



Report of the EURIM Personal Identity Group meeting on the Identity and Passport Service' corporate plan, 15 June 2006, 1000-1200 hours in Committee Room 13, Palace of Westminster

Chairman: Stephen Darvill (LogicaCMG)

Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The Identity and Passport Service's document 'Safeguarding your Identity; Corporate and Business Plans 2006-2016' raises a number of questions about ID Cards plans. What are the indicators of success for the project? How would success be judged? How will 'improved services' be measured? It also appears from recent statements that the ID Cards Team is awaiting responses from the IT industry on how the technology should work, while the implementation of the National Identity Register will be dependent on proposals from suppliers.
2. The introduction of ID cards entails political risks (e.g. civil disobedience). A better risk assessment strategy for identifying and quantifying where and when things will go wrong during normal operations (e.g. changes to registrations, lost cards, insider fraud etc.) is also needed. The Scheme is unlikely to be perfect, but is expected to be better than the existing situation. Problems are more likely to arise in other areas than the technology, and to identify these might be a valuable contribution for EURIM to make. Projects also commonly encounter problems because of changes in objectives and targets on the part of ministers.
3. Substantial data is available from existing private sector CRM and IM systems about the volume of lost, compromised and stolen identities under different systems and also the routines and costs for correcting them. This should be part of the risk assessment, but there is no sign that the banks and FS organisations that can provide the operational information have been consulted on these. There should be a requirement on the IPS to publish how it will deal with the many errors and corrections that will occur each week in the system.
4. Biometrics research presented at a forensics seminar organised by the Jill Dando Crime Science Institute on the practical experience of the US online fingerprint systems revealed a major problem with false negatives, even though the systems were operated to much lower tolerances than in the UK, often exacerbated by poorly maintained equipment and other human-related causes. This and similar data could be used to develop evidential policy, but appears not to have been tapped by IPS. There is a clear need for Government to widen its sources of information, and to include international examples of large IM schemes: EURIM could help harvest this experience and collate the evidence to inform policy-making.
5. The ID cards system may stand or fall on its ability to deal with exceptions. Quantifying outcomes financially would provide a basis for evaluating costs, including those associated with the misuse of identity. Estimating to what extent levels of fraud would be controlled by the measures planned would better provide for the realisation of the benefits expected. Biometrics will improve the situation, but cannot be a panacea.
6. It was agreed that EURIM should invite IPS to address the PI Group at a time of its choosing, so that we know more of their thinking and evidence base. In the meantime, EURIM should position itself as a 'critical friend' of the IPS, and provide case studies of operator and user experience of large-scale biometrics and IM systems to reduce errors and uncertainty, deal with exceptions and manage risk.

1. Introduction

1.1 The purpose of the meeting was to discuss how the objectives of the Identity and Passport Service might best be delivered, and what role there might be for EURIM in helping to meet the many challenges facing the IPS team. It was noted that Members had stated that they wished to hold this meeting, even though a speaker from IPS was not available.

2. 'Conducted tour' of IPS strategy/intent

2.1 This section of the minutes should be read in conjunction with the pdf version of the Powerpoint slide presentation sent by email with this document.

2.2 The Identity and Passport Service was established under the Identity Cards Act which received the Royal Assent on 30 March 2006, with a stated Mission of: 'Safeguarding your identity'. The IPS is self-financing, with a budget of ~£300 million which also helps fund FCO embassies, high commissions and consulates.

2.3 The Corporate Plan sets out the strategies for the next 10 years while the Business Plan identifies performance indicators and targets to March 2007. The primary objectives of the IPS in the Corporate Plan are to improve services and customer convenience, enable travel and increase international security and assist in the prevention of crime. In delivering these objectives, the National Identity Scheme is said to offer benefits for individuals, private organisations and Government.

2.4 The IPS Vision is to provide leadership in identity authentication and verification. Being able to prove identity is stated as a fundamental requirement in modern society, though this might be contestable.

2.5 Strategic objectives are listed as:

- Customer confidence - putting the customer first
- Identity authentication - establishing the identity of customers with greater certainty
- Transforming identity management - promoting best practice across Government
- Unlocking staff potential - motivating and rewarding staff
- Efficiency and business assurance - providing business assurance and innovation
- Innovation and effectiveness

2.6 The mission and vision are underpinned by a set of 5 internal 'values':

- Working together
- Customer service
- Embracing and supporting change
- Valuing people
- Personal responsibility

2.7 IPS delivery partners comprise the Immigration and Nationality Directorate, UKvisas and the Foreign and Commonwealth Office. IND will remain responsible for the immigration status of foreign nationals under the NIS, UKvisas are responsible for improved identity authentication, particularly through biometric capture, and FCO is responsible for issuing UK passports to British citizens overseas, typically issuing over 450,000 each year. The FCO and IPS are implementing the biometric e-Passport as a joint project.

2.8 The Plan describes current partnerships with service providers, which include EURIM members ATOS Origin, Siemens Business Services and Equifax, along with MMT, Worldchoice UK and Special Mail Services Ltd. Enhancement of current services involves ongoing and short-term initiatives to improve current processes and services associated with passports, to be delivered via 4 key projects:

- Authentication by Interview
- Personal Identity Process
- e-Passports
- Passport Validation Service

The first two relate to improving the application and enrolment process by interviewing people in some depth, while the latter two are designed to meet international passport security requirements. IPS has begun to issue passports with an electronic chip, and will complete the roll-out of this programme

during the third quarter of 2006. The electronic chip will contain a facial image created from photos submitted with application forms.

2.9 IPS anticipate piloting the recording of fingerprints as a second biometric from volunteers in late 2007. This prepares the UK to match mandated EU standards for both fingerprint and facial biometrics for Schengen area passports.

2.10 Evolution to the NIS is planned for the period 2006-2010, and will involve introducing best practice registration processes including interviewing all first-time applicants and customers applying for passport renewals. Best practice will also involve recording up to three biometric types (fingerprints, irises and facial image) for all applicants and providing an automated identity authentication and verification process.

2.11 Key changes will also include:

- a secure end-to-end process for all products and services to limit fraud and misuse;
- a unique identity number for registered ID card and passport holders;
- an online service to allow accredited organisations to verify the identity of individuals;
- developing the NIR, including the data storage and applications processing technology;
- developing policy on behalf of the Home Secretary to support the development of cross-Governmental best practice in identity management.

2.12 Other aspects of the Plan were described, including the identity product set, finances, risk management and the vision of IPS for 2016 – details in the accompanying slides. Key performance indicators are aligned with strategic objectives, while the Plan identifies 12 areas of risk management and business assurance activity, including transferring risk to partners.

2.13 IPS will produce 'Vital Signs' information for Ministers on a weekly and monthly basis on all aspects of performance. Reports will show the performance of each office on a weekly basis and are used to highlight not only areas of concern but also areas of performance above expectation.

2.14 IPS was created as an Executive Agency of the Home Office with corporate governance assigned to a CEO with 4 executive directors, and the Agency Strategy Board, chaired by the CEO, who will also have responsibility for responding to the requirements of the National Identity Scheme Commissioner.

3. How IPS strategy might be implemented - Discussion

3.1 There was some speculation that the CTO Council had been created because of the inability or unwillingness of the CIO Council to deliver practical solutions to progress the Transformational Government strategy. What executive powers does the CTO Council have, if any, and what might they be able to achieve? It would be unfortunate if something 'fashionable' were to emerge from the deliberations and be adopted by the eGU as a requirement for all future large scale IT projects, whether appropriate or not. This would represent the wrong perspective for breaking the programme down into smaller projects. A Service Oriented Architecture (SOA) within an Enterprise Architecture may not necessarily be the best way forward: smaller projects tend to have a higher success rate than large projects.

3.2 Others understood the CTO Council to be a logical extension to the next level down, set up to achieve co-ordination across the public sector as effectively the agents of the CIO Council. They could offer guidance to address systemic problems, although the value of this remained to be seen. OGC would claim they have worked to improve project management over the last ~5 years, though as yet there have been no published test cases via the Gateway Process.

3.3 There had been no discernible sign of new thinking in any of the presentations made about large-scale IT governance that will reduce the risk of failure. What are the indicators of success for the project? How would success be judged? How will 'improved services' be measured? These questions remain unanswered, while it appears from recent statements that the ID Cards Team is waiting for responses from the IT industry to draw up a level two specification that would outline how the technology should work, and that the implementation of the National Identity Register will be dependent on proposals from the chosen suppliers, decided after trials held during the procurement phase.

3.4 Transfer of risk and the achievement of greater certainty might lead to the establishment of an SOA, but in the final analysis, the risk that cannot be transferred is that of a sovereign nation. How much of a problem was the lack of numeric identification for their objectives? The media would be sure to pounce at the first sign of a glitch in the system. There should be a much better risk assessment strategy for identifying and quantifying where and when things go wrong (applicable to all systems, not just ID cards).

3.5 However, the question of EA's or the management of the implementation project is not the risk; the big risk lay with internal issues such as the staff conducting face to face interviews, and the morale of the department – these cannot be project managed. Also, the Government was introducing absolute identity into a society that has never experienced it.

3.6 Problems are more likely to arise in other areas than the technology, and to identify these might be a valuable contribution for EURIM to make. The IT industry should be conveying the message that projects often encountered problems because of continual changes in objectives and targets set by ministers. Introducing ID cards for the first time is a political risk that may crystallise around a substantial proportion of the population refusing to register.

3.7 Would online authentication apply to a person's ID, or to a document? At the moment, we have authentication of a document, with no current guarantee that the person receiving a passport, credit card or token is the actual person it is intended for. Would the ID card be delivered to the individual in response to a PIN number entry, or would it be sent in the mail? However, the introduction of biometrics has provided solutions that are sufficiently strong to padlock a token to a unique individual.

3.8 There should be a requirement on the IPS to publish how it will deal with the many errors and corrections that will occur each week in the system. There will also be people who set out to defraud the system, others who find that their identity has been taken by someone else, especially in the early stages of registration when identities are being established.

3.9 It is intended that there will be a mechanism by which an individual can request information about every transaction, including every request for identity. This establishes 3 sets of data: the location of an individual, and the time and subject of the request. How will this data be handled, and how will the public be assured that it is secure? Any number of organisations or people could make identity checks, and in order to reduce risk, a proper system of channels and permissions was needed for accessing the NIR (although it was acknowledged that such mechanisms are probably already envisaged).

3.10 Substantial data is available from existing private sector CRM and IM systems about the volume of lost, compromised and stolen identities under different systems and also the routines and costs for correcting them. However, there is no sign that anyone has contacted the banks and FS organisations who can provide the operational information on the volumes that are likely to have to be handled. This should be part of risk assessment.

3.11 During the EURIM-CESG event on the large-scale roll-out of biometrics it was pointed out that biometrics are extremely efficient at uniquely identifying white male Anglo-Saxon engineers aged 18-35. The biometrics of other groups are less stable than was thought,

3.12 There are problems with people who have eyes with different focal lengths and dark-skinned people don't have much contrast in the eye so it can't be processed. If you have astigmatism, if the eyes move, the camera has problems with them. If you can't see very well there can be also be problems. It would therefore be advantageous to collate data from large-scale systems that use biometrics. Experience has shown that none offer the 'gold standard' that many think can be achieved.

3.13 Moreover, data can be modified after collection and registration. Thus, we have recently learned that a proportion of those tasked to process illegal immigrants are themselves illegal immigrants! It was ever thus: in WWII, identity cards were available on the black market 48 hours before they were officially issued! So we do need routines for when things go wrong, based on the experience available from those who run large scale ID-systems as live applications.

3.14 So our message to Government should be that the system will not be perfect, but it will be better than the existing situation. IPS would almost certainly have its own database of lost and stolen passports used in projections of fraudulent use and forgery of ID cards, and how this might be

balanced by biometrics. There are several examples of large-scale biometric schemes (e.g. Nigeria and South Africa), but not in use for a civil application. Achieving high-quality identification through large-scale applications involves significant technical, organisational, social, legal and political issues, and the potential benefits are unpredictable.

3.15 There are obvious challenges associated with implementing the ID Cards scheme, and there are signs that IPS are beginning to recognise where the areas of difficulty are; EURIM should therefore identify particular areas where it can help, such as risk management, and make a positive contribution to the scheme.

3.16 The Science and Technology Select Committee enquiry into the Government's use of scientific evidence heard in oral evidence that for the use of ID cards, it is extremely selective. The Jill Dando Institute of Crime Science last year held a seminar on ID technology which included a report of research on the practical experience of the US online fingerprint systems. A major problem here was the number of false negatives, even though the systems were operated to much lower tolerances than in the UK, often exacerbated by poorly maintained equipment and other human-related causes. The online use of biometric identifiers involves interrogating the database – is this person known on this file? The JDI seminar had identified a lot of work on biometrics (offering both good and bad news vis a vis ID cards) for intelligence and evidential purposes (DW: the JDI mission is to 'change crime policy and practice'), but this does not appear to have been tapped.

3.17 Is there any evidence that the Government listens to and acts upon evidence available from organisations and individuals outside their preferred sources? EURIM had hosted 2 exercises recently for parliamentarians that had produced evidence – the ID-Entity panel and the CESG team of speakers on their experiences of large scale roll-out of biometrics systems. Had any of this been seriously considered by Government, and would they be likely to listen in the future? Should Government be widening its sources of information, especially in the consultation process, and is this a question for the STSC to put?

3.18 It was agreed that much more could be done in this area and that EURIM should produce a note on how this might be organised/achieved.

3.19 Much of the debate about ID cards over the past few years had been clouded by philosophical objections, and that it is only since the Act was passed that people have begun to address the practicalities of implementation and look at experience elsewhere in the world of operational, large scale biometric systems. **EURIM could help harvest this experience and collate the evidence to inform policy making.**

3.20 The United Arab Emirates (and Malaysia, Brunei and Oman) have recently adopted national ID smart cards using fingerprint technology. In the Sultanate of Oman, a smart card-based citizen ID programme has been deployed using the "ResIDent" smart ID card system from Gemplus, and fingerprint technology by biometrics vendor Sagem. The system helps government and citizens alike. The government is able to enhance its identification processes, improve its infrastructure, modernise its national registry system, increase homeland security and provide better quality services to citizens. Cardholders, meanwhile, can identify themselves electronically.

3.21 In the UAE, a nationwide ID programme using Java Card-based technology from Gemplus and Sagem's AFIS technology has been launched. The scheme has more than 2 million multi-application biometrics-based Smart Cards rolled out that will combine ID with driving licence, border control and emergency medical data. An iris system that filters out the effect of contact lenses, glasses and eyelashes, has made some 50bn live comparisons in the UAE, where it is used to check all visitors against people barred from re-entering the country (mostly immigrant workers from the Subcontinent, not white Anglo-Saxon engineers).

3.22 However, in the above example, those that the system fails to match are allowed through. False negatives are a significant problem for most systems. We therefore need to look at the evidence from practical experience with operational systems, and identify useful case studies, and we need to use this evidence to gain and convey an understanding of what it is reasonable to expect biometrics-based systems to deliver, rather than promote scare-stories. The availability of funding and improving technology, together with the transfer of risk to the private sector, suggested that complacency might present the greatest danger.

3.23 Some felt that IPS did not have a true understanding of the outcomes, or how they will manage and optimize those outcomes. This might seem simplistic, but trying to understand the ROI model requires developing an understanding and a visualisation of what will happen in the public and private sector, so that the correct decisions can be taken. The danger of the present thinking is that they will do as the politicians bid. It was also doubted from the presentation that citizen-centricity was driving the policy: it appears rather to have been added as an afterthought, rather than being central to the business plan. Perhaps Government should be more honest about what it is trying to achieve through the ID card.

3.24 Outcomes could probably be quantified financially: there are significant dangers and costs associated with the misuse of identity. Quantifying the outcomes would provide a basis for evaluating costs, while estimating to what extent levels of fraud would be controlled by the measures planned would better provide for the realisation of the benefits expected. Biometrics will improve the situation, but cannot be a panacea.

3.25 It should be noted that the ID Cards system would not be used as a biometric search: a card check tests the biometric of the person transacting against the NIR, it does not try to find out who the person is. The checks would test the validity of the ID card and that the person presenting it was the person named on the NIR. The only time a biometric search is undertaken is at the time of application; a collection of checks are available, and the biometric is just one of them. This is the most important step in the process; the system would not allow the duplication of an individual's biometrics in another record.

3.26 There is a hierarchy of circumstances of use depending on the level of security required. It was noted that SPs, not the IPS, are responsible for the authentication services. It is important to keep separate authentication from the quality of the credential in terms of setting expectations of the value of the data, because if an authentication fails, does the credential get blamed, or the authentication process?

3.27 In operational terms, the issue is how rapidly and reliably can the overall system be expected to perform in practice, given that spoofing of an ID card and/or biometrics will almost certainly be fairly readily achievable. The registration process can also generate a collection of synonyms that can then be checked against benefit claims and lead to very significant savings – but this may not be openly acknowledged.

3.28 While the Government appeared to have understood the business case for the ID card needed to be made around administrative efficiency and tackling fraud, they may have been unwilling to make that case because of opposition and publicity generated by civil libertarians. However, biometric technology is changing rapidly, and new systems are being tested.

A new interactive European Biometrics Centre of Excellence in Brussels is designed to showcase advanced identity management solutions to customers and illustrate potential real-life examples of biometrics technology. These range from cutting edge e-ID card and passport technology to 3D facial, electronic iris and finger print recognition. The Biometrics CoE presents opportunities to test the latest biometrics solutions and debate issues with leading experts.

3.29 Scare stories have a value too – as in the case of skewed distributions of errors, which need to be understood. Looking at balancing risk and risk management, this should not be confined to the system - there are also possible problems downstream. While this would be difficult to tackle, it should not be ignored.

3.30 It was pointed out that the majority of issues raised in the NAO report on the UKPS passport problems of 1998 were around business processes; the IT system itself did not fail. The faults lay with lack of training, introduction of child passports, rolling out offices in pairs instead of singly etc. There are many exceptions and problems with the performance of the application processes and getting ID cards through, which take up much of the time; the end to end business process itself is straightforward.

3.31 **A task for the PI Group might be to help the Government understand the likely problems that will be encountered, using evidence from the experience of other projects.** This should involve looking at how business processes might be configured to overcome problems and propose

solutions, perhaps based on corporates' actual examples. This would generate real figures around errors and outcomes without scaring them.

3.32 A tendency for the large suppliers to adopt a 'don't rock the boat' position when considering policy or large procurements in case this jeopardised their chances of winning a contract might be considered natural, but it should be acknowledged that failure to disclose doubts or give considered advice that goes against the current policy is likely to lead to yet more large IT project failures. However, there is a much stronger political dimension to ID cards, and much of the criticism is not directed towards the technology.

3.33 The ID cards system may stand or fall on its ability to deal with exceptions. Because of the large component of human involvement in the overall system, there was a danger that the operational culture would be dominated by the 'OSI' ('Oh sod it') principle! For a low-paid operative on their 1000th interview for a primary identity check with a non-English speaker, morale will be an immense problem. Research has consistently shown that the prime reason for project failure is that changing requirements during the set-up stages. Being a political project, the potential for changing requirements, technical or policy-related, in the ID cards system is even greater than usual. Risk management issues are therefore likely to be more significant than in any project thus far.

3.34 In terms of perceived value, a simple check akin to those in the financial services sector could be introduced for the benefit of the cardholder. Thus involved, cardholders can be alerted every time a credit card was used through an SMS sent containing the details of the transaction; this could be easily stopped if the transaction was fraudulent.

3.35 How does the health record and biographical footprint used in the NHS Connecting for Health (CfH) programme compare with the ID cards database? Are there different approaches to different elements of the respective user communities, including dissenters? There are proposals to produce an ID card in the NHS. **It would be important for the Government to understand the difference** in that IPS has been tasked to set up core information, the use of which should arguably not be regarded as part of the ID cards scheme but part of the processes of each department to use the information on the ID card. This makes it very different to the NHS where all the information is available for authorised access.

3.36 The Group wondered what opportunity EURIM might have to engage directly with IPS. Do we know what IPS already knows and what they do not know? How do we get our message to IPS? Legislative progress and attempts at procurement exercises had been subject to political disagreements. A number of factors had held up the process, including change of personnel at civil service and political levels. . A review is also in progress and a report is expected on 4 July.

3.38 It is possible to identify 3 strands of activity in the IPS:

- the e-borders programme
- ID Cards
- Renewal of the IPS passport support contract

These strands could be bound together in a different way, and reconfiguring them would be likely to delay any procurement exercise until the autumn.

3.39 Some members are impressed by the level of knowledge of staff at IPS, and the amount and quality of the research. However, this did not preclude constructive criticism from outside, and system benefit might be a case in point. The question is how best could EURIM help?

3.40 It is important not duplicate what is being done elsewhere, and we should also consider what EURIM can do as opposed to what Intellect might do as a collective exercise on behalf of suppliers. What appears to be missing are examples of user experience of big organisations who have operated systems over a number of years, the processes, error rates etc around them, how they deal with bad publicity when things go wrong, and who bears the blame. Intellect has set up a working group to take on board the technology issues; it would not look at the wider political issues, nor the reasons for and the implications of failure.

3.41 Tapping the experiences of the financial sector in dealing with identity management and identity fraud, and using this and other sources to develop a risk management strategy, might be a very useful exercise. However, no representatives of such organisations were present, and in any

case some of those with the most relevant experience might be reluctant to divulge information, because remuneration terms with IPS for identity services were part of their mainstream commercial operations. A solution might be to have suppliers to the financial sector organisations approach their own contacts to help persuade them that this would be a valid exercise for the common good.

3.42 The PI Group might accept offers from BT and Vodafone of their experience in large-scale IM projects and profiling of large numbers of 'transaction footprints', which hold many potential lessons for ID cards. The people involved with the Royal Mail's most accurate files (those used for the postman's rounds and associated quality control and security checks) appear not to have been consulted by the IPS. Moreover, no-one had so far satisfactorily resolved the issue of people having more than one address and/or no permanent address – churn rates of 400% per annum and more were common in City Centre wards.

3.43 It was agreed that EURIM should invite IPS to address the PI Group at a time of its choosing, so that we know more of their thinking and evidence base. In the meantime, EURIM should position itself as a 'critical friend' of the IPS, focus on those issues where it could make a constructive contribution (e.g. how known problem areas have been addressed by others) and provide case studies of operator and user experience of large-scale biometrics systems and identity management to reduce errors and uncertainty, deal with exceptions and manage risk.

4. Progress report for the Showcase

4.1 Arrangements for the Showcase were progressing well, with 16 exhibitors now that BT had joined to display their URU voice recognition system. A draft floor plan of stand allocations had been drawn up as a guide for exhibitors setting up, but this was necessarily flexible.

4. Date of next meeting

4.1 It was agreed that the next meeting of the Group would be held some time after 16 July.