PART 1: Identification Roadmap 2005 - 2020

Biometrics Technology Roadmap for Person Identification within the Police Service

© Copyright 2005 Police IT Organisation (PITO)
The copyright in this work is vested in Police IT Organisation and the information contained herein is Confidential. This work, either in whole or in part, must not be reproduced or disclosed to others or used for purposes other than that for which it is supplied, without PITO's prior written permission, or if any part hereof is furnished by virtue of a contract with a third party, as expressly authorised under that contract.

Foreword

The first PITO Identification Roadmap was produced in 2003 following a forward looking initiative included in the PITO Forward Plan 2003-8 to '*establish a corporate plan, or 'roadmap' for identification, taking full account of the Police Science and Technology Strategy'*. Its purpose was to give a view of the future of identification within the police service, based on an examination of the present position and how the situation was changing, or was expected to change over time.

The original roadmap was widely circulated and generated great interest, both from stakeholders, and internationally. It was fully aligned with key strategic drivers and by taking a long term view, it also helped to inform these strategies to ensure that they deliver best business benefit.

In order to remain relevant to the needs of the police service, such a roadmap must be regularly revised to reflect changes in technology, police requirements, business processes and strategy. This updated roadmap is the first revision of the original document, and has been produced by going back to the stakeholders, considering the impact of changes in strategic drivers such as the Police Science and Technology Strategy, the National Policing Plan and the National Intelligence Model, as well as the effects of new legislation and advances in technology.

Human identification is a key element in the reduction and investigation of crime and is thus central to the provision of effective capabilities to assist the Police Service in meeting strategic objectives. Whilst it is important to realise that a roadmap is not in itself a plan, it is a principle component of PITO's planning for the delivery of identification capabilities. It creates an effective framework within which a clear view of developments in identification technology can be maintained, and provides a mechanism for focussing on those development paths which could be influenced for the benefit of the police service.

With this view, PITO is already laying the groundwork for the future so that added benefit can be gained from future advances. Examples of this include IDENT1, the new *Strategic Identification Services Platform* which will build on the success of NAFIS, initially by adding a palm searching capability and also by expanding the geographic coverage to include Scotland, thereby delivering a truly national capability to the fingerprint bureaux of England, Scotland and Wales. Other examples include the Lantern project to deliver mobile access to IDENT1 data, and FIND, a project to provide a Facial Images National Database by 2006, enabling mugshots to be retrieved and viewed by any force.

It is important to stress that this document should not be thought of as a programme plan for the delivery of identification services. However, it can be used as a principle element in building a coherent programme of work for the future and this revised roadmap includes a number of recommendations designed to ensure that the longer term aims for identification capabilities within the police service can be achieved as quickly and efficiently as possible.

Finally, I would like to express my thanks to all of those that have contributed to the production of this updated roadmap, since it is only by regular maintenance that the content and conclusions reached can remain relevant to the needs of the police service.

Dr Fred Preston
Director Identification
PITO

CONTENTS

Section			Page
1	**MANAGEMENT SUMMARY**		**1**
	1.1	Summary of contextual changes	2
	1.2	Summary of roadmap changes	3
	1.3	Conclusions and recommendations	4
2	**INTRODUCTION**		**7**
	2.1	Background	7
	2.2	What is technology roadmapping	7
	2.3	Document Structure	8
	2.4	Acknowledgements	8
3	**IDENTIFICATION TECHNOLOGY ROADMAPS**		**9**
	3.1	Overview	9
	3.2	Roadmap Diagrams	9
	3.3	Summary	26
4	**BUSINESS CONTEXT**		**28**
	4.1	Introduction	28
	4.2	Stakeholders	28
	4.3	Wider Context	28
	4.4	Strategic Mandate	29
	4.5	Current Usage of Biometrics by the Police	32
	4.6	Current Identity Projects within PITO	32
5	**IDENTIFICATION TECHNOLOGY**		**36**
	5.1	Introduction	36
	5.2	Biometric technology	36
	5.3	Technologies considered	37
	5.4	Technology applicability overview	38
6	**EXTERNAL FACTORS**		**40**
	6.1	Introduction	40
	6.2	Research	40
	6.3	Legislation	42
	6.4	Standards	44
	6.5	Risk Areas to Monitor	44
	6.6	Softer Issues	46

7 CONCLUSIONS 48

7.1 Making best use of IDENT1 48
7.2 Video processing 48
7.3 Supporting research 48
7.4 Making best use of biometrics 49
7.5 National identification of officers 49
7.6 PITO working with partners 49

ANNEX A REFERENCE DOCUMENTS 51

ANNEX B TERMS AND ABBREVIATIONS 53

1 MANAGEMENT SUMMARY

This Identification Roadmap sets out the PITO vision for how identification technology can best be used to provide the Police Service with real operational benefit over the next 15 years to 2020. It is the first update since the original Roadmap was published in 2003 [TRM2003].

The National Policing Plan (NPP) sets the context for the work that PITO does in providing IT systems for policing for the next three years. The Police Science and Technology Strategy (PSTS) looks forward five years and adds detail of how the NPP will be implemented in the near term. This roadmap document places the current policing identification projects in context going forward fifteen years into the future. Thus, an inventory of opportunities is outlined by the roadmap that will feed back into the next generations of the NPP and the PSTS.

PITO does not have the power to achieve this vision alone. The potential future applications and the operational benefits they provide that are outlined in this document will only become reality if enthusiastically supported by the Police Service, the wider criminal justice system and central government. This identification roadmap is a tool to help encourage that enthusiasm through the communication of the 'bigger picture', and as such should be distributed as widely as possible.

Each current PITO identification project has its own milestones and targets, as well as measurable benefits that it seeks to provide, however it is important to recognise that, when placed into a strategic framework such as this roadmap and delivered through a coherent programme, the long term benefits are potentially far greater than the measurable targets by which the project is justified in the short term.

For example, in the short term:

- FIND will enable the rapid sharing of mugshots between police forces, but the provision of this basic service is the key foundation upon which any future facial recognition services will be built, both for processing intelligence photographs, or for identifying known offenders on CCTV footage. Five of the nine primary application areas for which the future vision is mapped out in this document will not be able to be achieved without the capability to be provided by FIND (see section 3.2 PAAs 1, 2, 3, 6 and 7).

- Lantern will provide the capability for fingerprint checks in the field in support of ANPR, but it is the forerunner on the roadmap of a wider vision to provide identification to police officers at the frontline through the use of mobile technology, and the lessons learned by this project will have benefits for future mobile deliver of identification services. The fundamental application areas of 'identification of individuals at point of contact' and the 'rapid identification of persistent offenders will not be able to provide the police service with maximum benefit without a mobile ID capability such as that provided by Lantern (see section 3.2 PAAs 1 and 2).

- In the short term, the IMPACT programme will provide specific inter-force intelligence functionality in response to the Bichard inquiry, but going forward it will form the basis for the PITO vision for providing superior knowledge at the point of decision – providing the right information at the right time, in the right way to the right person. The last primary application area of 'Personalisation of information to police officers' was a purely visionary roadmap in 2003, but, with

the establishment of project IMPACT it now has a tangible foundation upon which PITO can build to realise the full vision (see section 3.2.10).

1.1 Summary of contextual changes

In order to update the PITO identification roadmap document, an analysis was made of how any changes in the policing context impacted the original projections and findings. The key contextual changes since the 2003 Roadmap are highlighted below:

1.1.1 Legislation Changes

The Criminal Justice and Police Act (CJ&P) (2001) meant that after arrest DNA and fingerprints could be taken only with consent (consent was no longer required once someone was charged). Since the 2003 Roadmap, this has changed, with the introduction of the Criminal Justice Act (CJA) 2003, which enables the police to take fingerprints and DNA from a "person who is in police detention, having been arrested for a **recordable offence**" (without having to wait until they are charged).

Practically speaking, this change has not led to a dramatic increase in the volume of fingerprint sets taken, however, the numbers are starting to rise, as systems and procedures are upgraded and it is expected in the long term that the amount of identification data processed will increase (against the amount taken prior to the CJA) by around 80% by volume, e.g. from 100 000 to 180 000 fingerprint sets taken per month.

1.1.2 Policing Intelligence Initiatives

The driver for the police to focus resource more intelligently has increased significantly since 2003. The National Intelligence Model (NIM) is an accepted cornerstone of police best practice, and has ACPO minimum standards to help guide forces through the practical issues of compliance. The Bichard inquiry has led to the establishment of the IMPACT programme within PITO, looking to rapidly deliver and improve on the ability to integrate intelligence between UK forces. The ability to share biometric data between forces (starting with facial 'mugshot' images) is a key part of this.

1.1.3 Identity Management in Government

There is increasing interest in Identity Management across the globe. Other parts of UK government (concentrated in the Home Office (HO)) are now becoming more active in this area that PITO has been leading for some years. Information sharing across government departments is expected to become more and more important as we see a shift toward Identity Management over the next decade. For example, IND recently developed their Biometrics Strategy which resulted in plans for an Identity Management Framework housing an Identity Management Service serving all parts of IND and also key partners including PITO.

There are subtle differences in the requirements of each part of UK government (e.g. PITO, ICP/UKPS, IND/UKvisas) since different populations are sought to be identified (e.g. criminals; citizens; asylum seekers; etc). This is likely to mean that other government departments will build their own identification roadmaps in the near future to meet their unique application areas, and it would make sense to then align appropriate parts with the future generations of PITO's roadmap.

1.1.4 Technological advancement

Significant advances relevant to policing are occurring in biometrics technologies. On the one hand we are seeing improving matching performance, leading to more accurate and speedier outputs from biometric systems. On the other hand, biometric capture ("input devices") are also improving with the emergence of technologies such as better mobile fingerprinting devices, able to capture several fingers in one go, and contact less whole-hand scanners, showing the potential to read "rolled prints" and palms from the whole hand without touching the subject.

It is the advancement in enrolment technology that is particularly exciting, as the ability to be able to easily capture biometrics through improving enrolment technology has significant potential to provide business benefit in the custody environment alongside the existing benefits of having the biometrics for the investigative side of the Police Service.

1.2 Summary of roadmap changes

This review led to a significant restructuring of the document in order to improve its clarity and operational value. The document is now delivered in two parts:

1. The roadmap for operational use
2. Informative annexes

The review highlighted changes and progress in the field of *identification for the Police Service* in four key areas:

Identification of criminals: Application areas which concentrate on the identification of criminals have moved on largely as predicted. This was expected to be the case, as the identification of criminals is a traditional strength of the Police Service, and is core to the systems that PITO currently operate and develop, such as NAFIS, IDENT1, PNC and ViSOR.

The area where there is room for considerable improvement with regards to the identification of criminals and alleged criminals is when the wider criminal justice system is taken into account. Criminal Justice IT has been tasked with developing this area but has found it far harder to make progress than expected. They are currently striving to find a means to enable a consistent reference number to follow people through the criminal justice system, but as yet are not giving serious thought to the use of fingerprint technology.

As technology experts in this area, PITO are in a position to help and should continue to develop links with CJIT with a view to better use being made of PITO identification systems by the wider criminal justice community.

Processing of video and voice: The estimated dates for technology capable of delivering cost-effective functionality in this area have slipped significantly since the original roadmap.

The PSDB (soon to be HOSDB) work in this area is currently in difficulty due to numerous IT issues relating to the movement from analogue VHS storage to digital storage and playback within the CCTV industry. PSDB would like to work more closely with PITO in this area.

Identification of Police Staff: It has become clear during this roadmap review that providing a national capability to electronically and biometrically identify

police officers to systems is an application area with several potential follow on benefits.

For instance, the realisation of an effective national evidence and property booking and tracking system and the intelligent presentment of intelligence data to police staff appropriate to their rank, location, skill-set and access device cannot realistically be delivered with optimum benefit without a co-ordinated national means of securely identifying police staff to systems.

Identification of the general public: The ability to be able to identify members of the general public and their entitlements is also something that the police would greatly benefit from. However, unlike the other primary application areas, the development of such means of identification are not within the Police remit, rather PITO must actively engage with other agencies to ensure the policing requirement is suitably addressed. This is currently a fast moving and rapidly changing area, with significant technical change taking place with key documents such as UK passports, visas, and driving licences. There is also the potential of a UK national ID card achieving significant population coverage within the lifetime of the roadmap. At this point in time, this is still an area that requires a watching brief. Once the plans for these new forms of ID start to be delivered then further work in this area will be required.

1.3 Conclusions and recommendations

The original PITO Identification roadmap made four key findings with regards to how PITO could best focus its efforts to ensure that identification capabilities are delivered to the Police Service in a most timely manner. The review of the primary application areas has shown that all four of these findings are still valid, and has additionally highlighted two new areas where PITO have an opportunity to positively influence the development of identification services for policing.

Championing the vision for joined up identification: It is still clear that the vision of moving towards a coherent identification platform, with IDENT1 at the heart of this architecture has long term strategic benefit.

This roadmap continues to provide a focus to ensure that development effort in IDENT1 is prioritised to be inline with overall police and government strategy with regards to the addition of new technology, the improvement in information accessibility and the development of information sharing facilities across departments and borders.

Once digital mugshots are integrated into IDENT1 (via FIND) the time will be right to consider a multi-modal trial. Such a trial is likely to be extensive, and it would be prudent to include other modes of identification that are being considered for inclusion into **IDENT1** at this time (e.g. voice/iris/3D facial etc).

Over the last two years this vision has been further refined through the consideration of enriching identification data through the effective national handling of intelligence data through systems such as ViSOR, and in the longer term, IMPACT.

Video processing: Core to meeting a number of police needs is the development of more effective ways of handling the large and growing amount of Closed-Circuit Television (CCTV) evidence the Police Service deal with. Specific effort should be spent in progressing the use of this technology.

This review has highlighted the importance of PITO involvement in this area, as there are a number of IT issues that are hindering PSDB work in this area that PITO could assist in.

Supporting research: The Police Service cannot rely on the commercial sector to meet all their needs, given the largely unique identification requirements of law enforcement. PITO must continue to closely monitor research initiatives into technology that could support key policing needs, and be prepared to actively support research, both financially and with resource, as required. Such support mechanisms are already in place with regards to encouraging collaboration between PITO, Academia and commercial suppliers. These links need to be maintained and extended.

Providing a national identification strategy: It is clear from the work carried out to produce this roadmap that there is a lot more to be gained from simply using existing capabilities more effectively. The National Fingerprint Board is seeking to ensure that this is done for fingerprinting technology and similar management and best practice structures would be of benefit for wider identification functions in the future, through a 'National Identification Board'.

Making best use of biometrics will also involve relationships outside of the Police Service. The HOSDB (formally PSDB) is set to establish a Biometric Centre of Excellence during 2005 (see Annex D in Part 2). PITO should continue to maintain regular contact with this body in its new form to disseminate best practice from the Police Service to wider UK government.

National identification of officers: This is a new key recommendation. Whilst the original identification roadmap did include 3 primary application areas to which standardised officer identification was key, they were all long term goals and as such were not put forward for immediate action. With the increasing prominence and success of the National Intelligence Model (NIM), and with the establishment of the IMPACT programme in response to the Bichard inquiry the need of this capability has become more urgent.

Without a simple and secure means to identify officers electronically, it will become increasingly difficult to provide operationally acceptable user interfaces to ever more sophisticated and distributed intelligence systems. Thus if the long term vision of IMPACT is to be successfully achieved, a means of intelligently tailoring the interface to the role, rank, skills, location and access device of a member of Police staff is vital.

There are many other side benefits to the development of standardised national identity for police staff. If every police officer were to have a biometric ID card for physical and logical access control, projects need to be but in place to ensure that the potential of this card, with regard to reducing paperwork and bureaucracy elsewhere, be fully realised.

PITO working with partners: The area where there is room for considerable improvement with regards to the identification of criminals and alleged criminals is when the wider criminal justice system is taken into account. Criminal Justice IT (CJIT) has been tasked with developing this area but has found it far harder to make progress than expected. They are currently striving to find a means to enable a consistent reference number to follow people through the criminal justice system, but as yet are not giving serious thought to the use of fingerprint technology.

As technology experts in this area, PITO are in a position to help and should continue to develop links with CJIT with a view to better use being made of PITO identification systems by the wider criminal justice community.

PSDB (soon to be HOSDB) has expertise in imaging, whereas PITO is the centre of expertise for Police Service IT. As mentioned previously, PSDB would like to work more closely with PITO with a view to resolving the IT issues that are delaying development in this area. It is therefore a key recommendation of this roadmap that PITO make the formal IT support of PSDB in this area a priority.

PITO should continue to work closely with other parts of government, particularly as the Home Office develops its approach to Identity Management and government-wide frameworks and systems are likely to be developed. PITO has a lot of experience to contribute both in terms of the technologies and the procurement and operation of national identification programmes with international links. This roadmap provides PITO with a communication tool to enable engagement with key partners, with regards to identification, at a strategic level.

2 INTRODUCTION

2.1 Background

PITO's Identification Programme aims to deliver world-class automated human-identification capabilities to its customers and stakeholders. PITO is currently nearing the end of work to update its current NAFIS fingerprint identity platform to a new platform (IDENT1) with a longer-term vision. IDENT1 will provide the basis for PITO's new human identification services until at least 2013 (the end of the current IDENT1 contract term), and will be based upon an extensible architecture capable of supporting multiple biometric technologies.

In order to achieve the aim of deploying such an integrated suite of identification capabilities, PITO must develop an appropriate roadmap for development, deployment and implementation of appropriate Biometric technologies. This document is the second iteration of that roadmap.

2.2 What is technology roadmapping

The use of technology roadmaps to capture a view on the future of technology-related developments is relatively recent. Early adopters such as Motorola, Philips and major oil multinationals demonstrated the value of bringing together experts from a number of departments to collate information and knowledge held across an organisation and then display it in a simple visual way to show the linkages between research, development, products and the requirements of applications along a timeline.

Roadmaps can take various forms. The generic roadmap is a time-based chart, comprising a number of layers that typically include both commercial and technological perspectives. The roadmap enables the evolution of markets, products and technologies to be explored, together with the linkages between the various perspectives.

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

Benefits of roadmapping include:

- The business processes that have to be put in place to create the roadmap often create better communication and unification of mission understanding within organisations.
- It can clarify the rate-determining steps (e.g. research or legislation not being in place) and highlight opportunities for increased effort to reduce critical timescales.

Roadmaps cannot be purchased off the shelf. They need to be produced with the input of key stakeholders and by an empowered team. If they are to be of true value they need to be maintained within the organisation for which they are relevant and updated on a regular basis (perhaps annually).

2.3 Document Structure

This roadmap is presented as two documents. This document is Part 1 and contains the main narrative of the roadmap:

1. MANAGEMENT SUMMARY
2. INTRODUCTION
3. IDENTIFICATION TECHNOLOGY ROADMAPS
4. BUSINESS CONTEXT
5. IDENTIFICATION TECHNOLOGY
6. EXTERNAL FACTORS
7. CONCLUSIONS

A. REFERENCE DOCUMENTS

B. TERMS AND ABBREVIATIONS

Part 2 of the roadmap contains a number of Annexes referenced from Part 1 for readers wishing to explore the work performed to produce this roadmap in more detail. Annex A and Annex B are also repeated in Part 1 for reader convenience.

2.4 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.

3 IDENTIFICATION TECHNOLOGY ROADMAPS

3.1 Overview

This section presents the roadmapping diagrams and descriptions which pull together the analysis conducted in earlier sections of this document.

3.2 Roadmap Diagrams

The roadmap diagrams place relevant activities on a timeline. The timeline stretches from the recent past (2003) to 2020. In acknowledgement of the fact that there is less certainty about the long-term future than about the short-term future, we have used a logarithmic scale for the time line. This affords more space for detail about near term activities necessary to reach the end goals.

We use bold vertical lines to separate the period's short term (next 2 years), medium term (the following five years) and long term (beyond).

Separate layers are included in the diagrams for relevant:

- Police applications – using biometrics to perform a specific operational function
- Drivers – existing external influences, such as home office strategic documents that give impetus to a particular application
- Inhibitors that could delay the introduction date of applications if a particular external activity does not coincide with technical development (e.g. passing of new legislation).
- Central Police products and programmes, designed to meet identification needs, such as NAFIS or VIPER
- Technology necessary to enable products (often developed by suppliers)
- Research necessary to enable the technology

3.2.1 Overview

This version of the roadmap has been considerably restructured to be more efficient for the reader's familiar with the approach taken and in particular the analysis of Police requirements leading to the Primary and Secondary Application Areas (PAA and SAA respectively). The reader unfamiliar with this analysis can refer to Annex E.

The remainder of this section presents the roadmap charts for each PAA.

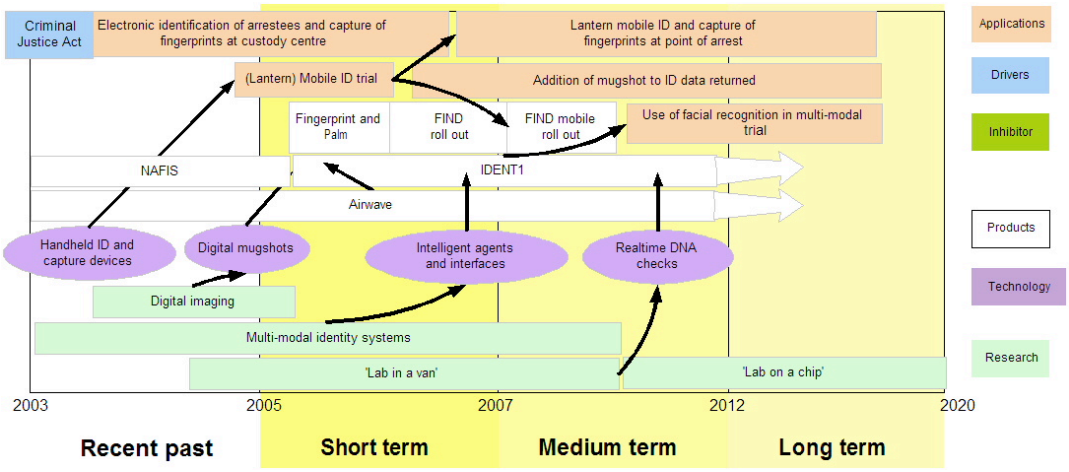
3.2.2 PAA1: Identification of individuals at point of contact

With the Criminal Justice Act 2003 enabling the Police to take biometric identification material from a person who has been arrested, rather than having to wait until they are charged, this roadmap explores the technology that needs to be in place to make this power

practically usable, and how the benefits provided to the Police Service might be better realised through the development of Biometric technology over time.

Table 3-1: PAA 1 supporting mandate

"Providing facilities, which enable officers to access information remotely, rather than returning to the police station, could significantly enhance police visibility." [PBTF]
"Identifying and eliminating threats to public safety, taking account the increased risk of terrorist activity" [PSTS2004]
"Effective management of investigations including the use of intelligent systems to assist decision making" [PSTS2004]



3.2.2.1 Electronic identification and capture of prints at custody centre on arrest

The introduction of the Criminal Justice Act means that arrestees are now fingerprinted at custody centres and their identities are checked against IDENT1. This does, however, mean officers still have to take suspects to the custody centre for booking before they can check their identity.

3.2.2.2 (Lantern) Mobile identification trial

Project Lantern has deployed a mobile fingerprinting demonstrator.

It is assumed that data services to any such mobile terminals used by the police after 2006 will be provided using **Airwave**, although other technologies are being considered. It should also be noted that, in certain cases, mobile units might contain watch list data themselves, obviating the need for a link back to the central database. This is already being done in the USA where palm pilots are storing face and fingerprint data for offline checks.

3.2.2.3 Lantern Mobile identification and capture of prints at point of arrest

The Lantern **mobile identification trial** will enable forces to choose to purchase portable terminals should they identify a need for rapid in-the-street identification within their operations. These might be carried by individual officers on the beat, or installed into patrol vehicles. Alternatively, for less pressing cases, equipment at the custody centre could still be used. Lantern proper is expected to go live in 2006.

3.2.2.4 Addition of Mugshots to ID data returned

Digital imaging technology further enhances the police ability to identify individuals. Specifically, with the planned addition of storage capability for **digital mugshots** (via FIND) circa 2006 and mobile access to FIND in 2007, identification at point of arrest services could be further enhanced through the provision of this image in response to a possible identification to enable an officer to visually confirm the identification result.

3.2.2.5 Use of facial recognition in multi-modal trial

Once **digital mugshots** are fully integrated into **IDENT1 (via FIND)**, the system will have fingerprint, palm print and facial data on a number of arrested individuals. In the mean time, considerable research effort will have gone into the efficient use of multi-modal biometric systems (Annex I), an area where, even now, clear performance advantages can be seen.

At this point, a proper investigation into the combination of the identity information held within **IDENT1** and elsewhere into a truly **multi-modal identity system** should be supported. This is likely to involve the assessment of the state of technologies such as **intelligent agents and intelligent interfaces** (see Annex I in Part 2) to provide the police with the foundation for a 'holistic' and integrated identification system.

Such a trial is likely to be extensive, and it would be prudent to include other modes of identification that are being considered for inclusion into **IDENT1** at this time (e.g. voice/iris/3D facial etc).

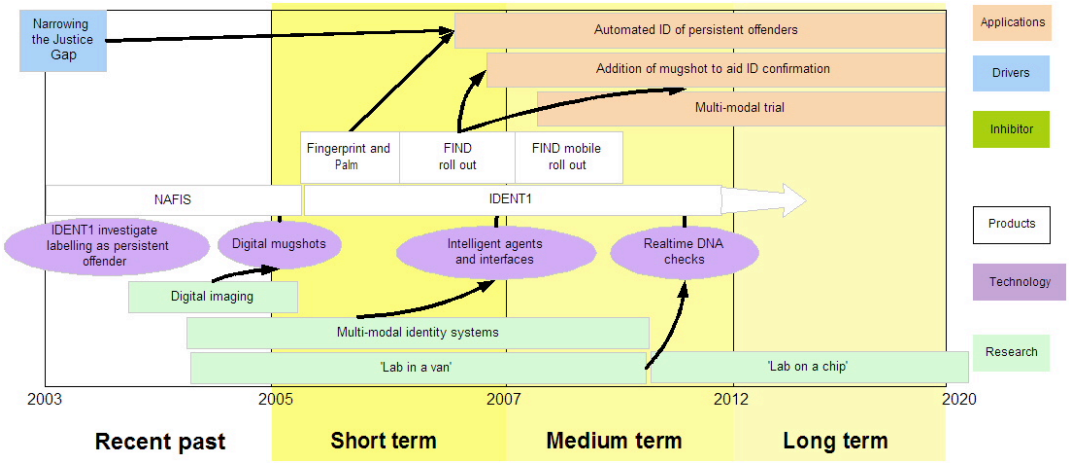
Significant police research effort is going into the use of DNA in the field through the PSDB **'lab-on-a-chip'** work, and there is a great deal of police interest in the use of DNA for identification purposes, however, technology developments to enable **real-time DNA checks** are still some way off. As a stepping stone, mobile units are expected to be available for near real-time processing of DNA samples: "Lab-in-a-van".

3.2.3 PAA2: Identification of persistent offenders

Home office research suggests that approximately 10% of offenders commit around half of all serious crime. It is a lynch pin of the plan to reduce the justice gap to target persistent offenders, and indeed this has seen the establishment of the Persistent Offenders Scheme. In order to effectively target persistent offenders, the Police Service needs to be able to identify them as such as rapidly as possible, whenever they come into contact with them.

Table 3-2: PAA2 supporting mandate

"To deliver effective custodial and community sentences to reduce reoffending and protect the public" [NPP]
"Identifying and eliminating threats to public safety, taking account the increased risk of terrorist activity" [PSTS2004]
"We now need to develop a strategy to deal more effectively with adult persistent offenders" [NJG]



3.2.3.1 Automated identification of persistent offenders

Narrowing the Justice Gap identified the need to tackle persistent offenders as key to the police strategy to increase the number of offences brought to justice and thereby reduce the justice gap. A key issue remains – the effective identification of an individual as a persistent offender in the first place.

Supporting the identification of persistent offenders through the use of biometrics is largely an information management issue. The ability to identify persistent offenders is largely a process of building on this core identification application i.e. **IDENT1**.

Once such a project has been completed, then the identification of persistent offenders will be possible through existing police identity channels (e.g. IDENT1 and fingerprint capture units). However, this application has not progressed as planned since exactly defining what a persistent offender is, has proved difficult.

3.2.3.2 Addition of mugshots to aid confirmation

With the ability to label and identify individuals as persistent offenders included in **IDENT1**, subsequent enhancements to **IDENT1** may also improve the police ability to identify persistent offenders. For instance, **digital imaging** technology could be used, via

the addition of **digital mugshots** to **IDENT1** (via FIND circa 2006), police will be able to manually confirm the identity of an individual standing in front of them against the returned photo, providing greater assurance that the identification is correct. This additional assurance is all the more important in cases where the identification is related to a specific criminal function, such as the identification of persistent offenders.

3.2.3.3 Multi-modal trial

As **IDENT1** develops further, and consideration is given to adding further modes of identification, research into **multi-modal identity systems** should be monitored to assess the benefits of combining those modes to achieve an ever more flexible and accurate identification system through the use of **intelligent agents and interfaces**.

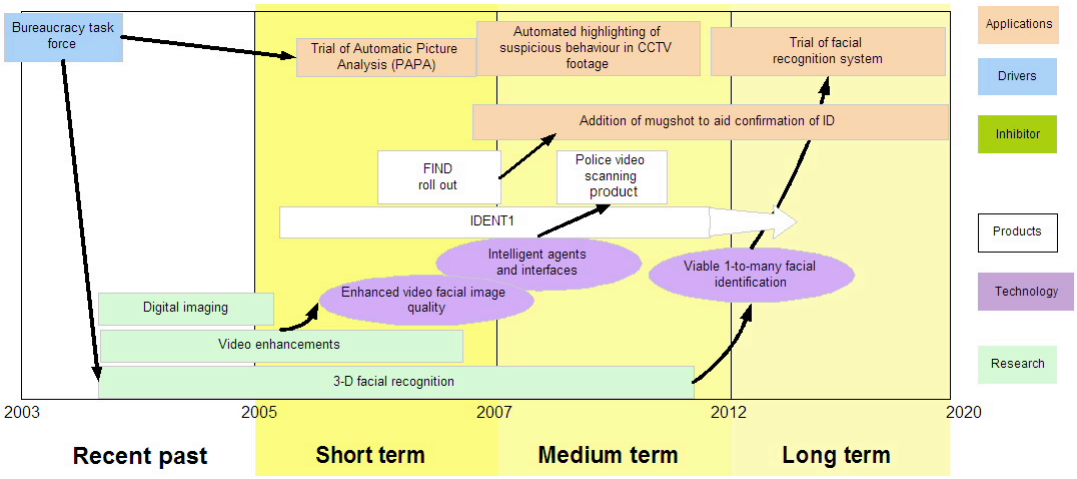
In the short to medium term, persistent offenders will be identified using fingerprints. This works well for, but is limited to, dealing with persistent offenders face to face. Development of other technologies, such as facial recognition, or **real-time DNA checks** and **lab-on-a-chip** may allow the identification of persistent offenders in other scenarios in the future.

3.2.4 PAA3: Automated and intelligent scanning of CCTV footage

When a crime is recorded on CCTV cameras, the process of actually spotting the footage of that crime and then identifying possible suspects who may have committed the crime is a manual and often extremely time-consuming process. It would be of great operational advantage to the police if this process could be automated, initially through the identification of parts of footage that contain suspicious activity, and ultimately, the identification of a list of possible subjects through the use of facial recognition.

Table 3-3: PAA3 supporting mandate

"To reduce crime and the fear of crime" [NPP] *"Effective use of intelligence-gathering technology" [PSTS2004]* *"Technology can assist in handling the product of CCTV to secure best evidence efficiently." [PBTF]*



3.2.4.1 Trial of video scanning system

The **Bureaucracy Task Force** made explicit recommendations regarding making better use of CCTV facilities. The first step to providing operational advantage to the Police Service through the automated analysis of CCTV footage is not so much about biometric identification, but more about **the development of video scanning technology to highlight suspicious or criminal behaviour**.

PSDB has been looking to begin to meet police requirements in this area through the development of the Police Automatic Picture Analysis System (PAPA). PSDB are due to accept delivery of a PAPA demonstration system in the first quarter of 2005. Currently this is limited to functionality that facilitates the organisation, synchronisation, and tagging of video footage, but it is envisaged that PAPA will provide an extensible platform that will enable the addition of more sophisticated video analysis in the future.

Whilst PSDB have been making progress in this area, the movement of the CCTV market from analogue systems based on VHS tapes to digital systems with varying proprietary means of playback and storage is presenting a large number of IT issues.

PSDB have expertise in imaging, whereas PITO is the centre of expertise for Police Service IT. PSDB would like to work more closely with PITO with a view to resolving the IT issues that are delaying development in this area. It is therefore a key recommendation of this roadmap that PITO make the formal IT support of PSDB in this area a priority.

3.2.4.2 Automated highlighting of suspicious behaviour

If initial trials of using such technology prove successful then the Police Service can use the technology to provide a **police video scanning product** to forces specifically designed to spot behavioural patterns related to criminal activity. Such a product could be improved over time as **intelligent agent** technology improves. This is taking longer than thought in the previous version of the roadmap. In order to stop this capability slipping further, the formal support by PITO of the efforts being made by PSDB in this area should be considered a priority.

3.2.4.3 Trial of facial recognition system

Longer term, such a system could be expanded to include the biometric identification of those acting suspiciously. For this to be practical, however, a number of steps need to precede:

- **3D facial recognition** technology needs to develop and mature to improve the ability to use facial recognition for identification (**development of viable 1-to-many facial recognition**).

- **Video enhancement** technology (such as research currently being done by PSDB) needs to develop to provide an **improved ability to enhance video footage to retrieve higher quality facial image** from CCTV.

- A facial images database (e.g. **FIND**) needs to be available to match the footage against it.

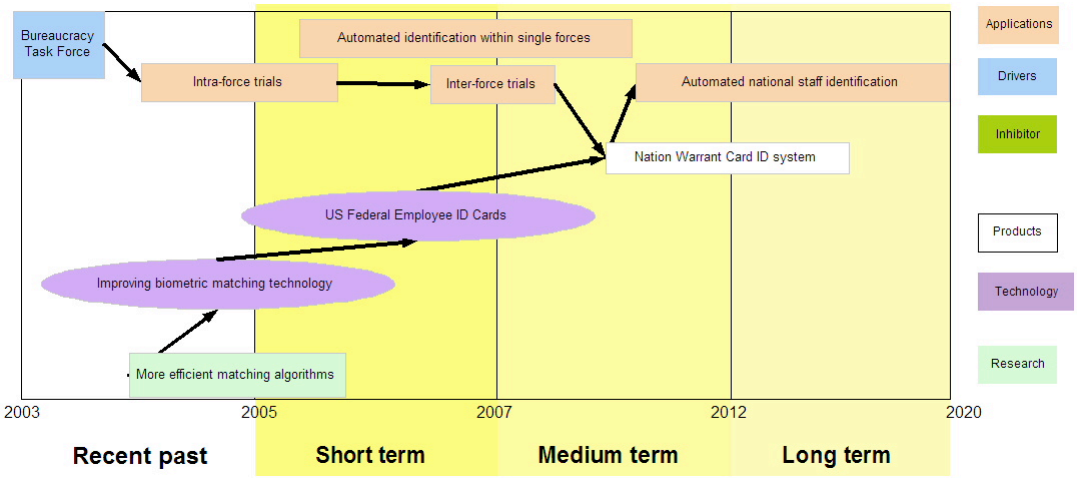
3.2.5 PAA4: Automated identification of police officers

Biometric technology could be used to automate the identification of police officers, enabling a diverse range of functions to be streamlined in day-to-day operations, including:

- Access to secure areas
- Access to IT systems
- Movement in and out of crime scenes
- Proving identity and credentials to officers in other forces
- The digital signing of transactions

Table 3-4: PAA4 supporting mandate

"Secure exchange of data between forces and other agencies" [PSTS2004] *"Further exploitation of IT will enable officers to remain on the beat, ensure that intelligence assets are used appropriately and permit greater public access to policing services through the use of e-based technologies." [PBTF]*



3.2.5.1 Trials by individual forces

The automated identification of police officers is key to enabling a number of initiatives to reduce paperwork and increase officer time available for frontline activities in line with the recommendations within the **Bureaucracy Task Force.** Individual forces are already exploring the possibility of improving their security and operational efficiency using **biometric access control** for both logical and physical access (see section 4.5 for more detail).

3.2.5.2 Automated identification within individual forces

Trials within individual forces will, and are, leading towards biometrics being used to identify officers for access to the buildings and systems of an individual force, either using:

- **1:1 matching against a template stored on a secure token** or,
- **1:N matching against a biometric database**

3.2.5.3 Inter-force trials

Whilst it does provide some operational benefit to automate the identification of officers at a single force level, that benefit is greatly increased if identification of officers is possible at a national level, when officers are dealing with forces other than their own, where surroundings and staff are unfamiliar and manual identification is a greater burden.

In order to achieve such a cross force identification system, identity compatibility needs to be facilitated between forces at a national level. One way to achieve this would be through a **cross-force identification system** including a standardised biometric to enable logical and physical access, as well as identity verification throughout the entire Police Service. This could be achieved through the national standardisation of warrant cards.

This trialling has not begun and so appears to be a lower priority than originally thought. Perhaps the work going on in the US to provide smart ID cards to all Federal employees will provide a boost to this application since standards are being set and products will shortly be available off the shelf from the major smart card system suppliers.

3.2.5.4 Automated identification across forces

Once a trial has proved the value of a **cross-force identification system**, and then the use of this system can be encouraged throughout the whole Police Service, enabling seamless access to secure areas and information systems across all participating forces, dependant on the credentials of a particular officer, and their ability to verify their identity within the system. This will enable forces to work together more easily, maintaining physical and information security without increasing the administrative overhead to manage access permissions and building passes.

The establishment of a national police warrant ID card system would seem desirable, allowing all forces to be joined up and recognise each other's staff. There is no technical reason why this could not be developed within the next year or so, in the light of whatever comes out of the US Federal employee ID card initiative.

The applications for police identity are numerous, and maximum benefit from any such scheme would only be obtained if advantage were taken of this potential for usage beyond simply physical and logical access control, e.g.:

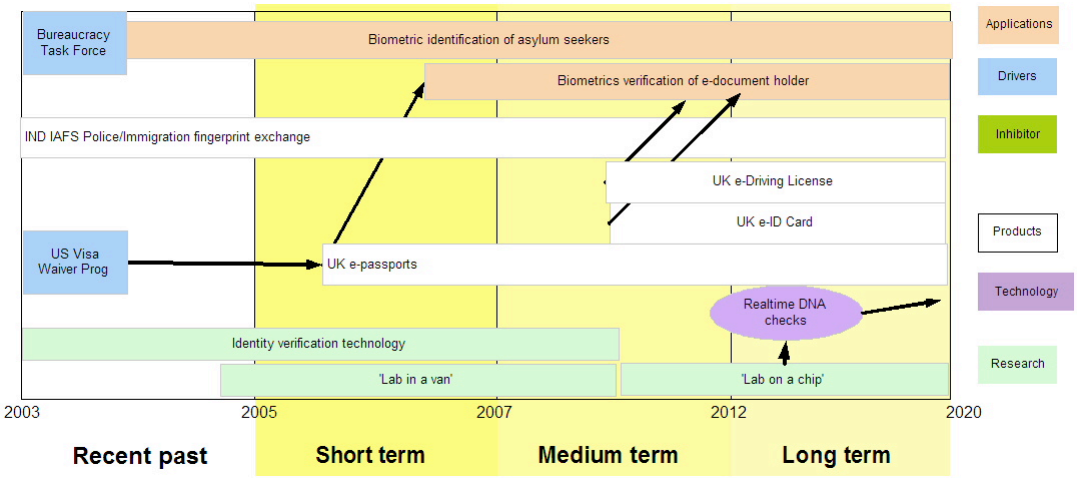
- Gun control
- Automating car log books
- Maintaining chain of evidence (see section 3.2.9.1)
- Protecting valuable kit from mis-use (e.g. police cars, airwave radios)

3.2.6 PAA5: Proof of public entitlements

One area of identification that is of particular interest to the police force is the ability to identify those without criminal records. Recent developments in the area of legitimate entitlements and licences, such as passports and driving licences, mean that biometrics are likely to be key to enabling the police to move forward in this application area in the near future.

Table 3-5: PAA5 supporting mandate

"To regulate entry to and settlement in the United Kingdom effectively in the interests of sustainable growth and social inclusion" [NPP] *"A citizen entitlement 'smart card' will assist in dealing with the growing problem of identity fraud and reduce the inconvenience caused to members of the public in confirming their identity. Its introduction could eliminate procedures associated with the production of driving documents" [PBTF]* *"Further exploitation of IT will enable officers to remain on the beat, ensure that intelligence assets are used appropriately and permit greater public access to policing services through the use of e-based technologies." [PBTF]*



3.2.6.1 Biometric identification of asylum seekers

The police are already able to identify whether someone is registered as a legitimate asylum seeker through the joint **PIFE** project with IND (see Annex D in Part 2). This enables fingerprints taken using Livescan to be compared to the IND's IAFS fingerprint database.

3.2.6.2 Biometric identification of entitlement holder

The Police **Bureaucracy Task Force** highlighted the value that some sort of identity card would provide to operational policing. The ability of the police to be able to identify members of the public using biometrics largely depends on the development of biometric identification schemes, and the police gaining **legal access to identity** data gathered as a part of these schemes.

Since the initial roadmap, much work has taken place in this area. E-passports will be issued in the UK from October 2005.

DVLA has plans to issue a smart driving licence as soon as possible, despite no longer being part of the ID Card "family of cards" proposed earlier. It is not yet clear when this will be, because it depends upon draft EU Regulations that have not yet been passed. It is thought that issuance of biometric driving licences might begin in 2006, certainly before the UK ID Card are issued.

The ID Card Programme is likely to go ahead once the ID Card Bill is passed into law. This might be April 2005, or delayed until after the next general election.

Even if an ID card is not issued to all UK citizens in the medium term, the addition of biometrics to Passports, and driving licences, will still provide the police with a much greater potential to verify the identity of individuals faster, and with greater assurance, than they can currently.

When such schemes are in place and the police have established legal access to the identity information, then a trial to enable the police to access that information and perform successful identifications should be established to test the technology before attempting national rollout.

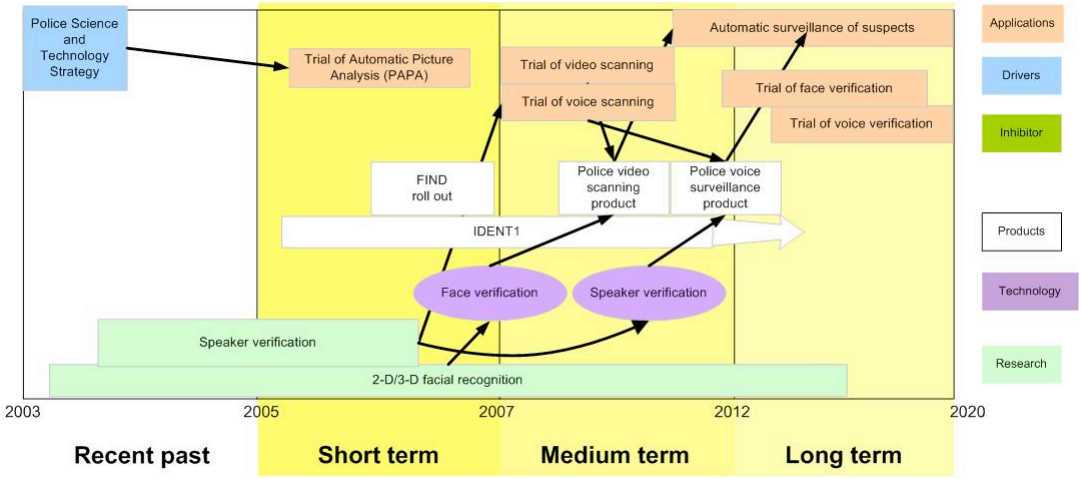
The potential for DNA to be used to identify the public in the future cannot be ruled out, but is unlikely to be technically possible for **real time DNA** identification within the lifetime of this roadmap, and would also raise legitimate public acceptability and ethical concerns (see section 6.6).

3.2.7 PAA6: Surveillance of suspects

The police can save time and money through the use of biometric technology to improve the efficiency of the surveillance process.

Table 3-6: PAA6 supporting mandate

"to combat terrorism and other threats to national security" [NPP]
"Undertaking effective surveillance" [PSTS2004]
"Technology can assist in handling the product of CCTV to secure best evidence efficiently." [PBTF]



3.2.7.1 Trial of video scanning system

The **Police Science and Technology Strategy** states that the police should be using technology to ensure that they undertake effective surveillance. The estimated dates for these trials have slipped back significantly from the original roadmap.

More effective surveillance can be tackled initially through the use of **intelligent agent** technology to assist officers undertaking surveillance by **highlighting human activity** and hence increase officer alertness at appropriate moments, using similar technology to that used to spot suspicious behaviour as detailed in section 3.2.4.1. Whilst this is not using biometrics, it is starting to provide a surveillance infrastructure into which biometric identification can be added in the future.

3.2.7.2 Trial of voice scanning system

Voice surveillance (e.g. phone line monitoring) could similarly be improved though the use of **word recognition** technology to perform automated scanning of speech to look for and highlight key words and phrases for officer attention. Again, whilst this is not using biometrics, it is starting to provide a surveillance infrastructure into which biometric identification can be added in the future. The estimated dates for advances in this area have slipped back significantly from the original roadmap.

3.2.7.3 Automated surveillance of suspects

The results of the video and voice scanning trials should be used (if the trials prove successful) as input into **police voice** and **video surveillance products**. Initially these products will use behaviour and word recognition technology rather than biometric identification technology, but the biometric verification of the suspects under surveillance can be added as and when supporting technology (e.g. **video enhancement**) sufficiently matures.

Since the trials have not begun, it is likely that this application will not be realised for several years to come. The estimate in the original roadmap of 2005 for this application being delivered was clearly over-optimistic.

As mentioned previously in section 3.2.4.1, PSDB are active in the area of video processing and are close to the acceptance of a demonstrator system for automatic picture analysis (PAPA). If this are is not be stall further, it is vital that PITO look to work more closely with PSDB in this area to support their work, particularly with a view to providing the IT expertise that PSDB do not necessarily have.

The ACPO Video evidence and analysis group should be approach with a view to endorsing PITO /PSDB co-operation in this area.

3.2.7.4 Facial verification trial

It is likely that **facial verification** of suspects under surveillance will be ready to integrate before voice, as **2-D and 3-D facial recognition** is further advanced, and the prospect of viable 3-D facial recognition in the next 3-5 years gives further cause for optimism as to the viability of this technology in a surveillance scenario in the longer term. The practicalities of this will be better understood once the FRVT Facial Recognition Grand Challenge results are known in late 2005 (see Annex I in Part 2). Also, **facial recognition** evidence is better understood in the UK legal system than voice, and court guidelines for what is deemed to be 'good' and 'bad' facial evidence already exist.

This will enable the automated surveillance of particular individuals as they traverse a particular environment (e.g. a shopping centre), even if they move from camera to camera, thus drastically cutting the manual officer intervention required in this important police activity.

3.2.7.5 Speaker verification trial

Speaker verification is a more problematic due to the behavioural element in the way we speak (i.e. we can change pitch, it is affected when we have a cold) and the relative ease with which a voice can be disguised using technology over a telephone if someone is aware / suspicious that they are being listened to. Whilst voice may provide some assurance as to whether the right individual is being monitored, the possibility of using such a tool as legal evidence is still some way off.

3.2.8 PAA7: Tracking persons through the criminal justice system

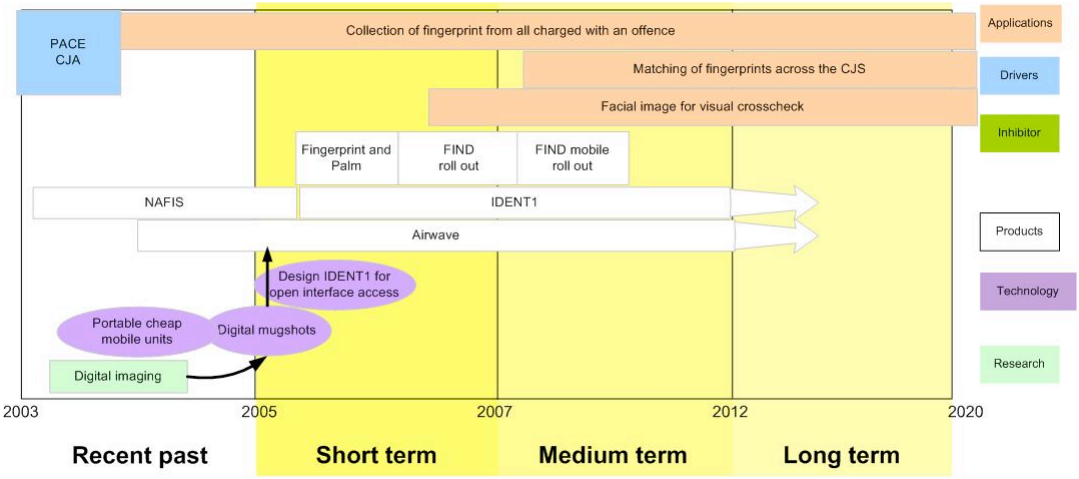
Tracking a suspect as they move through the criminal justice system is an area where biometrics can provide significant benefits by:

- Ensuring the person who turns up at court is the person charged

- Ensuring that the person who goes to prison is the same person who was arrested
- Ensuring that the right individual is released from prison at the end of sentence
- Ensuring the correct person reports for community service / parole / bail reporting
- Enabling third party security staff to validate that they are transporting the correct individual.

Table 3-7: PAA7 supporting mandate

"To ensure the effective delivery of justice" [NPP] *"Secure exchange of data between forces and other agencies" [PSTS2004]* *"Dedicated prisoner handling teams, enabled by IT applications, working closely with the CPS and supported by joint criminal justice units, will increase the quality of prosecution case files through a much more efficient process." [PBTF]*



3.2.8.1 Collection of fingerprints from all people charged with an offence

Since the introduction of **PACE**, the police have been able to take fingerprints at point of charge and retain that information until a person is acquitted. Thus, whilst an individual is in the criminal justice system from point of charge to end of sentence or acquittal, the Police Service has fingerprint data, currently held within **IDENT1** to enable biometric identification.

3.2.8.2 Matching of fingerprints throughout the criminal justice system

Since the police are able to gather fingerprint data from all peoples being processed by the criminal justice system, there are significant gains to be had for all parties within that system simply by seeking to make best use of that data. To identify every point where identification could add benefit requires a detailed analysis, but the following list contains some obvious examples:

- The **Criminal Justice Act** 2003 contained new clauses to enable the collection of fingerprint data "after a person has been arrested". This potentially enables the

police to verify that when a person is later charged, they are indeed the same person who was arrested for that offence.

- When an individual turns up for a court appearance, court access to mobile identification would help prevent substitutions.

- Similarly, portable identification terminals could be used to ensure that parties transported to and from court by security personnel are who they claim to be.

- Mobile identification could be used by parole officers and community service supervisors to prevent substitution.

- Identification upon prison entry could be done to ensure the person locked up is the person originally charged with the offence.

- Identification upon prison exit would help ensure that the correct individual was released.

- Assumable identification will permit the accurate tying of personal data, such as antecedent history, to a particular individual.

Thus, the **development of the means to enable access to IDENT1 by CJS partners** is required, and dissemination of the service throughout the CJS will be assisted by vendors undergoing **equipment development** to provide **more portable and cheaper mobile identification units** that can subsequently be integrated with **IDENT1** and **Airwave** to provide mobile identification facilities throughout the CJS.

It was hoped that there would be progress in this area by 2005. There seems to have been very little since fingerprints are still not routinely and uniformly used in many parts of the CJS (e.g. prisons; courts). We have therefore pushed this application out to 2007/8 and recommend that efforts are made to improve co-operation in this area between PITO (IDENT1) and the rest of the CJS, and formal discussions are held with CJIT regarding the potential re-use of PITO systems by the wider CJS community specifically for this purpose.

3.2.8.3 Facial image for manual cross check

This police function is largely in a controlled environment, therefore the value of multi-modal identification is limited, and the use of fingerprint technology is probably sufficient for the function within the lifetime of this roadmap. There is no point adding additional expense for minimal gain. However, **digital imaging** may be of benefit, and as **digital mugshots** are intended to be included within the **IDENT1** platform anyway, separate of any criminal justice identification initiative, there is value to enabling this facial image to be provided for wider criminal justice use. Any court officer or member of security staff transporting prisoners will have a greater feeling of assurance if provided with a photo to enable them to manually cross check the result of a fingerprint identity check.

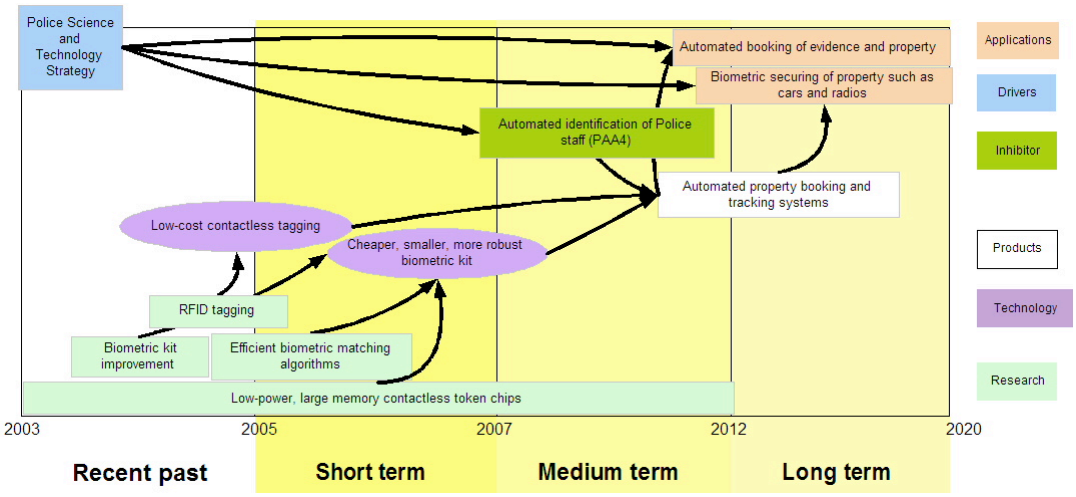
3.2.9 PAA8: Booking of property and evidence

There are a number of areas where the ability to be able to track what an officer did with pieces of property and evidence is of great importance. In particular the greater the integrity of an auditable record regarding the way a particular piece of evidence was handled, the better protected the police are against accusations of mishandling of evidence in court.

Also, this is an area where the use of biometrics can see a dramatic reduction in paperwork and administration overheads (e.g. automating car log books).

Table 3-8: PAA8 supporting mandate

"To ensure the effective delivery of justice" [NPP]
"Effective location and recovery of evidence" [PSTS2004]
"Protection of officers and vulnerable individuals" [PSTS2004]



3.2.9.1 Automated booking of evidence and property

The **Police Science and Technology Strategy** calls for the effective location and recovery of evidence, as well as the protection of police officers from false accusations. A good audit trail of property and evidence is key to fulfilling such a need.

The key enabler to the automated booking of property and evidence is the meeting of another requirement – that of the **automated identification of police officers**, as discussed in section 4.5. Once an officer can be identified automatically, that identity can be used to book in and out property and evidence automatically.

As can be seen from section 4.5, initiatives taken to biometrically identify officers within individual forces will be the first means available to the Police Service to provide **automated booking and tracking systems** (e.g. replace paper based car log books), possibly utilising technology such as **RFID tagging**. However, future national standardisation of officer identification would benefit this booking function further, as it would enable booking systems to work cross-forces and also remove any confusion as to whether the integrity of the audit trail provided by one force was better than another, particularly important when seeking to prove the 'chain of evidence' in court.

3.2.9.2 Biometric security protecting equipment such as cars and radios

Biometric equipment development will, over time enable the cost effective addition of biometric security to police property, such as cars, radios and guns as **cheaper, smaller and more hardwearing equipment** becomes available and suitable for such use. This will enable the use of biometrics to protect items such as radios and cars, for instance, a passer-by will not be able to jump into a police car and drive off, or steal a police radio and listen in, as such actions would require the biometric identification of an officer to the device before it will function.

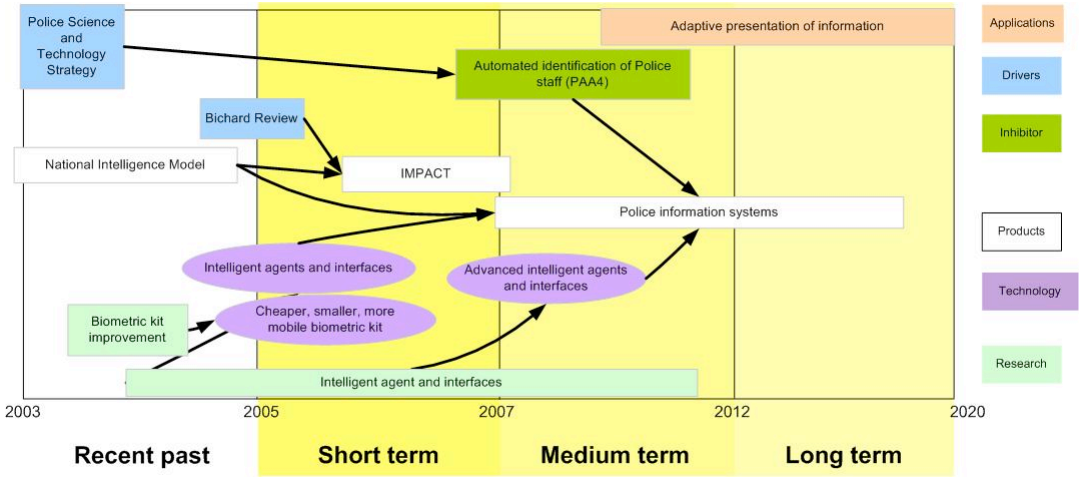
In the long term, **development in contactless cards to enable the use of biometrics alongside low cost RFID tags** may further enhance property tracking services, combining biometric security with low cost tagging, enabling the cost effective biometric protection of lower cost police property, not just cars, guns and radios.

3.2.10 PAA9: Personalisation of information to police officers

The ability to provide targeting information to officers, suitable to their current role, rank and location would provide a considerable time saving to staff, particularly if this information was available in the field.

Table 3-9: PAA9 supporting mandate

"Effective management of investigations including the use of intelligent systems to assist decision making" [PSTS2004]
"Further exploitation of IT will enable officers to remain on the beat, ensure that intelligence assets are used appropriately and permit greater public access to policing services through the use of e-based technologies" [PBTF]



3.2.10.1 Personalisation of information provided to officers

The **Police Science and Technology Strategy** stresses the need to make best use of IT, ensuring that it is used to best advantage in any given context.

In addition, since the original roadmap was produced, the driver for the police to focus resource more intelligently has increased significantly. The **National Intelligence Model** is an accepted cornerstone of police best practice, and has minimum standards to help guide forces through the practical issues of compliance. The **Bichard** inquiry has led to the establishment of the **IMPACT** programme within PITO, looking to rapidly deliver and improve on the ability to integrate intelligence between UK forces.

As intelligence processes and systems become more and more sophisticated, the need to provide an interface that is able to guide officers to the functionality that they require at any given time will become a requirement of paramount importance. No matter how good the back end integration of intelligence systems are, the operational benefit of this integration will be severely limited if the interface is so complex as to make the systems virtually unusable. The key to being able to simplify complex interfaces is the ability to

personalise the presentation of data to the role, location, skills, and access devices of individual users.

As with the previous key application area, the ability to be able to personalise the information presented to officers hinges on the prior ability to be able to meet the requirement to **automatically identify officers**. Whilst this is possible via username and password, this roadmap assumes that the Police Service would seek to take advantage of and reuse police biometric access control systems in order to benefit from the additional security and reduced day-to-day administration costs.

The key research and development role here is not to do with biometrics as such, but the effective use of **intelligent agent and interface technology** (see Annex I in Part 2) within **police information systems** (e.g. the PNC, IMPACT). As new methods of identifying police staff with biometrics are developed (e.g. individual force initiatives, or a cross force identification scheme) these will need to be integrated with **police information systems** in order to provide the identity of the individual to the system when the system is accessed. It is the role of the **intelligent agent** to take that identity and other appropriate parameters such as the type of access device, the location of the officer, the officer's rank, the case they are currently working on, etc. and combine this data to present information in the most helpful and accessible fashion.

Biometric access from mobile devices will further add to the convenience and time saved by such a system.

3.3 Summary

This section summarises the progress and changes in the primary application areas since the production of the original roadmap in 2003 [TRM2003].

3.3.1 Identification of criminals

The roadmaps for the identification of persons at point of contact, and for the identification of persistent offenders[1] have moved on largely as planned (PAA1 and PAA2). This was expected to be the case, as the identification of criminals is a traditional strength of the Police Service, and is core to the systems that PITO currently operate and develop, such as NAFIS, IDENT1 and PNC.

The area where there is some cause for concern with regards to the identification of criminals and alleged criminals is when the wider criminal justice system is taken into account (PAA7).

Criminal Justice IT has been tasked with improving this area but has found it far harder to make progress than expected. They are currently still struggling to find a means to enable a consistent reference number to follow people through the criminal justice system, and as such are not giving serious thought to the use of fingerprint technology at this time.

PITO should continue to develop links with CJIT with a view to better use being made of PITO identification systems by the wider criminal justice community. There has been some issue with the technical definition of a persistent offender on PNC that has caused development in this area to be stall but the rest of the technology is in place to move ahead rapidly once this is overcome.

3.3.2 Processing of video and voice

PAA3 and PAA6 are both application areas that hinge around the effective processing of video or audio inputs.

The estimated dates of delivery for these application areas have moved significantly since the original roadmap.

PITO is not currently putting significant resource into these areas, however, there is work taking place on video processing in PSDB. PSDB have imaging expertise, but they look to PITO for guidance as to how best to tackle more mainstream IT issues.

The PSDB work in this area is currently in difficulty due to numerous IT issues relating to the movement from analogue VHS storage to digital storage and playback within the CCTV industry. PSDB would appreciate PITO's help in this area.

It is recommended that PITO give assistance to PSDB in the area of CCTV processing to ensure that this application area can be realised in the foreseeable future.

3.3.3 Identification of Police Staff

It has become clear during this roadmap review that providing a national capability to electronically and biometrically identify police officers to systems (PAA4) is an application area with several potential benefits.

For instance, the realisation of an effective national evidence and property booking and tracking system (PAA8) and the personalised presentment of intelligence data to police staff (appropriate to their rank, location, skill-set and access device) (PAA9) cannot realistically be delivered with optimum benefit without a co-ordinated national means of securely identifying police staff to systems.

It is recommended that PITO consider establishing a programme to standardise and deliver a national means of securely identifying police staff. This means can then be used as a building block across all systems to enable better security and the effective delivery of user-friendly interfaces to complex systems.

This is particularly relevant to PAA9. The realisation of the long term vision of IMPACT will require an effective means of officer identification on a national scale.

3.3.4 Identification of the general public

The ability to be able to identify members of the general public and their entitlements (PAA5) is also something that the police require, however, unlike the other primary application areas, the development of such means of identification are not within the Police remit, rather PITO must respond to make use of suitable identification as and when it arises.

This is currently an extremely volatile area, with significant technical change taking place within UK passports, UK Visas, and UK driving licences. There is also the potential of a national ID card achieving significant population coverage within the timescale of this roadmap. At this point in time, this is still an area that requires a watching brief. Once these new forms of ID start to be delivered then further work in this area will be required for police applications to make best use of them. PITO is already engaged closely with the ICP, IND and UKPS, etc, through the Home Office forums for biometrics.

4 BUSINESS CONTEXT

4.1 Introduction

This section details the business drivers behind the production of this roadmap by exploring:

- The stakeholders who have an interest in biometric identification within the Police Service
- The wider context:
  - The impact biometric identification usage within the Police Service will have outside of the Police Service.
  - The impact biometric identification applications outside of the Police Service will have on its use inside the Police Service.
- The strategic mandate for the roadmap - how does biometric identification help the Police Service and the home office meet current objectives?
- The starting point - what current uses of biometrics are there within the Police Service and how can they be built upon?

4.2 Stakeholders

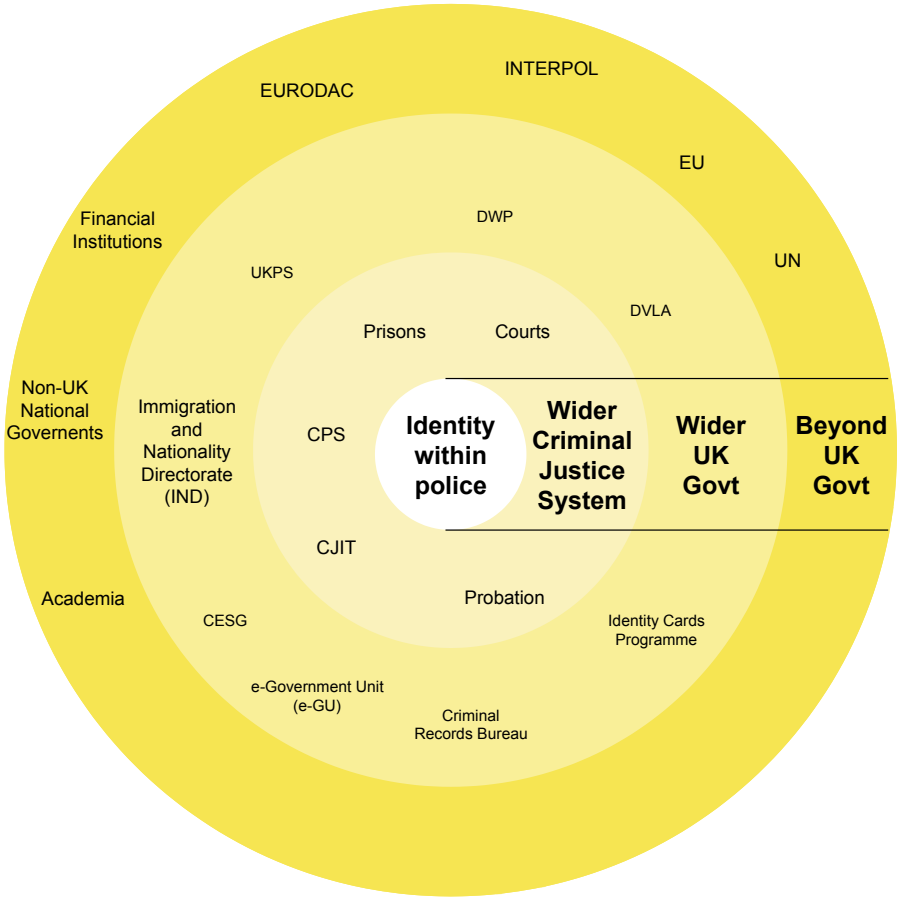
Many bodies are involved in supplying the science, technology and information systems used by the Police Service. The key stakeholders are described in this section. Those bodies in the wider context are introduced in section 4.3.

The main bodies representing the policing at a national level in England and Wales are the Association of Police Authorities (APA), the Home Office (HO) and the Association of Chief Police Officers (ACPO). In Scotland, the key bodies involved along with the Home Office are the Association of Chief Police Officers Scotland (ACPOS) and Convention of Scottish Local Authorities (CoSLA). These are described in Annex M.

4.3 Wider Context

This section paints the wider picture outside of "Identity within police" (PITO and the direct stakeholders). Figure 4-1 shows a context diagram for this study. The biometric activities of these organisations are detailed in Annex D.

Figure 4-1: Wider context of this study



4.4 Strategic Mandate

This section provides a brief description of the strategic documents relating to the operation of the Police service that form the bedrock of the requirements for biometric identification explored in this roadmap.

It is these documents that provide the focus for the development of the identification capability requirements and application areas discussed elsewhere in this document (see section Annex F). If it were not possible to identify the benefit of a particular application or the need for a particular requirement based on the strategic mandate then the legitimacy of that requirement or application would have to be seriously questioned.

At the same time, this roadmap document necessarily informs future versions of mandate documents since it has a longer-term vision. Also, since the roadmap does not represent a plan of what will be done, it is able to push boundaries and present an inventory of possibilities, only some of which will be selected for implementation within available budgets.

4.4.1 National Policing Plan (NPP)

The National Policing Plan [NPP] is a three-year rolling strategy document designed to provide a single point of definition for the Government's priorities for the Police service, performance indicators by which that service is assessed and new developments planned to enable priorities to be met. The priorities of the current NPP (2004-2007) are to:

- Provide a citizen focused service to the public, especially victims and witnesses, which responds to the needs of individuals and communities and inspires confidence in the police particularly amongst ethnic minority communities.
- Tackling anti-social behaviour and disorder.
- Reducing burglary, vehicle crime, robbery and drug-related crime in line with the Government's Public Service Agreement targets.
- Combating serious and organised crime, both across and within force boundaries.
- Narrowing the justice gap by increasing the number of offenders brought to justice.

A number of actions are set out within the NPP describing how these national priorities can be delivered at a local level.

The NPP also includes the presentation of a "Planning Framework", designed to assist Chief Officers in the definition of local plans by identifying the criteria by which such plans will be assessed in terms of raising Police performance within the priority areas of the NPP.

The NPP is updated on a yearly basis.

4.4.2 Police Science and Technology Strategy (PSTS)

One means of delivering the priorities outlined in the NPP is through the effective use of IT. The PSTS [PSTS2004], referred to within the NPP, is a five-year strategy (currently 2004-2009) aimed at providing a framework to guide the planning and delivery of valuable science and technology services to frontline policing. PITO, along with the Forensic Science Service (FSS), the Police Scientific Development Branch (PSDB), and the IT divisions within the nation's individual Police Forces are expected to use the PSTS as a guide for their deployment and development plans for 2003/04 and beyond.

Thus, PSTS, as the framework for the delivery of the objectives of the NPP through the appropriate use of technology, is the key strategic document for shaping the direction of the PITO identification roadmap.

The purpose of the PSTS is defined as:

> *'to ensure the Police Service is equipped to exploit the opportunities in science and technology to deliver effective policing as part of a modern and respected criminal justice system.'*

In order to achieve this purpose, the PSTS aims to:

- Establish priorities for current and future science and technology applications and research
- Co-ordinate the development and implementation of technology between users and suppliers to ensure a coherent and effective process
- Implement processes for future scanning to ensure that the Police Service can exploit new technology at the earliest opportunity and is prepared for new technology based threats.

In order to help ensure that these aims can be met, the Police Science and Technology Strategy Group (PSTSG) has been established to monitor the development and implementation of the PSTS and update it on a yearly basis.

The PSTS outlines:

- Policing priorities and the systems required to support them
- Policing capabilities, current and future
- Science and Technology requirements needed to provide the capabilities
- A Framework for delivery
- Future Scanning

The current issue of PSTS (2004-2009) identifies ten primary policing capabilities, listed in priority order that should be the focus of current and future science and technology deliveries for operational policing at this time. These capabilities are:

1. Identifying and eliminating threats to public safety, taking account of the increased risk of terrorist activity.
2. Effective use of intelligence-gathering technology.
3. Secure exchange of data between forces and other agencies.
4. Mobile data input and retrieval.
5. Maximising the value of evidence.
6. Effective management of investigations including the use of intelligent systems to assist decision making.
7. Monitoring offenders that pose a threat.
8. Undertaking effective surveillance.
9. Effective location and recovery of evidence.
10. Protection of officers and vulnerable individuals.

These capabilities are cross-referenced against the primary application areas of this identification roadmap in Section 3.

4.4.3 Other relevant documents

This roadmap is focussed on the delivery of identification capabilities to the Police Service through the appropriate usage of technology, and therefore it must be developed with the framework for technology delivery outlined within the PSTS.

The PSTS is inextricably linked to the NPP, as it is the practical development of how NPP objectives should be delivered through the appropriate use of science and technology.

Therefore, the NPP and the PSTS are the main drivers for this roadmap. There are however, a number of other documents of relevance that are worth considering when assessing the potential benefits to be delivered through the development and use identification technology. These additional documents are referenced to specific application areas in section 6.1 in order to increase the weight of evidence for the value of the development of these long term policing capabilities.

The other strategic documents considered in this report are:

- The National Intelligence Model
- The Bichard Inquiry
- The Bureaucracy Task Force

- Narrowing the Justice Gap
- Forensic Integration Strategy

A Brief summary of the content of these documents can be found in Annex C.

4.5 Current Usage of Biometrics by the Police

Broadly speaking, biometric technology is used within parts of the UK Police Service for the following person identification/verification requirements:

- Linking people to criminal records
- Proving presence at crime scenes
- Physical access control
- Logical access control
- Casualty bureau (e.g. tsunami type work)
- Surveillance
- Anti-terrorism intelligence

Collecting latent fingerprints at the crime scene and use of NAFIS/IDENT1 to identify criminals are the obvious examples. Other examples include:

- Surveillance: Newham Council, in partnership with the Metropolitan Police are using 256 CCTV cameras to help reduce offences in a traditionally high crime area of London. Facial images acquired are compared to watch-lists of local criminals convicted of street crimes (including robbery), and youth offenders who have been placed under curfew. Similar systems are now being used by Harrow Borough council, Greater Manchester Police, West Midlands Police and the MOD Police.
- Logical access: 27 UK forces are now using fingerprint scanning for data system logon to fixed force network terminals.
- A number of forces and national police organisations have adopted the use of biometrics in physical access control.
- Bedford and Northants Forces are currently using a manually assisted facial recognition system to help verify persons reporting on Bail.
- Surrey and Northants Forces are currently trialling the use of Livescan Lite units that can be moved to appropriate places for operational convenience. This trial is to see what benefits can be realised from better identification away from police stations using non-ruggedised kit.
- Northants police area currently trialling car based mobile fingerprinting units as part of the Lantern project.
- West Yorkshire Police have been using facial recognition since mid 2004 and are being considered as one of the pilot users for the FIND project.

4.6 Current Identity Projects within PITO

This section briefly describes the current Identity-related IT projects within PITO.

4.6.1 IDENT1

The IDENT1 project is in the process of taking over responsibility for the provision of fingerprint identification services for the Police Service from NAFIS. PITO have awarded an eight-year contract to the Northrop Grumman Corporation.

IDENT1 is intended to take identification services forward, building on the capabilities and performance provided by NAFIS through the implementation of an extensible identification architecture capable of automated fingerprint recognition, support for mobile capture and identification, but also expansion into the use of other automated identification technologies as and when a business requirement is identified. In the short term, IDENT1 will support finger and palm print.

Current IDENT1 milestones are:

- 1st April 2005
    - Transfer of Responsibility from NAFIS to the IDENT1 Service
    - Transfer of Responsibility of Scottish Livescan
- August 2005
    - Implementation of palm searching capability
- January 2006
    - Transfer of Responsibility of the Scottish Automated Fingerprint Recognition System to IDENT1
- January 2007
    - Implementation of Full IDENT1 Operational Capability

Whilst the immediate aims of IDENT1 are to enhance on NAFIS functions and develop the palm searching capability, the medium to long term development goals of the platform are more far reaching. Enhancement areas identified for IDENT1 are:

- Accessibility – enabling the access of identification services through new channels (e.g. mobile)
- Additional Capability – identification through new technical means (e.g. facial, voice, hand geometry, multi-modal)
- Information Sharing – enabling automated exchange of identification data with other agencies (e.g. other criminal justice organisations).

This long term view for the delivery of joined up identification, not through focusing on any one identification technique, but through combined 'Feature Management' is key to the long-term delivery of PITO's identification strategy, as outlined in this document.

4.6.2 Other Identification Projects

Whilst the use of biometric identification today at a national level is predominantly through NAFIS and IDENT1, there are other projects that are important to mention in this roadmap because of their potential for helping support biometric identity requirements in the future. Such projects include:

- FIND (Facial Images National Database) – a national database, with the ability to deliver facial images to officers whenever and wherever they need them. Current milestones for FIND are:
    - June 2006 - Provision of a nationally available collection of facial images
    - End 2006 – Ability to provide/return facial image in response to a positive fingerprint match
- Lantern – the delivery of a mobile capability to assist in the identification of suspects through the use of fingerprint technology. Target date for delivery is mid 2006. Refer to Part 2 for more information.
- NVIS - National Video Identification Systems (NVIS) strategy for national identity parades.

  The NVIS strategy aims to achieve an integrated approach to the operational procedures and technical standards of video (or still photographic) identification parades of persons suspected of committing a crime.

  The approved system will have full operational capabilities together with technical training and documentation to allow police forces to select a system best suited to their reasonable operational needs. It will have a single national volunteer database and suspect's database with the ability to contribute to the proposed FIND project.

  The two existing video ID systems, VIPER and PROMAT (see Part 2 for further information), are being formally reviewed with the aim of converging these two system towards the NVIS strategy
- IMPACT – The vision of this programme is to deliver an effective integrated national, regional and local information sharing and intelligence capability, which will improve the ability of the police and partner agencies to proactively use information for intelligence purposes to prevent crime, bring offenders to justice, safeguard children and vulnerable persons and further professionalize the investigation process. The key strategic drivers for the IMPACT programme are recommendations 1 to 4 of the Bichard Inquiry report [BI]. The Bichard Inquiry progress report [BIPR] includes some milestone dates for delivery for IMPACT.
- ViSOR - The ViSOR system (developed by PITO for the police and probation service) will provide for the risk assessment and management of sex offenders, violent offenders, dangerous offenders and potentially dangerous persons. National rollout is scheduled to complete by April 2005. It will be a central national application with links into the Police National Computer (PNC). Clearly, there is potential for linking FIND with ViSOR when both are operational, since their main biometrics will be facial mugshots.

More detail can be found in Annex K.

4.6.3 The PITO Biometrics Demonstration Facility

PITO have a Biometric Demonstration Facility, the purpose of which is to promote biometric technologies to the police force, PITO staff and its customers. This is achieved through the proactive testing and evaluation of new biometrics technologies and the new application of biometric technologies.

The demonstration facility includes biometric equipment based on the following technologies:

- Hand Geometry
- Iris
- Voice Recognition
- 2-D Face Recognition
- Fingerprint access control to facilities
- Biometric Pen for Signature Verification
- Lantern Fingerprint Mobile Device
- Fingerprint Keyboard for biometric logon

Visitors to the lab this year have included:

- Ministers
- UKPS
- PSDB
- PITO internal staff and stakeholders

5 IDENTIFICATION TECHNOLOGY

5.1 Introduction

This section introduces the technologies that are to be considered in this technology roadmap. The structure of this section is as follows:

- The use of biometric technology for person identification is briefly introduced. Further background material can be found in Annex H
- The technologies considered in this report are introduced. The detail of the status, risks and milestones for each of these technologies can be found in Annex I.

5.2 Biometric technology

Biometric identification can be defined as the:

> *"automated identification, or verification, of human identity through measurable, repeatable physiological and behavioural characteristics".*

Biometric technologies vary in complexity, capabilities, and performance. However, common elements can be identified. A conventional (uni-modal) biometric system can be decomposed into four components:

- Biometric Capture Module, e.g. a fingerprint reader or iris scanner;
- Feature Extraction Module, software to select the active matching data and produce a feature vector of the biometric;
- Matching Module, that compares the captured biometric with an existing database;
- Decision module, that provides a degree of confidence in any identity matched against the person providing the biometric sample.

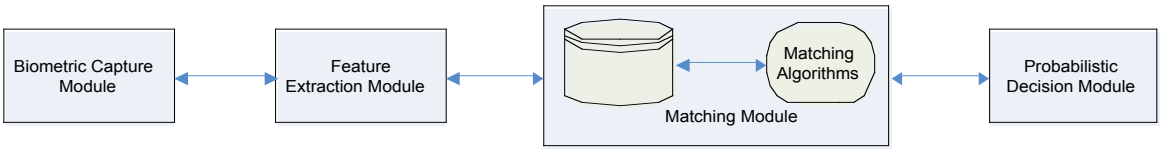


Figure 2: A simple biometric system

Depending on the application, biometric systems can be used in one of two modes: verification or identification.

- ***Verification***: Verification is defined as a 1-to-1 matching procedure. Therefore, any ID 'verification' process can be facilitated with either token or a retrieved record from stored population data. Verification is used to verify a person's identity, i.e., to authenticate that individuals are who they say they are.

- ***Identification***: Identification is defined as 1-to-many matching. Therefore, any identification process must be used in conjunction with a store of enrolled

population data. Identification is used to establish a person's identity—that is, to determine who a person is.

Although biometric technologies measure different characteristics, all biometric systems involve similar processes that can be divided into a number of distinct stages. A more complete biometric system would include enrolment and verification or identification.

Biometric technologies measure and analyse human physiological and behavioural characteristics. Identifying a person's physiological characteristics is based on direct measurement of a part of the body: i.e., fingertips, hand geometry, facial geometry, voice characteristics and iris patterns. Identifying behavioural characteristics is based on data derived from actions, such as signature. Each of these technologies and processes will be expanded upon in this section of the report.

5.3 Technologies considered

In this section, a number of technologies used within biometric identification systems are listed. These are explored in more detail in Annex I. Three categories of technology are considered:

- **Primary:** The primary technologies are those with obvious applications in policing and those that have reached a level of maturity such that practical applications can be imagined within the timescales of this roadmap.

- **Fringe:** The fringe technologies are those in a more embryonic state of development, with less obvious immediate applications, however, they are technologies that it is believed are worth continuing to observe and re-evaluate as this roadmap is taken forward year on year.

- **Supporting:** The supporting technologies are those that are not directly related to biometrics, but the development and status of which is essential to the deployment of effective biometric identity solutions.

5.3.1 Primary biometric technologies

- Fingerprint (AFIS)
- Fingerprint (Non AFIS)
- Palm (AFIS)
- Iris
- Facial
- Dynamic Signature
- Voice
- Hand/finger geometry
- DNA

5.3.2 Fringe biometrics technologies

- Body Odour
- Ear geometry

- Gait
- Retina
- Facial thermogram
- Keystroke dynamics
- Footprint

5.3.3 Supporting technologies

- smart cards (contact & contact-less)
- multi-modal algorithms
- intelligent agents
- intelligent interfaces

5.4 Technology applicability overview

Figure 5-3 places each technology being considered on a 2 x 2 matrix to show the maturity of each and to what degree they have clear application in policing. The quadrants are deliberately labelled on the axis with extreme opposite viewpoint (e.g. mature/immature) so as to indicate a field across which the technologies can move over time. Technologies are considered most useful when they move out of the darker regions into the top right of quadrant four.

Where technologies are evolving with respect to application in policing, arrows are used to indicate the direction they might have moved by the time the roadmap is updated in 12 months.

The matrix has four quadrants that can be characterised as follows:

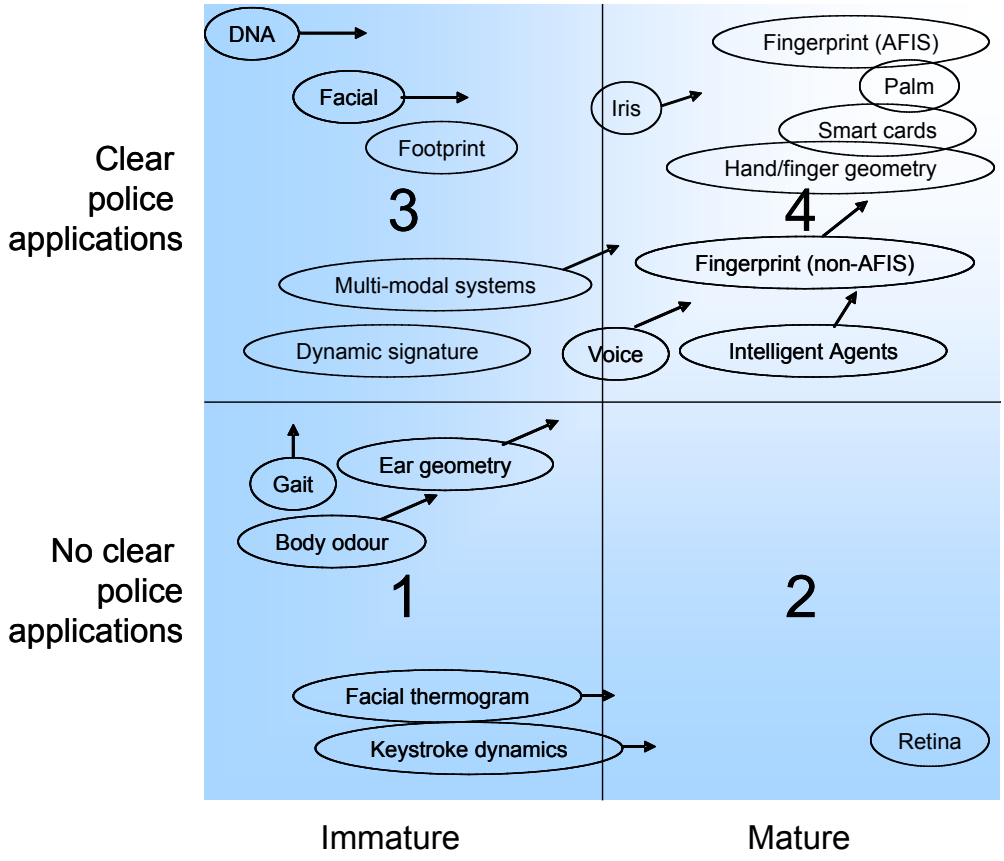
1. ***Immature technologies with no obvious policing application***. For example, gait does not seem to be maturing, but if it did, it could well be used for police surveillance applications. We recommend PITO keeps a passive watch on these technologies, but does not waste resources on them.

2. ***Technologies that have matured but have not caught on for various reasons***. For example, retina has been deployed, but is not popular with users; it shows no clear advantages over other technologies. We recommend PITO does not waste resource on these technologies.

3. ***Less mature technologies with clear application within policing***. For example, there is much demand for DNA as biometric, but it will be some years before it can be considered a truly automatic technology giving real-time results. Therefore DNA is placed at the extreme top left of the matrix. These are the technologies in which PITO should consider encouraging research so as to speed their maturity.

4. ***Mature technologies with clear application in policing.*** These are the technologies that PITO might use today. Clearly, these include AFIS. Iris is moving into this quadrant, but still requires to be proven for large database sizes. We recommend that PITO consider operating trials and rolling out these technologies as appropriate, taking non-technological factors into account.

Figure 5-3: Technology current applicability to identification in policing



Whilst incremental improvements have been made to biometric technologies in recent years no large scale movements have occurred in any one field.

Facial recognition technology stands out as the one where effort is being concentrated and therefore it is most likely to see advances in this (including 3D facial recognition and video image processing) over the next period.

Undoubtedly, generic developments will continue to occur in the feature extraction and matching algorithms, however the most important areas in the biometrics field that is likely to see large scale movements in the foreseeable future is that of collection.

One of the impasses of current biometrics systems is the device used to capture the biometric trait from an individual. Recent attempts at such developments have included contactless fingerprint capture and simultaneous collection of both iris images at once.

6 EXTERNAL FACTORS

6.1 Introduction

This section highlights the wider issues that could potentially limit the Police Service's ability to obtain the capabilities identified in section 4.1. Whilst these areas are beyond the direct control of the Police Service, it is important that PITO are aware of all these wider areas and seeks to influence the direction and decision of relevant bodies to ensure as favourable an environment as possible for legitimate police operations.

This section is structured as follows:

- An overview of biometric research in government organisations, academic institutions and beyond.
- An overview of Legislation matters as relating to police business.
- An overview of international standards as relating to biometric technologies.

6.2 Research

Fundamentally, if PITO is unable to influence, or support research initiatives sufficiently then the whole strategy laid out in this roadmap may be placed in jeopardy. It is of particular importance, therefore, for PITO to continually monitor advances in this area, and seek to encourage the research community to plug any identified gaps in development that may hinder the ability of the police force to perform its required capabilities.

Currently PITO does not fund any research activities but only provides some support in kind. See section 6.2.2 for detail of universities PITO support in this manner.

As well as the academic establishment, private sector companies continually develop new products and so there is a second level of less fundamental research always taking place. By meeting with such suppliers and sharing the aspirations of the roadmap, PITO will be able to guide the focus of their developmental effort. It will be important to emphasise that any roadmaps shared are not firm commitments to purchase in the future.

6.2.1 UK Government

The UK government is directly investing in the development of scientific tools for the Police Service through bodies such as the FSS and PSDB, as laid out in the PSTS (see section 4.4.2). Current research areas that may influence the roadmap include:

- DNA – "lab-on-a-chip". This is some way off, so we have included "lab-in-a-van" as a half way house solution.
- Chemistry – improved techniques for recovering latent fingerprints
- Application of video enhancement to evidential images
- Development of portable identification and capture systems.

6.2.2 UK Universities

There are a number of UK academic institutions that have an interest in research into biometric technologies and technologies that support biometric systems. In the UK these include:

- **University of Kent:**
    - extensive biometrics work within Electronic Engineering Department with particular emphasis on multi-modal systems and intelligent agents and interfaces
    - involved in the VitaB project (see Kingston below)
    - Have set up the International Centre for Advanced Research in Identification Service (ICARIS) in conjunction with Sheffield University, an information sharing network for the purpose of furthering human identification.
- **University of Southampton:** expertise in the area of gait recognition.
- **University of Bournemouth:** developing research related to the modelling of human hair characteristics and the way that these are visualised.
- **Kingston University:**
    - producing innovative developments in the use of CCTV technology and in the area of motion prediction
    - has set up a network of academia (with Kent and Sheffield Universities) and end users in the field of video related threats (VitaB) and an innovative approach to tracking vehicles and people using CCTV.
    - working with Surrey on the REVEAL project (Recovery of Evidence from Video: Extracting Archiving and Learning).
- **Surrey University*:***
    - working on new facial identification techniques and the 3D modelling of faces.
    - also working with Kingston on REVEAL (see Kingston above).
- **Sheffield University:**
    - have obtained funding (brokered by PITO) from the US government for the development of large scale facial image test sets for use in assessing the performance of facial recognition systems. Sheffield University are currently gathering 3000 3D head images on behalf of the FBI. The primary purpose is to look at variation of features across the population. It is hoped that this (raw) data will eventually be made available for research purposes. They are also leaders in forensic anthropology and the identification of human remains.
    - Involved in ICARIS (see Kent above).
- **Nottingham University:** developing techniques for the production of 3-D representations of faces from video footage.

- **University of Westminster:** PITO have assisted with the formulation and delivery of the first biometrics orientated degree course (MSc) to be offered by a UK University, which is now in its second year.

- **Loughborough University:** Research on the physical nature of latent fingerprint deposition during grip and linking it to fingerprint of that person.

Other universities also involved in research related to Identification and which is of interest to PITO, include Queen Mary's, St Andrews, Strathclyde, East Anglia and Manchester and the Biometrics team also endeavours to maintain close links with these.

PITO is continuing to support bids for funding under the Electronic and Physical Science Research Council (EPSRC) Crime Prevention and Detection Technologies Calls, in respect of Kent, Kingston, Sheffield, Bournemouth and Nottingham Universities. It is also active in building collaborative links between Universities in order to focus effort in the area of identification related research and development.

PITO is already bringing students into the organisation and there are plans to increase the scope of this cooperative effort in order to build even stronger relationships with academia. It is probable that students at both MSc and PhD levels will be invited into the organisation to assist with specific projects whilst pursuing their studies.

6.2.3 European Investment

Many of the European Framework 5 & 6 projects involved biometric research. The University of Kent were involved in a biometric Framework 5 project called 'Fingercard' and were also involved in a consortium that bid to establish a Biometric Network of Excellence under Framework 6. Fingercard was a self-enrolling biometric smart card, enabling an individual to present credentials (i.e. I am the legitimate cardholder) without having to give away their true identity (since the enrolment process is self contained).

Another example of research in biometrics sponsored by the European Commission is the now complete BioVision project [BIOV], to develop a European wide view on the direction of the biometrics market in preparation for Framework 6.

6.3 Legislation

It is imperative that relevant legislation is in place in advance of new policing applications going live if delays are to be avoided. Identification of relevant legislation through this roadmapping process is the means to ensure that the necessary amendments to Acts of Parliament can be tabled and, if appropriate, passed in time.

Legislation regarding the police ability to identify individuals has been changing rapidly over the last few years. This section highlights the key acts and the current state of affairs regarding what the Police Service can and can not expect to be able to do in this area.

The piece of legislation that has the single biggest impact on the Police service use of identification is the Police and Criminal Evidence Act or PACE (1984). More recently, the Criminal Justice and Police Act (CJ&P) (2001) has amended and updated some of the powers in PACE.

PACE originally enabled the capture of DNA, fingerprint and photo evidence at point of charge; however, these had to be discarded if the offender was subsequently acquitted for that crime. For persistent offenders, the photo could be kept if deemed to be more recent than one currently on file. The CJ&P Act modified these powers to enable all this

information to be kept for all suspects charged, whether or not they were ultimately convicted.

Thus, after the CJ&P, it was the case that when someone was arrested and a custody record created, DNA and fingerprints could be taken, but only with their consent. Consent was no longer required once someone was charged.

Since the initial Roadmap, this has changed, with the introduction of the Criminal Justice Act (CJA) 2003, which has had new clauses added to enable the police to take fingerprints and DNA at point of detention or more precisely, from a "person who is in police detention, having been arrested for a **recordable offence**", without having to wait until they are charged.

Practically speaking, this change has not led to a dramatic increase in the volume of fingerprint sets taken, however, the numbers are starting to rise, as systems and procedures are upgraded and it is expected in the long term that the amount of identification data processed will increase (against the amount taken prior to the CJA) by around 80% by volume, e.g. from 100 000 to 180 000 fingerprint sets taken per month.

Whilst PACE is predominantly for the Police Service, the laws around the gathering of identification evidence are actually applicable to any "Investigative Agency" including Customs and the Inland Revenue.

Another bill to impact photo usage is the Prevention of Terrorism Act 2002. This makes specific provision for the taking of photographs of people in custody suspected of terrorism and the powers to forcibly remove any mask or headwear if required (this needs an explicit power otherwise it would be an assault). These photos may be retained whether the suspect is charged or not.

Other acts that impact on identification services and the usage of biometric data include:

- **Regulation of Investigatory Powers Act 2000:** Covers surveillance activity (e.g. telephone and CCTV).
- **Data Protection Act (DPA) 1998:** How data held on an individual can be used. Also deals with the rights of an individual to access that data.
- **Human Rights Act 1998:** Defines acceptable behaviour for the treatment of human beings.

This is a complicated and rapidly changing legislative area, and there are a number of recent acts and upcoming bills that are expected to change the legal identification landscape yet further. These include:

- **Coroners Act:** There is a proposed amendment to the Coroners Act due in 2005 to enable elimination samples to be taken from external locations (e.g. taking fingerprints or DNA from a bedroom to try and identify if a missing person has been found).
- **Extradition Act 2003:** The only grounds for appeal against extradition from one EU country to another are mistaken identity. This Act includes legislation relating to the power to take fingerprints from an extradition subject within the EU for the purposes of establishing their identity.
- **Serious Organised Crime and Police Bill:** This bill was introduced in 2004, and as well as including the legislation for setting up the National Intelligence Agency, it also includes legislation to enable the capture of fingerprints for identification purposes without consent, outside of police premises if an officer has reasonable grounds for suspicion.

6.4 Standards

This section discusses standards relevant to biometric systems. Standards are about supporting interoperability and data interchange among applications and systems.

The application of standards is of particular relevance in the realm of law enforcement, as the identification of criminals can be an international affair. Moreover, operational efficiency is not only damaged by lack of compatibility across international borders, but also between the UK's different police forces, and also across different government agencies. The potential for operational efficiencies through effective data sharing are significant, and the principle barriers that prevent such benefits being realised due to an inability to easily share data, a problem that can be overcome through a co-ordinated and proactive approach to international standardisation.

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, IAfB representing 50+ member companies, numerous commercial organisations and numerous UK government departments (e.g. PITO, UKPS, Home Office).

The FIND image standard, "Police Standard for Still Digital Image Capture and Data Interchange of Facial/Mugshot and Scar, Mark & Tattoo Images", is currently awaiting ACPO approval, and now needs to be handed over to the Biometric Team for ongoing support and development - keeping track of changing worldwide standards and drawing in the NVIS Standards. The benefits of this standard will be that UK Forces will have a minimum standard to adhere to, and also represents a stake in the ground from which further developments can be made.

Further detail of the current status and milestones for biometric standards is available in Annex J.

6.5 Risk Areas to Monitor

This section summarises some of the high level areas of risk that must be continually monitored to ensure the roadmap's continuing accuracy.

6.5.1 Legislative Changes

Legislative changes in recent years have had a specific impact on the police ability to process biometric identifications of individuals (see section 6.3). As is often the case with new and complex legislation dealing with technical issues, there is a degree of ambiguity regarding some powers, and in particular how these powers should be interpreted in the light of other laws such as the Data Protection Act and the Human Rights Act. With this in mind there is a risk that police activity in this area will be affected and potentially hindered by specific cases, challenges and rulings in the area of biometric identification in the next ten years.

6.5.2 Commercial Applications

As well as presenting opportunities for re-use, commercial developments of biometric solutions also present a risk to police usage of biometrics, particularly in the area of public perception.

The quality requirements of commercial organisations are likely to be very different. For example, when using fingerprints to log onto PC based systems, an organisation might rank user convenience over accuracy, leading to a lower quality threshold than used in police systems. This will lead to users of commercial biometric systems becoming aware of and being used to biometric systems where false identifications do arise, creating the potential for a false mistrust of the police use of what is perceived to be the 'same' technology.

In a society where the use of biometrics is widespread, the police will have to be careful to communicate their different quality requirements, and therefore their different quality thresholds, to the general public. Note that this risk is more applicable to overt identification technologies, such as fingerprinting rather than covert technologies such as applying biometrics to CCTV.

6.5.3 Resistance to National Identification

The use of biometrics for identification is often controversial. No matter how useful biometrics is to the police, they are likely to create more problems than they solve if they are not used within public acceptance.

At this point in time it seems that the perceived traditional British opposition to national identity cards is slowly being eroded by threats of terrorism, rising identity theft, and also the rise of a number identity schemes in other European countries. Indeed, with the Identity Cards Bill currently going through the commons, with a target of achieving royal ascent in April 2005 the reality of Identity cards may well soon be something that becomes part of the British public's everyday lives.

However, public acceptance of biometric identification will depend heavily on the clarity of the benefits it provides society versus the potential danger it represents.

The Police Service can manage that risk by making sure that any required limitations on the use of identification data (to prevent potential abuses) are clearly set out, well communicated to the public and studiously adhered to.

6.5.4 Attacks and Countermeasures

Every biometric technology faces the continuous risk that a new and innovative method will be found to compromise its integrity and 'beat the system'. In the majority of cases such attacks can be dealt with through appropriate countermeasures, and thus the risk is that costs will increase, and development in a technology area will fail to keep up with criminal efforts to defeat it.

It is possible that a fundamental flaw will be found in a technology that cannot be overcome with countermeasures and will present a permanent limitation on that technology's usefulness.

6.5.5 The Changing Profile of Crime

ACPO studies into future crime patterns have identified that, as the security of material possessions is improving rapidly, the weakest point of attack available to a criminal is increasingly the person. Thus it is expected that over the coming decade, crime against people will increase as crimes against property decrease. If this proves to be correct then it is likely that criminal resource will be focussed increasingly heavily on defeating identification technology, and the benefits to be gained from such attacks must be carefully monitored and minimised through proper risk analysis on any biometric identification system. Things to be considered include:

- Are a number of records held in a central database? Would it be more sensible to use a token-based identification scheme with 1:1 matching on a smartcard, removing the criminal opportunity to obtain multiple sets of identity data from a single source?
- How easy would it be for a criminal to force an individual to use the system against his or her own will? Are their measures in place to prevent this?

6.5.6 Cost of Multi-Modal Identification

As the Police Service start to develop the capability to combine different modes of identification to provide more accurate and timely identification results, the cost associated with processing each mode needs to be taken into account, and the complexity of the identification function undertaken needs to be proportionate to the identification need at that point in the policing process. For instance, it may be that during a criminal investigation, the cost of performing both fingerprint and DNA identification early on in the case is an unnecessary expense, and DNA need only be analysed to back up an investigation as and when such additional assurance and evidence is required to assist with the enquiry.

With this in mind, as the complexity of identification options open to the police increases, so the need for detailed policy and best practice guideline increases to ensure optimum benefit is gained from the technology, both in terms of operational gain, and cost control.

The use of a multi-modal approach will mean that the current National Fingerprint Board and fingerprint bureaux costs would increase as there will be the need for a National Identity Board and associated identity bureaux with a wider range of expertise. This would be a considerable change to business processes within policing.

6.6 Softer Issues

There are other, less tangible areas that may constrain the use of biometric applications within the Police Service. Whilst such softer issues may not provide black and white answers as to what can and cannot be achieved, it is important to ensure they are given careful consideration. The tripartite structure of the PITO board should help ensure that these factors are not overlooked. Key areas are outlined in the following subsections.

6.6.1 Public Acceptability

It is widely accepted that Rule of Law requires popular acceptance. Any government that tries to enforce a law that the majority of its citizens do not agree with will find it difficult to do so. This affect is further enhanced in a democracy such as the UK, where one badly received piece of legislation could cost a government the next general election. With this

in mind, the way that new powers are sold to the public is very important. Any new power the police force is given and looks to exert must be carefully communicated to the public, emphasising the benefit to society of the new power, and the constraints in place to stop that power being abused, thus facilitating the required public acceptance. If such benefits and constraints are not in place, then the new power is, at best being rushed through, and at worst altogether inappropriate.

6.6.2 Ethical Considerations

Even if a power is publicly acceptable, this does not necessarily mean that it is ethical. The Home Office seeks to ensure that the legal acts that it puts forward to Parliament are ethical and balance the needs of the entire community through the diverse make up of the Bill's team responsible for each legislative document. For instance, legislation regarding the use of DNA might have input from ACPO, SPU, FSS, but also liberty bodies such as the Human Genetics Council, as well as specialist legal personnel.

6.6.3 Personal Privacy

The privacy of the individual is a much-discussed area of consideration in this age of electronic networks and mobile communications. The ability of technology to track the actions of people and objects is greater than ever before, hence the role of legislation in the protection of privacy is key to the rights of the individual. The issue here is what is "reasonable" to ask for, and what steps are "proportionate" to take, both in terms of protecting privacy, and in terms of revealing activity as part of a legitimate police investigation. As new identification and surveillance techniques start to be used, particularly those relating to biometrics, it is likely that the boundaries that define what actions are "reasonable", and "proportionate", will be unclear. In order to resolve such issues specific legal challenges are likely to be required, and this is an area that PITO should be observing closely.

7 CONCLUSIONS

The original PITO Identification roadmap made four key findings with regards to how PITO could best focus its efforts to ensure that identification capabilities are delivered to the Police Service in a most timely manner. The review of the primary application areas (summarised in Section 3.3) has shown that all four of these findings are still valid, and has additionally highlighted a fifth area where PITO have an opportunity to positively influence the development of identification services for policing.

7.1 Making best use of IDENT1

It is still clear that the vision of moving towards a joined up identification platform, with IDENT1 at the heart of this architecture has long term strategic benefit.

This roadmap continues to provide a focus to ensure that development effort in IDENT1 is prioritised to be inline with overall police and government strategy with regards to the addition of new technology, the improvement in information accessibility and the development of information sharing facilities across departments and borders.

Once digital mugshots are fully integrated into IDENT1 (via FIND), the system will have fingerprint, palm print and facial data on a number of arrested individuals. In the mean time, considerable research effort will have gone into the efficient use of multi-modal biometric systems (Annex I), an area where, even now, clear performance advantages can be seen.

At this point, a proper investigation into the combination of the identity information held within IDENT1 and elsewhere into a truly multi-modal identity system should be supported. This is likely to involve the assessment of the state of technologies such as intelligent agents and intelligent interfaces (see Annex I in Part 2) to provide the police with the foundation for a 'holistic' and integrated identification system.

Such a trial is likely to be extensive, and it would be prudent to include other modes of identification that are being considered for inclusion into IDENT1 at this time (e.g. voice/iris/3D facial etc).

7.2 Video processing

Core to meeting a number of police needs is the development of more effective ways of handling the large and growing amount of Closed-Circuit Television (CCTV) evidence the Police Service deal with. Specific effort should be spent in progressing the use of this technology.

This review has highlighted the importance of PITO involvement in this area, as there are a number of IT issues that are hindering PSDB work in this area that PITO could assist in.

7.3 Supporting research

The Police Service cannot rely on the commercial sector to meet all their needs, given the largely unique identification requirements of law enforcement. PITO must continue to closely monitor research initiatives into technology that could support key policing needs, and be prepared to actively support research, both financially and with resource, as

required. Such support mechanisms are already in place with regards to encouraging collaboration between PITO, Academia and commercial suppliers. These links need to be maintained.

7.4 Making best use of biometrics

It is clear from the work carried out to produce this roadmap that there is a lot to be gained from simply using existing technologies effectively. The National Fingerprint Board is seeking to ensure that this is done for fingerprinting technology and similar management and best practice structures would be of benefit for wider identification functions in the future, through a 'National Identification Board'.

Making best use of biometrics will also involve relationships outside of the Police Service. The HOSDB is set to establish a Biometric Centre of Expertise during 2005. PITO would do well to establish regular contact with this body as soon as it is established to assist in ensuring that best practice from the Police Service disseminates to wider UK government.

7.5 National identification of officers

This is a new key recommendation. Whilst the original identification roadmap did include 3 primary application areas to which standardised officer identification was key, they were all long term goals and as such were not put forward for immediate action. With the increasing prominence and success of the National Intelligence Model and with the establishment of the IMPACT programme in response to the Bichard inquiry the need of this capability has become more urgent.

Without a simple and secure means to identify officers electronically, it will become increasingly difficult to provide operationally acceptable user interfaces to ever more sophisticated and distributed intelligence systems. Thus if the long term vision of IMPACT is to be successfully achieved, a means of intelligently tailoring the interface to the role, rank, skills, location and access device of a member of Police staff is vital.

There are many other side benefits to the development of standardised national identity for police staff. If every police officer were to have a biometric ID card for access control, projects need to be but in place to ensure that the potential of this card, with regard to reducing paperwork and bureaucracy elsewhere, be fully realised.

7.6 PITO working with partners

Progress in joining up the CJS has been slow since the production of the original roadmap in 2003. We are still a long way from seeing reliable tracking of individuals through the CJS. This would require the uniform collection and verification of fingerprints at each handover point (e.g. prisons, probation, etc.). This is seen as a major hole in the CJS, but one that PITO is unlikely to be able to fix alone since it goes beyond PITO's remit.

The area where there is room for considerable improvement with regards to the identification of criminals and alleged criminals is when the wider criminal justice system is taken into account. Criminal Justice IT has been tasked with developing this area but has found it far harder to make progress than expected. They are currently striving to find a means to enable a consistent reference number to follow people through the criminal justice system, but as yet are not giving serious thought to the use of fingerprint technology.

As technology experts in this area, PITO are in a position to help and should continue to develop links with CJIT with a view to better use being made of PITO identification systems by the wider criminal justice community.

There is increasing interest in Identity Management across the globe. Other parts of UK government are now active in this area that PITO has been leading for some years. There are subtle differences in the requirements of each part of UK government (PITO, IND, UKPS, UKvisas) since different populations are sought to be identified (e.g. criminals; citizens; asylum seekers; etc). PITO should continue to work closely with other parts of government, particularly as the Home Office develops its approach to Identity Management and government-wide frameworks and systems are likely to be developed. PITO has a lot of experience to contribute both in terms of the technologies and the procurement and operation of national identification programmes with international links.

PSDB (soon to be HOSDB) have expertise in imaging, whereas PITO is the centre of expertise for Police Service IT. PSDB would like to work more closely with PITO with a view to resolving the IT issues that are delaying development in this area. It is therefore a key recommendation of this roadmap that PITO make the formal IT support of PSDB in this area a priority.

ANNEX A REFERENCE DOCUMENTS

The following references were used in compiling this report. The labels in square brackets are used where citations of these references are necessary in the body of this document.

[BI] *Bichard Inquiry,* June 2004 (available from www.bichardinquiry.org.uk)

[BIOV] BIOVISION, Roadmap to successful Deployments from the User and System Integrator Perspective, prj number IST-2001-38236. EC roadmap in preparation for Sixth Framework of support for R&D. Published in 2003

[BIPR] *Bichard Inquiry progress report,* January 2005 (available from www.bichardinquiry.org.uk)

[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

[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.

[ISS4PS] Information Systems Strategy for the Police Service

[ITL1-2000] ANSI/NIST ITL 1-2000Interchange Format for Fingerprint, Marks, Scars and Tattoos (MST) Information

[NIM] *National Intelligence Model,* NCIS, 2000

[NIMMS] *National Intelligence Model Minimum Standard,* ACPO NIM, April 2003

[NIMMS2] *National Intelligence Model Minimum Standard 2,* ACPO NIM, December 2004

[NJG] *Narrowing the Justice Gap*, Home Office Framework Document, October 2002.

[NPP] National Policing Plan 2004-2007, Home Office, November 2003.

[PBTF] *Police Bureaucracy Taskforce,* http://www.policereform.gov.uk/bureaucracy/index.html

[PFP2004] PITO Forward Plan 2004 to 2009, July 2004

[PSTS2004] *Police Science and Technology Strategy 2004-2009*, SPU, 26 May 2004.

[TRM2003] *Biometrics Technology Roadmap for Person Identification within the Police Service*, AMTEC, v1, July 2003.

ANNEX B TERMS AND ABBREVIATIONS

Term	Definition
ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers of Scotland
AFIS	Automated Fingerprint Identification System
Airwave	The name of the public safety and radio communication service being rolled out to the police.
ANSI	American National Standards Institute
APA	Association of Police Authorities
API	Application Programming Interface
APIS	Automated Palm Identification System
ARC	Application Registration Card
ATM	Automated Telling Machine
BFT	Biometric Facial Template (IND project)
BS	Building Society
BSI	British Standards Institution
BTF	Bureaucracy Task Force
BWG	UK Government Biometrics Working Group (UK Govt)
CBEFF	Common Biometric Exchange File Format
CCTV	Close-Circuit Television
CD	Committee Draft
CEN	Comité Européen de Normalisation
CESG	Communications- Electronics Security Group
CJ&P	Criminal Justice and Police (Act)
CJA	Criminal Justice Act
CJIT	Criminal Justice Information Technology
CJS	Criminal Justice System
COSLA	Convention of Scottish Local Authorities
COTS	Commercial, Off The Shelf
CRB	Criminal Records Bureau
DARPA	Defense Advanced Research Projects Agency (USA)
DNA	Deoxyribonucleic acid
DPA	Data Protection Act
DSS	Department of Social Security (now DWP)
DSV	Dynamic Signature Verification
DVLA	Driving License Authority
DWP	Department for Work and Pensions (replaces DSS in UK Govt)
EMV	Europay, MasterCard, Visa. The smart card credit/debit payment international standard being rolled out currently.

Term	Definition
EPSRC	Electronic and Physical Sciences Research Council
ETSI	European Telecommunications Standards Institute
EU	European Union
EURODAC	European Asylum Seekers Fingerprint System
FBI	Federal Bureau of Investigation (US)
FCO	Foreign and Commonwealth Office
FIND	Facial Images National Database
FIS	Forensic Integration Strategy
FRR	False Rejection Rate
FSS	Forensic Science Service
HMIC	Her Majesty's Inspectorate of Constabulary
HO	Home Office
IAfB	International Association for Biometrics
IAFP	Immigration and Asylum Fingerprint Programme
IAFS	Immigration and Asylum Fingerprint System
IBIP	Immigration Biometric Identification Programme (IND)
ICAO	International Civil Aviation Organization
ICP	Identity Cards Programme
ICTU	Information and Communications Technology Unit (UK Home Office)
ID	Identity
IDENT1	Replacement PITO system for NAFIS that will ultimately provide support for identification using a variety of biometric technologies beyond fingerprint and palm.
IEC	International Electrotechnical Commission
IMPACT	Information Management, Prioritisation, Analysis, Co-ordination and Tasking
IND	Immigration and Nationality Directorate
IPR	Intellectual Property Rights
IRIS	IND project to use Iris Scanning for expedited passage at UK Borders.
ISO	International Standards Organization
ISR	Image Storage and Retrieval
ISRP	Immigration Stateless Refugee Project
IT	Information Technology
IVR	Interactive Voice Response
JTC	Joint Technical Committee
Lantern	Police project to add roadside identification to ANPR and beyond using mobile fingerprinting.
Livescan	Hardware and software for the recording of a person's fingerprints directly from their fingers in a digital format.
MRTD	Machine Readable Travel Documents

Term	Definition
MSc	Master of Science
NA	Not Applicable
NAFIS	National Automated Fingerprint Identification System
NCITS	National Committee for Information Technology Standards (USA)
NFB	National Fingerprint Board
NIM	National Intelligence Model
NIM	National Intelligence Model
NIST	National Institute of Standards and Technology
NP	New Proposal
NPL	National Physical Laboratory
NPP	National Policing Plan
NSPIS	National Strategy for Police Information Systems
NTWG	New Technology Working Group (ICAO)
NVIS	National Video Identification System
OeE	Office of the e-Envoy (HO)
ORD	Operational Response Database
PAA	Primary Application Area
PACE	Police and Criminal Evidence Act
PAPA	Police Automated Picture Analysis
PC	Personal Computer
PDA	Personal Digital Assistant
PhD	Philosophy Doctorate
PIFE	Police/Immigration Fingerprint Exchange
PIN	Personal Identification Number
PITO	Police Information Technology Organisation
PKI	Public Key Infrastructure
PLX	An intelligence-flagging IT system currently being piloted by three police forces (source: Bichard).
PNC	Police National Computer system
PPAF	Policing Performance Assessment Framework
PROMAT	An electronic video identification parade system (similar to VIPER)
PSDB	Police Scientific Development Branch (HO)
PSTS	Police Science and Technology Strategy
PSTSG	Police Science and Technology Strategy Group
PSU	Police Standards Unit (HO)
R&D	Research and Development
SAA	Secondary Application Area
SCC	Serious Crimes Cache

Term	Definition
SIM	Subscriber Identity Module. The smart card inside digital mobile phones.
SPU	Science Policy Unit (HO)
TETRA	TErrestrial Trunked RAdio
UK	United Kingdom
UKPS	UK Passport Service
UN	United Nations
UNHCR	United Nations High Commissioner for Refugees
US/USA	United States/United States of America
USB	Universal Serial Bus. An interface technology replacing standard serial ports.
VIPER	Video Identification Parade Electronic Recording
ViSOR	Violent Sex Offender Register
WSQ	The Wavelet Scalar Quantization (WSQ) Grey-scale Fingerprint Image Compression Algorithm is the standard for the exchange of fingerprint images within the criminal justice community