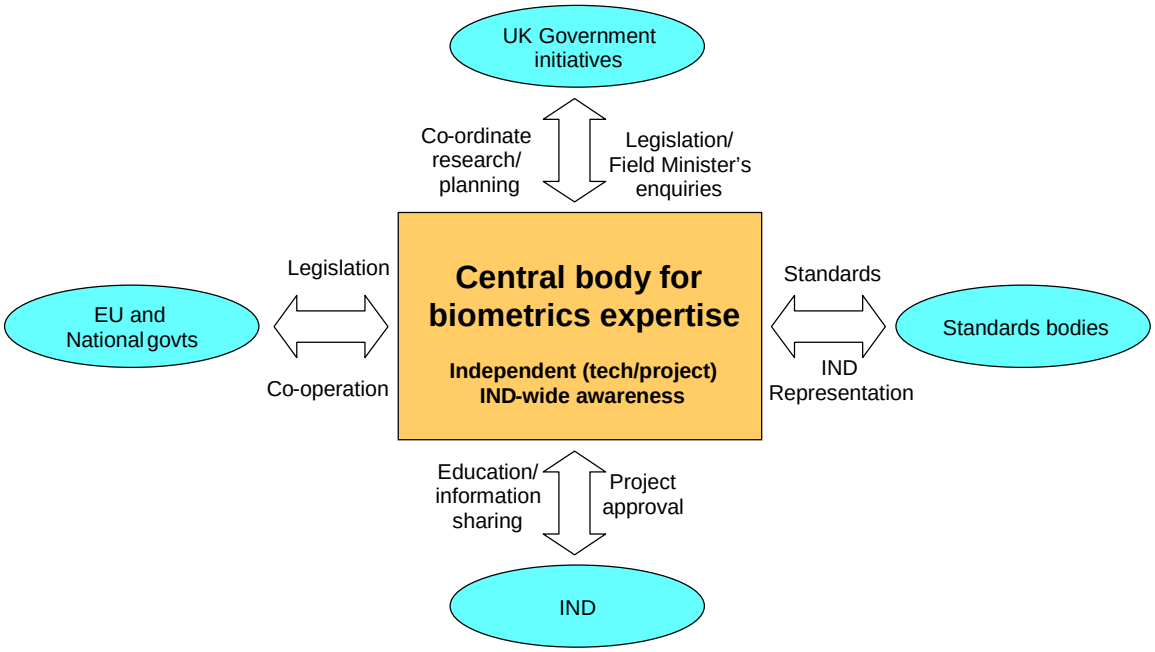
for background checking and in order to prevent multiple identities in multiple systems. Whereas some implementations might well choose to use another biometric, such as iris, after enrolment is successful for the day-to-day operation.

The nature of this constraint might change as other databases (e.g. PITO's IDENT1, UKPS and UKvisas start to collect other biometric data). For example, the possibility of passports containing biometrics from 2004/5 will be significant, though it is likely to take several years before all passport holders carry these new passports.

- ***Standards & Interoperability.*** Technical interoperability rules for IND biometrics projects should be drawn up in line with existing biometrics data standards such as CBEFF. For all new projects, consideration should be given to the storage of raw image biometric data, rather than just templates, for future-proofing purposes.
- ***Multiple biometrics***. Consideration should be given to acquiring two, or even all three, of the biometrics types at the points of enrolment. This would provide for maximal future-proofing, but the cost implication would need to be considered. The capture of more than one biometric could help address problems associated with those individuals who cannot provide certain biometrics (e.g. not having all required fingers), but would also lead to more exception cases (e.g. have to deal with those without irises too). This would also build up the databases for deploying multi-modal biometrics systems where matching is performed on more than one biometric at the same time. This can have advantages so long as manual intervention is available to arbitrate when the match results disagree. The research being carried out by PITO in Integrated Intelligent ID systems will be relevant here and IND should make every effort to work closely with PITO so as not to duplicate effort.

3.8.1.1 Central expert body

We recommend that a body of *independent* expert biometric advice should be available to IND on demand as business needs arise. This body would provide technical assurance and must be independent of bias towards any one biometric technology and must not benefit from the sale of any related products.



It might be appropriate for the central biometrics body to represent the whole of the Home Office that would then include the Prison Service and Central Home Office as well as IND. We make the following recommendation regarding the workings of a central expert body:

- The body must have the powers within IND to prevent it becoming another "talking shop". These are likely to include setting IND biometrics policy, and deciding which biometrics projects are allowed to start up.
- This same expert body should also co-ordinate communication within IND about relevant biometrics activities both inside and outside of IND. As well as biometrics expertise, group members will come to possess and provide the IND-wide view of biometrics that very few currently have and that IND departments would find difficult to provide impartially.
- Education should be part of this body's role and this should be carried out as part of the improved communications strategy. The body should conduct workshops and other educational activities as appropriate. This might include business applications of biometrics and best practice in processes such as enrolment, for example.
- In order to remain objective, this body's core membership should not be involved in the delivery of any particular project (even if they are independent, for success it will be important to be *perceived* to be independent of potential fingerprint, iris and facial 'camps').
- The body should facilitate access to biometrics expertise within IND. These experts may well be heavily entrenched in particular biometrics projects and so might not be best placed to be core members of the body.
- A representative of the body should be the first port of call for biometrics-related enquiries from external bodies (e.g. Ministers; Entitlement Card Unit; PITO; DfT.). This would ensure that a consistent message about IND biometrics strategy is heard outside of IND.
- The body should be pro-active, defining and undertaking initiatives to improve the knowledge, planning & implementation of Biometric technologies, such as undertaking (or participating in existing) bench-marking assessments of vendors and technology.

- The body should address the immediate biometrics concerns but consideration should also be given to expanding the body's role to encompass more generally e-ID technologies including PKI, cryptography, tokens (smart cards, optical cards, etc).

3.8.2 Project planning

BISTD has been in existence for only two years. We understand that there is a project initiation process in place within BISTD, but that this is currently being refined.

We suggest the following high-level **process flow** for ensuring potential projects fit with the IND biometrics strategy before they are approved:

1. Potential new project idea with a Business Case defined.
2. Identify the requirements for person identification or verification without reference to any biometric technologies
3. Characterise the application in terms of areas such as:
    - Application Identification requirement (IC/ES/WS)
    - Demographic of customer base using application
    - Degree of automation / manual supervision required
    - Speed of response required
    - Expected enrolment database size
    - Expected daily throughput
    - Proportion of users that the exception handling processes could cope with.
    - Mobility (where used)
    - Likely places and method of enrolment
    - Environmental constraints
    - Identify the need for identity record information sharing.
    - Anti-spoofing measures required (e.g. if unattended access control)
4. Provide the information collected to the independent body for rapid evaluation of whether biometrics should be used, and if so which biometric technologies are appropriate. This evaluation will include:
    - Consideration whether biometrics (or other electronic ID technologies) are appropriate.
    - Placing the project in context and evaluation of external constraints which might affect the technology choice (e.g. data sharing and standards)
    - Selection of 1:1 or 1:n matching
    - Recommendations for trialling
5. Feedback by the independent body to a project initiation team. This team should consist of IND senior management stakeholders interested in IND's use of biometrics and would ultimately ensure that new projects are in line with IND business goals.
6. Pilot or Implementation?

If any particular project goes ahead, formal requirements should be drawn up and the independent body should provide technical assurance throughout the project life as well as facilitate communications between the new project and other relevant parts of IND.

In addition, we would make the following recommendation in the area of project planning:

- ***Process Flow.*** IND should review, modify and approve the draft process flow presented above for approving new biometrics projects.
- ***Experience Exploitation.*** Draw on experience and knowledge gained from planning and implementing previous similar projects.
- ***Programme costs***. It should be remembered that the technology might represent as little as 10% of the initial investment when deploying biometrics. Other factors will dominate costs, such as training, system development, installation, network and system upgrades.
- ***Data sharing.*** In order to maximise the possibilities for data sharing, emerging standards should be adhered to in all applications (ICAO, SC37 and SC17).

3.8.3 Implementation

The detail of biometric system implementation varies considerably from application to application. During this short study we have collected a list of issues which we recommend are looked into by the co-ordinating body when considering the IND biometrics strategy and how new projects should proceed. This list is not exhaustive, but represents the key issues we have managed to capture in the time available.

We make the following recommendations regarding implementations:

- ***Database Size.*** Database size will limit the performance of biometric matching (for 1:n identification) in terms of speed and accuracy. Knowledge of other information (biographical, geographical, temporal) should be used to constrain the volume of data searched for matching.
- ***Security Architecture.*** As more Biometric data is captured, processed, stored and accessed; end-end security managing access to that data will become more critical, particular as other third party organisations are enabled for identity checking (eg exporting the borders).
- ***Tokens.*** Wherever possible, we recommend the use of 1:1 *verification* matching with the use of an associated token (card, passport, keyed number, etc) since this will provide the fastest and most accurate response. Where business need demands 1:n *identification* can be used. Countermeasures will need to be built into any systems using tokens on a case-by-case basis to mitigate the potential risks introduced by using tokens. Bear in mind that token might appear in the form of biometric passports in the next few years.
- ***Standards.*** Standards should be used wherever available since this will lead to wider supplier choice and interoperability with others. Great care should be taken when considering technology that is proprietary and is therefore highly unlikely to be adopted by standards bodies. As such standards are emerging, IND must be represented as a whole in groups such as ICAO, SC17WG3, and IST44 or SC37.
- ***Limits***. Any technology selected must be shown to have an upgrade path. No technology should be approved unless it can be shown to not be at the limit of its performance. There might be ways of removing particular perceived limits of a particular biometric system which can be identified only by independent experts (e.g. the introduction of hardware tokens to change a 1:*n* comparison into a 1:1 comparison).
- ***Processes***. Particular attention must be paid to the required processes to enable the deployment of the technology. Ensuring that the enrolment procedure is stringent enough is often difficult to do and might be multiplied many times over if there are many enrolment stations.

4 SUMMARY

4.1 Key findings

4.1.1 Co-ordination within IND

- There is some detailed experience of biometrics within IND. Most of this is concentrated within a very small number of staff within IAFP and specialises in fingerprint technology. There are other pockets of experience but not in the same detail in the areas of specification, procurement, benchmarking/evaluating, roll-out and management of live biometrics systems.
- There is no agreed clear IND-wide biometric strategy for all parts of IND to align with. This is not surprising, since this is the main reason for this study, but is worth stating.
- As technology matures, projects wishing to use biometrics are appearing more and more frequently. There appears to be no mandatory central control for approving these technology projects.
- Co-ordination of internal communications relating to biometrics would benefit from some improvement. Progress towards a common goal may be improved if the apparent technology 'camps' could co-operate more closely.
- Co-ordination of biometrics research and planning is further advanced in some other UK government organisation, in particular PITO.
- Co-ordination of external communications relating to biometrics would benefit from improvement. Mixed messages about IND's biometrics plans are being received outside of IND and IND may not be aware of significant external activities ongoing which could influence IND operations. Opportunities to share the benefits of research and to influence external initiatives at an early stage may be lost if action to improve communication co-ordination is not taken soon.

4.1.2 Compliance with the framework

- The framework is presented which puts the current IND biometrics in context and allows the consideration of other areas where biometric technology is not currently being used.
- As many already know within IND, there is no single biometric appropriate for all applications. The choice of most appropriate biometric requires analysis of the requirements and constraints of each individual application.
- There is no mechanical way of determining which biometric is most appropriate for any new application since there are so many variable factors and the technology and external influences are changing apace. We believe that new project evaluation can only be fully achieved by experts who are up to date with both biometric technologies and IND activities and aims.

4.2 Key recommendations

4.2.1 Co-ordination of biometrics within IND

- The IND high-level strategy for biometrics needs to be agreed at senior management level taking into account legislation, policy, operational aims and the technical framework presented in this document.
- IND needs to consider the relevance of all the disparate standards groups to their business and determine in which they need to be involved. Some standards will emerge by themselves, but these should be tracked by IND to determine whether and when they become relevant.
- Agree the IND-wide centre of technology provision from where expertise can be concentrated and shared. IND senior management should agree the role of BISTD as the IND central IT provider. To distribute IT provision will lead to inefficient use of resources and increased costs. The model of central IT Service provision is a sound one and has been seen to work in other organisations such as PITO.
- Establish a central body of expert advice that is available to all IND departments on demand. As a minimum, we imagine that this body will:
    - Maintain knowledge of all IND biometrics activities and relevant legislation
    - Maintain knowledge of latest biometric technological advancements and standards
    - Provide independent technical assurance
    - Evaluate new biometric project requirements and have reasonable powers to prevent inappropriate activities starting up.
    - Provide education on biometric-related issues within IND
    - Co-ordinate internal communications on biometrics-related matters
    - Co-ordinate IND representation externally so as to ensure a uniform message is presented and act as a central point of contact for incoming enquiries
    - Ensure that maximum co-operation with other UK Government agencies is established
    - Maintain and champion IND's biometrics-related goals
    - Share research with other Government agencies
    - Ensure that IND biometrics pilots capture information/develop experience that will be needed in other IND biometric applications.
    - Seek to influence biometric suppliers to provide products / prove the capabilities of their products to meet IND needs.

4.2.2 Biometric project planning

- Put in place a mandatory project initiation process that ensures that project requirements are evaluated against IND-wide goals and available biometric technology options before being allowed to progress.

In the interim period before new procedures are put in place, all parts of IND as a whole needs to decide how to act on existing plans for biometrics. In this regard, we make the following recommendations for the interim period:

- Initiate the next steps as quickly as possible to minimise this 'limbo' period.
- Projects which offer 'quick wins' to the business should be allowed to proceed so long as they can be shown to be of low risk to the business.
- Projects using technology at its limits should not proceed. Where technical areas are less well advanced, IND should be looking to research institutions to analyse the problem from first principles. E.g. understanding the ramifications of collecting biometrics from under 5s might be an example area where IND and suppliers do not have enough knowledge and information.
- Preparations should be made to capture and feedback experience gained from new projects/trials to the central body once it is established.
- For further new projects arising, ensure that, where possible, consideration is given to the need for data sharing in the future as well as now. Take into account the impact of known likely biometrics initiatives such as biometrics travel documents.
- Look outside of IND for relevant examples where off-the-shelf systems are available to suit requirements. E.g. might the Schiphol iris/token system be used without any tailoring for UKIS expedited arrivals?
- No new biometrics projects should be initiated without being brought to the attention of the PSG first.

4.2.3 Implementation

It is not possible for a study of this brevity to make detailed implementation recommendations. However, these key recommendations have been identified:

- Each of the three key Biometrics (Finger, Iris and Face) has a role to play in the business of IND.
- Wherever possible, *verification* (1:1 matching against a token) should be preferred to *identification* (1:n matching), since this will provide best accuracy and speed of response.
- Where 1:n matching is used, database sizes should be constrained by any other known factors to minimise the search domain.
- Technologies should not be used at their limits. Any technology considered for introduction must have an upgrade path.
- Use standards to maximise the possibilities for data sharing and sources of supply.

4.3 Next Steps

This study has been extremely brief and so it has not been possible to address all areas in sufficient depth.

Several areas that deserve further consideration have been identified as follows:

- Further detailed assessment of the projects identified within this report to determine key success/failure criteria and summarise lessons learned.
- Further, more detailed evaluation of the framework of biometric requirements is required to produce a road map for biometrics within IND. This is similar to work which PITO is about to undertake and perhaps experiences could be shared here. This study is estimated to take around 60-70 man-days to complete.

- Further consideration needs to be given to the implications of biometric data sharing from technical and policy angles and how this feeds into strategy.
- Further consideration needs to be given to the implications of the use or absence of tokens in biometrics systems and this fed into the overall strategy.
- Define exactly the technology initiation process and how it will be made mandatory.
- Consider the 'straw man' Terms of Reference for the central expert body provided in section 4.2.1 and flesh out the exact appropriate powers of the above central expert body and how it can be ensured that it will not be another "talking shop".
- Consider where this body should be established. This might be within IND, in which case it would be appropriate to be housed within BISTD, or perhaps could be Home Office-wide. This is a matter for IND to decide based upon their detailed understanding of government operations.
- Consider whether this body should cover only biometric technologies or all electronic ID technologies such as hardware tokens (smart cards, optical cards, etc), cryptography, PKI, etc.

Annex A

LIST OF INTERVIEWEES WITH DATES

The following personnel were identified by IND as appropriate for interview. In the limited time available it was not possible to conduct further interviews.

The names of these individuals have been removed from this report as this information is not relevant to the report.

#	Name	Role	Dept
1		IAFS Programme Manager, Assistant Director	BISTD
2		IRIS project manager; Chief Immigration Officer	UKIS BCMP
3		Immigration Officers	UKIS
4		Head of National Forgery Section	UKIS
5		e-Borders technology	UKIS BCMP
6		Chair of PSG; Director	BISTD
7		Technical assurance fingerprint	BISTD
8		Head	Public Enquiry Office
9		Security and anti-corruption unit	Finance and Services
10		Head of UK Border Control Operations	UKIS
11		e-Borders Policy; Deputy Director	UKIS
12		Study co-ordinator, Assistant Director.	BISTD
13		Enforcement Unit	UKIS
14		Assistant Director	IND Policy
15		Head Entitlement Card Unit	Policy Unit
16		Dep Dir Head of Projects	BISTD
17		Warnings Index Redevelopment Programme	BISTD
18		Asylum Screening Project Team; Assistant Director	UKIS
19		Biometrics Programme Manager	PITO
20		Deputy Head	UKvisas, FCO
21		Tech Sys Architect	UKvisas, FCO
22		External technical expert assessor	NPL
23		Terminal 5; Head of IT Development	BAA
24		Terminal 4	UKIS
25		Aviation Sector Advisor	DfT
26		UKPS/DVLA ID Programme Manager	UKPS
27		Business Manager, Vignettes project	Integrated Casework Directorate

Annex B

LIST OF BIOMETRICS PROJECTS

During this study a record of projects that were mentioned and relate to the use of biometrics was kept and is presented here for information in this Annex. It is not intended to be exhaustive. Projects are identified as being either inside IND, external to IND but within UK government, or else international.

Key to project "Type" column:
Int: international
UK: United Kingdom non-IND
IND: Immigration and Nationality Directorate

Project list	Description	Type
General biometrics including areas where no projects yet		
Entitlement card	At public consultation stage. The Home Secretary wants all lawful residents to have a card to meet the Home Office agenda of fighting ID fraud and illegal working. 1. Control illegal immigration/work permits (reduce attractiveness of UK to undesirables) 2. Reduce general ID fraud (e.g. multi bank accounts, passports, drivers licenses) 3. Simplified access to government services through single unique ID If the scheme goes ahead, all UK residents will have a card and there will be three Entitlement Card types: 1. Passport 2. Driving License 3. Other (for those with neither of the above)	UK
UK Passport	Need to ensure only one passport issued to a person. Not clear which biometric technology will be used. However, very likely that it will be Facial stored on a contactless interface IC.	UK
IDENT1	New PITO programme aims to link multiple biometrics with each person and create a citizens database. Going live September 2003.	UK
RANS	RANS: Restricted Access to NASS Support. Asylum seekers are swapping under 5s to get special family treatment. Might be useful to identify a biometric that could be used for under 5s.	IND NASS
BAA/DFT staff access control	DfT is kicking off an Access Control project and as the first stage is drawing up a single requirements specification for all their sites to comply with. Initially this will be for DfT staff only, but could then role out to passengers for baggage control over 3-5 years. Trials at airports of iris, thumbprint, hand geometry (Manchester). No benchmarks available so not possible to assess and compare these. Hand geometry looking interesting because it adapts well to changes (updates itself). Heathrow Airport Ltd are investigating the use of biometrics for cost-effective Control Authority staff physical access control (a door) to particular secure area (airside) in terminal 4. Currently using magnetic stripe swipe cards which do not prove the legitimate cardholder is present. Too expensive to have permanent security guard checking IDs. Impressed by iris demo. No commitment made to any biometric yet.	UK
Iris scan		

Project list	Description	Type
SPT	IATA trial for expedited arrivals for US frequent flyers. Informed the IND IRIS project.	UK
IRIS	IRIS: Iris Recognition Immigration System. Within e-Borders. Automated border entry for expedited arrivals of low-risk travellers. Not using a token is considered to be a considerable administrative saving. Not yet rolled out.	IND (BCO)
Schiphol Airport	Uses smart cards and matches on the computer. There is no database problem (1:1 matching against the template on the card). Used for access to Parking & Lounges as well.	Int
Afghanistan	Iris-scan database size of 12,000. Looking to expand to 400,000.	Int
United Arab Emirates	An installation at land, sea, airports and detention centres in the UAE to identify previous refusals. Uses a 1:n search against a central database, which contained over 100,000 iris codes in May 2003 and grows daily. Plans exist to extend to visa offices at a later phase.	Int
Facial recognition		
Marigold	Not specifically a biometrics project yet, but collecting facial images. Proof of concept trial of Authority to Carry system. Joint venture with some airlines and other borders agencies. Collection of passport images for watch-lists & identify people without passports – Used for operational analysis.	IND BCO
BAA facial recognition	Trial in 1999 of spotting faces in crowds coming down an escalator. Set a benchmark for future facial recognition systems.	UK
BFT/Verlaine	BFT (alias "Project Verlaine") was inherited by BCMP at the end of 2002. Planned proof of concept. BCO are looking for a facial recognition technology to ensure that a person checking in for a flight is the same one who boards. Paper boarding cards and passport checks at the gate are clearly not sufficient and large numbers of inadmissible people are being assisted to the UK as a result. This is complementary to the UK visas “flushing” project which only covers visa applicants. BCO is planning a minimalist trial at Heathrow as a small number of mobile systems which UKIS could use rather than a large number of expensive fixed installations managed by airlines (who might not wish to cooperate anyway).	IND BCO
Hornet	Trial in April 2002. Reduction of illegitimate AS applications being granted. Tried to link AS applications to arrivals with valid travel docs indicating they already have nationality in some other safe place. Imagis demonstration facial recognition system set up in Croydon at the ASU. At point of application for Asylum, photo captured with digital camera and compared against database collected at Dover.	IND BCO
National Asylum Intake Reduction (NAIR)	New project within BCO to take up on the Hornet trial to try to meet govt target of 50% reduction in Asylum intake by Sept 2003.	IND BCO
Australian passport	Special camera with five lenses makes a combined template that is associated with passport number. Australia is culturally against fingerprint.	Int

Project list	Description	Type
Airport photo barcodes	Technique being used in e.g. Gatwick and Manchester airports to ensure that the traveller is the same at both ends when walking in transit. Important where domestic and international gates are in the same building where boarding cards might be swapped. Photo captured and barcode index into database stuck on to boarding card. On arrival at the end of transit, visual inspection used to ensure same passenger.	UK
FIND	PITO Facial Images National Database proposal.	UK
Fingerprint		
IAFS	Immigration and Asylum seeker Fingerprint System	IND (BISTD)
ARC	Application Registration Card. Smart card currently only used for asylum seekers. Extension of IAFS post 9/11. Stores 2 prints allowing spot checks. Card also used without prints for benefits claims.	IND (BISTD)
EDE	EDE: EURODAC Data Exchange. EURODAC is the European Union asylum seeker fingerprint database. The Dublin Convention states that asylum seekers must apply for asylum in first EU state in which they arrive. EURODAC went live in January 2003 and is being used to speed their return to that EU state.	IND (BISTD)
UKvisas	A UKvisas project in co-operation with IAFS. Fingerprinting specific foreign national visa applications to identify “flushers” who destroy their documents in transit and then seek asylum. Matching will NOT initially be done at point of visa application, just biometric collection.	IND (BISTD) UKvisas
PIFE	Police/Immigration Fingerprint Exchange. Currently manual. Automated from September 2003. Linking IAFS to NAFIS mutual cross checks. Need results realtime. Direct access to PNC is planned. Trials with 20 Met Police stations. Getting 30-40% hits. NAFIS holds around 10% of UK adult population.	IND BISTD
REPARC	Not currently a biometrics project. All asylum seekers will report regularly. ARC will be updated with next reporting date. The cardholder has to go to specific reporting places and present the ARC whereupon the chip is read/written by a POS unit.	IND BISTD
NAFIS	Police fingerprint system. NAFIS – National Automatic Fingerprint Identification System – managed service by TRW (Northrop Grumman).	UK
Dutch EU Resident smart card	Issuing EU Residency card that contains fingerprint biometric.	Int
US Immigration and Nationality Service (INS)	US-Mexico border “laser card” stores fingerprints for frequent crossings.	Int
Various ID cards	Nigeria, Hong Kong and Malaysia fingerprinting all nationals for ID card.	Int
Hand geometry		
Various	Only for staff controls at airports and other ports of entry. E.g. UK airports for staff and San Francisco for frequent flyers.	UK Int

Annex C
ISO SC37 ACTIVITY SUMMARY

ISO/IEC JTC 1/SC37 Proposed Scope of Work

Standardisation of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification.

Excluded is the work in ISO/IEC JTC 1/SC 27 for biometric data protection techniques, biometric security testing, evaluations, and evaluations methodologies

Structure

Special Groups and Study Groups were created to undertake the initial SC37 Work Items. These Special and Study Groups are as follows.

Type of Group	Title
Special Group 1	**Harmonised Biometric Vocabulary and Definitions**
Special Group 2	**Biometric Technical Interfaces**
Special Group 3	**Biometric Data Interchange Formats**
Study Group 4	**Profiles for Biometric Applications**
Special Group 5	**Biometric Testing and Reporting**
Study Group 6	**Cross-Jurisdictional and Societal Aspects**

The terms of Reference for each group being,

1. Harmonised Biometric Vocabulary and Definitions

Terms of reference:

To ensure an agreed and common use of terms and definitions throughout all SC37 International Standards. The group should be considerate in choosing terms of the problems of translating to other languages, and should take account of the current ISO/IEC International Standards and related documentation.

The mandate of this Special Group is:

(1) Draft Terms of Reference for a Working Group on vocabulary, including scope and purpose, for circulation to SC37 National Bodies and approved Liaison Organisations for feedback in order to prepare a document for approval at the 2003 SC37 Plenary.

(2) Identify sources of terms and definitions for possible use in a SC37 Harmonized Vocabulary, (e.g those drawn from the existing standardization, as well as from sources in the field of biometrics).

(3) Hold at least one meeting during the period in between the first and 2003 Plenary Meetings of SC37.

2. Biometric Technical Interfaces

Terms of reference:

To consider the standardisation of all necessary interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems. To consider the need for a reference model for the architecture and operation of biometric systems in order to identify the standards that are needed to support multi-vendor systems and their application.

The mandate of this Special Group is:

(1) Draft Terms of Reference for a Working Group on biometric interfaces, including scope and purpose, for circulation to SC37 National Bodies and approved Liaison Organisations for feedback in order to prepare a document for approval at the 2003 SC37 Plenary.

(2) Resolve comments from the JTC1 SC37 NP and CD ballots on BioAPI and CBEFF.

Select project editors for approved projects for BioAPI and CBEFF.

(4) Forward revised CD text to SC37 Secretariat for FCD Registration and Ballot.

(5) Hold at least one meeting during the period in between the first and second Plenary Meetings of SC37.

(6) To consider the need for further work on the BioAPI.

3. Biometric Data Interchange Formats

Terms of reference:

To consider the standardisation of the content, meaning, and representation of biometric data formats which are specific to a particular biometric technology. To ensure a common look and feel for Biometric Data Structure standards, with notation and transfer formats that provide platform independence and separation of transfer syntax from content definition.

The mandate of this Special Group is:

(1) Draft Terms of Reference for a Working Group on biometric data interchange formats, including scope and purpose, for circulation to SC37 National Bodies and approved Liaison Organisations for feedback in order to prepare a document for approval at the 2003 SC37 Plenary.

(2) Resolve comments from the JTC1 SC37 NP ballots on a multi-part International Standard for biometric data interchange formats.

Select project editors for approved sub-projects for biometric data interchange formats.

(4) Develop Working Drafts for approved sub-projects for biometric data interchange formats.

(5) Provide Working Drafts for circulation to SC37 National Bodies and approved Liaison Organisations for comment.

(6) If appropriate, following NP comments, provide a document for the SC37 Secretariat for CD registration and ballot.

(7) To consider the need for further work on biometric data interchange formats.

4. Profiles for Biometric Applications

Terms of reference: To consider the need for and approach to standardisation of profiles.

The mandate of this Study Group is:

(1) Study the scope and approach for developing profiles for biometric applications within SC37.

(2) Develop and submit a report on the consensus of the group on the above to the 2003 plenary meeting of SC37.

(3) Develop NPs for submission to the 2003 plenary meeting of SC37 for ballot, as needed and appropriate.

(4) Provide a recommendation to SC 37 on the need for the establishment of a standing SC 37 Working Group for Biometric Profiles.

(5) Respond to requirements and Identify applications needing biometric capabilities and making requests to other organisations for their input and cooperation.

(6) Provide a recommendation to SC37 regarding liaison organizations.

5. Biometric Testing and Reporting

Terms of reference:

To develop draft terms of reference for a new WG on the testing of biometric systems and components, and the reporting of results of such tests in an agreed and standardised format.

The mandate of this Special Group is:

(1) Review and revise the UK BWG ‘Best Practices’ in order to agree on testing and evaluation protocols for all types of testing, including operational testing, assessment and safety considerations.

(2) Study and encourage the submission of a new NP on BioAPI conformance testing.

(3) Establish close liaison with SC27 with regard to security evaluation.

(4) Resolve comments from the JTC1 SC37 NP ballots on an International Standard for biometric testing and reporting.

(5) Select a project editor for any approved project for biometric testing and reporting.

(6) Develop Working Drafts for any approved project for biometric testing and reporting.

(7) Provide Working Drafts for circulation to SC37 National Bodies and approved Liaison Organisations for comment.

(8) If appropriate, following NP comments, provide a document for the SC37 Secretariat for CD registration and ballot.

6. Cross-Jurisdictional and Societal Aspects

Terms of reference:

To study the scope and approach with regard to cross-jurisdictional aspects in the application of ISO/IEC biometrics standards. This could include the safe operation of biometric systems, the use of technical measures such as privacy maintaining and enhancing technologies, and development of codes of practice.

The mandate of this Study Group is:

(1) Study the scope and approach for developing International Standards or Technical Reports on cross-jurisdictional and societal aspects.

(2) Develop and submit a report on the consensus of the group on the above to the 2003 plenary meeting of SC37.

(3) Develop NPs for submission to the 2003 plenary meeting of SC37 for ballot, as needed and appropriate.

(4) Provide a recommendation to SC 37 on the need for the establishment of a standing SC 37 Working Group for cross-jurisdictional and societal aspects.

(5) Provide a recommendation to SC37 regarding liaison organizations.

** END OF DOCUMENT **