EURIM Status Report

E-Crime / Personal Identity

Citizen or Subject?

How Far Do We Control Our Own Identities?

July 2004

Foreword

This report is the culmination of an intensive consultation process that commenced in September 2003 and involved a wide representation of EURIM members. I was pleased to have been invited to chair the group and would like to thank those individuals that gave their time and input to this study.

The focus of the study was to enable positive steps to be taken that would move the Personal Identity agenda forward. I believe that this report provides such a platform.

The results of this study have provided positive feedback, some of which is reflected below.

The study group will now determine how to take the main key issues forward and, in doing so, make a practical contribution benefiting the individual, the service provider and UK PLC.

Jim Lound
Product Director – Experian
Chair – EURIM Personal Identity Study

"I do support your purpose and despite some concerns I think it is worth saying that any research in this area is worthwhile and it is illuminating to have a broader perspective that a joint public / private sector initiative bring".

Richard Kitchen
Chief Investigation Officer, DWP.

"Identity theft is rife. Individuals and organisations need to ensure that they know who they are dealing with and be assured that a person is entitled to the services, benefits or goods they are receiving or making claim to. Being able to validate and verify identities with a high degree of confidence is critical to UK PLC".

John Baker
CIPFA – Better Governance Forum

"From the consumer's perspective, to be able to utilise their personal identity attributes to attain a quicker, more convenient and effective service from both the private and public sectors must be a goal worth attaining, provided this is achieved in a controlled and accountable manner enabled through their positive consent. Combine this with the potential to reduce identity fraud, the prospects then become even more attractive"

Terry Duddy
Chief Executive, Argos

1. Introduction

The issues of Personal Identity are central to the growth of e-commerce, the modernisation of government and the fight against computer assisted crime. There are a large number of overlapping initiatives, public and private, local, regional, central and international (see appendix). There is also much confusion as to which of these are intended to be linked and, if so, how. Objectives, priorities and timescales, let alone funding, legal frameworks and target audiences vary.

In April 2004 the draft legislation associated with the National ID Card was published for consultation. This Status Report is not specifically about the National ID Card since the issues go beyond those covered in the proposed legislation and some may need attention well within the currently envisaged timescales.

With regards to the issues of personal identity and data sharing there are clearly two distinct models operating in the UK.

One is based on the assumption that the informed consent of the customer/citizen can and should "drive" the process and that sharing and processing should take place in accordance with those wishes.

The other is based on the assumption that opportunities for genuine informed consent are rare, or are not relevant in the public sector, and that the process must therefore be controlled by statute and regulation.

The real world is a mix of both and in a democratic society which believes in choice we should be seeking to increase opportunities for informed consent while ensuring that there is effective governance, monitored by independent third parties where informed consent is not a realistic option, including because of lack of genuine choice as well as statutory powers.

The EURIM Personal Identity Group has been tasked to: *try to secure political, professional and commercial consensus on the main personal identity and data sharing policy initiatives necessary to enable UK organisations, public and private, to better serve their customers/citizens while greatly reducing opportunities for abuse and fraud.*

The Group suggests that the objectives of such policy initiatives should be to:

- reduce opportunities for the abuse of personal data, including the impact of fraud based on impersonation or fictional (developed) identities;
- to protect individuals' privacy, in particular by protecting them from unfair, excessive or irrelevant data gathering;
- ensure legitimate users have access to relevant data where the individual voluntarily gives consent, plus that available to them under statutory (e.g. law enforcement) powers;
- facilitate improvements in customer/citizen service (choice, accuracy, speed, convenience, effort etc.);
- improve confidence and satisfaction, enhancing accuracy, with reasonable cost (whether as consumer or taxpayer), confidentiality (as appropriate) and reliability of service
- stimulate the development of attractive and commercially viable UK-based products and services that meet the needs of the individual, industry, commerce and government.

In scoping its terms of reference the group has defined personal identity information as that data which contributes towards:

- the validation of the identity – e.g. "does John Smith exist?";
- the verification of the identity – e.g. "is this John Smith?";
- the assessment of eligibility to obtain the product or service e.g. credit worthiness, need, medical or criminal status;

- the ability for the individual to establish their rights to benefits and services (especially in the public sector);
- the establishment of audit trails for both the sources of personal identity information (including updates) and the access requests (including identity and other bona fides of those making the request).

2. Summary of Main Issues to be Addressed

There are eight key issues that are deemed to be pivotal to the ability to achieve the mission statement and realise the stated objectives.

Co-ordinating Role – There is an immediate and urgent requirement for a body (new or existing) to bring together the disparate national and regulatory initiatives (see Appendix) involving Personal Identity to ensure that a coherent strategy and a consistent approach is applied (not necessarily with an objective to create one big monolithic project).

Buy In – to gain a collective commitment from local and central government departments and the private sector to adopt consent driven data sharing models where practical, through demonstrating the benefits associated with improvements in the effectiveness and efficiency of the service delivery providing improved customer service to the individual.

Data Sharing – There is a need to lift the barriers that prevent effective data sharing taking place. Revised legislation is needed to allow the wishes of the individual to share their data to be carried out where currently this is not allowed. The National ID Card draft legislation provides for data sharing but only in the context of establishing the level of confidence in the identity of the individual at the registration stage.

Interoperability – to ensure that individuals, if they wish, can re-use their proofs of identity (not restricted to the National ID Card) with as many service providers as will accept them, allowing service providers to be confident that identity tokens have been issued under robust conditions, to recognised authentication levels and utilising suitable methods of token holder verification e.g. PIN.

Liability – to protect token issuers from undue liability from reliant parties who use their tokens where there is no pre-arranged formal contract whilst recognising the potential for bilateral contracts established at the point of transaction for the purposes of the transaction only e.g. authorisation of the token to a central record maintained by the issuer of the token.

Personal Identity Kite Mark – whereby service providers adopt a pre-defined standard (bespoke to the service provider or generic) that specifies, for a particular transaction type, the breadth and depth of data that will be accessed and allows for the individual to be notified of an access to their personal data. Conformance to the standard could be recognised through the use of a Personal Identity Kite Mark visible to and readily recognised by the individual.

Legitimate Aliases – where individuals wish to use alternative names there is a need to make the process more formal to enforce registration of the new name with the ability to link the individual's aliases and create the ability to provide a (consent driven) single view of the individual’s data associated with the aliases. It is recognised that certain services benefit from offering anonymity and this is consistent with the consent driven model.

Enforcement Processes – whereby there are realistic legal frameworks, investigatory processes and penalties with regard to the creation/access/falsification of records to aid fraud and impersonation as well as for the creation/possession of false identity tokens (including electronic identity "tokens").

3. References to the National ID Card Draft Legislation

This section is intended not to provide a complete review of the draft legislation but to identify references that may have a bearing on this Personal Identity (PI) study.

3.1 Data Sharing

The draft legislation recognises the benefits of data sharing and has provided for the ability to access relevant data sources of PI related data in order to undertake background checks more effectively. It does not appear that this will require any consent from the individual to allow this to happen. Whilst this is a clear sign that data sharing is recognised as a benefit, it will only apply to those checks associated with the registration stage.

However, it would appear that some limited data sharing of the National ID data might take place as part of the ID verification process, as reference is made to providing confirmation of residency status. This information could, for example, confirm entitlement for services based upon nationality.

Therefore, there is some provision to increase data sharing but in the context of this PI study the requirement is much broader.

From a EURIM perspective it is clear that there is support for data sharing and it is proposed that EURIM continues progressing the data sharing agenda with the DCA, OIC, FSA and the Home Office.

3.2 Entitlement and Eligibility

In the context of the ID Card, the draft legislation acknowledges that identity naturally extends to entitlement and eligibility as per the example in 3.1 above.

This PI study considers that PI data is not just about identity but also the attributes used to establish entitlement and eligibility for products and services.

3.3 Choice

In relation to choice and, in particular, the taking of a biometric, the private sector members of the EURIM PI group suggest that the individual should have a degree of choice in the method of verification of the token holder. This would clearly extend to those individuals who could not physically provide a biometric.

However, within the ID Card legislation, an individual who cannot physically provide a biometric will still receive the 'standard' ID Card. For everyone else there will be no choice but to provide the biometric.

A three-tier card approach for example, whereby the highest level contains a biometric, PIN and photograph, the second level a PIN and photograph and the third level a photograph only, would have provided choice.

It is recognised that this would have increased the reliance on the non biometric data to prevent multiple registrations by the same person using different names.

4. Circle of Trust

The concept of the ‘Circle of Trust’is based on a consent driven model that allows the individual to give their consent for a Service Provider to the Individual (SPI) to access their personal data in relation to the provision of a service or product.

Examples of SPIs include the Department for Work & Pensions, local authority housing benefit departments, local transport organisations, airport authorities and, in the private sector, issuers of credit, debit, age, loyalty and travel cards.

Other examples would include organisations intermediating government services. Additionally, SPIs may delegate authority for specific services to other organisations to act on their behalf.

The SPI needs to have confidence in the identity of the person they are dealing with and have confidence that they are able to see the ‘full picture’ associated with an individual that it is complete, up to date and accurate and can be obtained in a timely fashion.

The SPI should be able to utilise their own data, data obtained directly from their partners and data procured through regulated data brokers (such as the already regulated credit reference agencies).

The data broker needs to have confidence that the SPI is a bona fide organisation and is requesting data that, in terms of breadth and depth, is consistent with the type of transaction being processed.

Both the individual and the SPI need to establish a level of trust in the Principal Data Broker (PDB) and the Secondary Data Broker (SDB).

In order to help establish these levels of trust there is a need for the SPI, PDB and SDB organisations to employ appropriate data security standards, particularly in relation to ensuring that their members of staff do not abuse their ability to access the personal identity data.

The ‘Circle of Trust’is completed through the individual electing to receive, as an option, notification of access to their data from the data broker and having the opportunity to look at a copy of their personal data utilised as part of the transaction processed.

The foundations of the ‘Circle of Trust’ include:

4.1 Individual Choice

The individual should have a personal choice regarding the method by which they present their Personal Identity attributes to an SPI, thereby allowing the SPI to be satisfied that the individual exists, it is the individual presenting themselves and demonstrates eligibility for the product or service requested.

These methods can be categorised as:

1. The individual presents physical documentary evidence to each SPI they interact with.

2. The individual consents to the SPI utilising electronic data obtained from external sources to create a virtual electronic token that can be utilised immediately by the SPI.

3. The methods utilised in 1 & 2 can contribute towards the creation of a physical token that can be re-used with the issuing SPI and with third party SPIs.

The choices below relate to the means by which the individual identifies themselves to the SPI, the level of authentication attained and the means by which they ‘attach’themselves to a token.

At the opposite ends of the spectrum there would be those:

- individuals who would like to carry just one identity token that allows them to conduct as much business as possible with as many SPIs as possible;
  vs
- individuals who would like to carry or have access to a whole range of different tokens to avoid having ‘all their eggs in one basket’, with the risk of serious inconvenience if they lose a high value ID token during an otherwise "trivial" loss street robbery or bag snatch.

- individuals who would wish to attain the highest level of authentication possible in order to be prepared for any situation (e.g. frequent flyers) and are willing to submit themselves to a rigorous authentication process;
  vs:
- individuals who merely want the minimum level of authentication because they do not perceive they have any need for a higher level (e.g. limited to concessional transport and library services) and do not wish to be subjected to a rigorous authentication process.

- individuals who are prepared to go to their perceived highest level of strength of attachment e.g. employing biometric technology;
  vs:
- individuals who are content with carrying a plastic card whereby physical possession is perceived to be an adequate measure.

Whilst choice is an honourable goal, the reality is that the acquisition of goods and services that carry higher levels of risk to the SPI (and to the individual if their identity is compromised), may require the individual to submit themselves to rigorous identity authentication processes either at the point of transaction or in advance (in order to obtain a re-usable and/or multi-function identity token).

It is therefore vital that the individual makes an informed choice, understanding the impact their choice may have on obtaining the optimum service from the SPIs they will interact with.

It is important to prevent individuals appearing to be second class citizens by virtue of not being able physically to provide a biometric due to some form of disability. This sentiment is reflected in the draft ID Card legislation.

Additionally, an individual should not be forced into owning a ‘high value’token when there is a perceived risk of coercion associated with their day to day personal business.

4.2 Interoperability

Interoperability is a pre-requisite to allow an individual’s choice of token to be re-used across more than one SPI, enabling the features inherent within the token to be utilised (e.g. identity confirmation, payment processing).

Interoperability is a pre-requisite if the SPI wishes to realise the benefits of utilising an individual’s existing third party token thereby enhancing customer service through the provision of a more efficient and effective process and perhaps even removing the need to issue its own token.

For interoperability to work in relation to personal identity, the SPI would need to establish for each transaction type their minimum requirements in relation to:

- Authentication level – e.g. HMG minimum standards – levels 0, 1, 2, 3.
- Recognised accreditation standard – tScheme, Identrus
- Type of token – virtual, card, smartcard, digital certificate
- Token authentication – central (i.e. checking back to source data), local
- Token holder verification – possession, photo, PIN, password, keyword, biometric.

NB: not all these attributes can logically be combined (e.g. mere possession of a digital certificate would not be a valid method of verification) and therefore the true number of combinations is limited but potentially still large. This is an issue that needs to be addressed as a multitude of possible combinations will cause confusion.

The SPI will need to identify to the individual which tokens they will accept (hence the need to limit the number of options).

The ID Card draft legislation recognises that the ID Card may carry more than one method of token holder verification.

The SPI will need to be able to readily identify whether the token offered by the individual is acceptable.

The SPI will need to be able to readily identify the components of the token either electronically and/or visually in relation to the:
- authentication level
- accreditation standard
- token authentication
- token holder verification.

In order to utilise the token the SPI will have to:
- take information from the token;
- initiate the local or central token authentication;
- capture the means of token holder verification as appropriate e.g. PIN.

To allow interoperability a flexible infrastructure must be established within the UK that will allow PI to work in a multi-channel environment. There is a range of standards in the marketplace. These standards must be harnessed in order to create the infrastructure.

4.3 Consent

The ‘Circle of Trust’model is based upon the individual consenting to the SPI’s utilisation of the attributes of the individual’s personal identity. Provision of consent will enable the SPI to have access to a wider set of data.

It is recognised that the question of consent in the context of a monopoly provider of benefit is an issue. The customer’s need for benefit makes it impossible to incorporate consent into the provision of the benefit; any consent given would be seen as having been given under duress and therefore invalid.

For the SPI to secure consent it will be necessary for the individual to be confident that the SPI will only access the breadth and depth of data appropriate to the transaction being undertaken. To expect that the individual would have a desire to understand the intricacies of this data and to specifically grant permission

to access each data item every time the transaction takes place is both unrealistic and impractical.

An alternative is for the individual to give consent on the basis of understanding the meaning of the prestigious PI Kite Mark and being made aware that their chosen SPI complies with its requirements. This implies a successful and on-going publicity campaign.

Such public recognition needs to be so strong that an SPI not carrying the Kite Mark would be seriously disadvantaged in terms of individuals having to demand it or individuals seeking out an alternative service provider.

The PI Kite Mark would confirm that the SPI is following a pre-defined (generic or bespoke) standard associated with the access and utilisation of an individual's PI attributes. The creation of these standards would be assessed by an independent, consumer / citizen focussed body with oversight from a well trusted and respected organisation, for example the Citizens Advice Bureau or tScheme.

An individual would have the right to see a copy of the standard for a specific transaction in order to be able to review the detail of the data requested and utilised.

The overall PI Kite Mark process would require formal governance to manage and police the scheme – implying the creation of some form of Data Services Authority (DSA). The role of the DSA could be undertaken by an existing body.

There would be a need to ensure that such a third party is indeed independent, effective and commands public confidence. This would entail adequate levels of funding, public accountability and a clear division of labour between regulation and policing.

For this to be successful it requires 'people power' to demand it on the one hand and on the other requires the accreditation process and governance regime to be rapid-response, efficient and cost effective and not overburden the SPIs.

A key issue will be to establish an acceptable and compliant method of allowing the appropriate PI data to be 'in place' prior to consent in order to allow the data to be immediately released when consent is given.

4.4 Data Acquisition and Sharing

There is a need for a greater awareness and understanding of what data sharing entails and how it benefits individuals and society as a whole, making a distinction between what could be termed 'administrative'data and fraud data.

There is a need for legislation to 'release'data currently imprisoned even with the individual's consent to share. One impediment is that data given to a Government Department in confidence cannot currently be shared even with consent.

The ID Card draft legislation proposes data sharing but only in the context of the background checks undertaken as part of the registration process and without the need for express consent.

An SPI has a number of options in relation to the acquisition of data; i.e. it can use data:

- owned by the SPI;
- obtained from its partners;
- obtained from the SPI's principal data broker.

An SPI could elect to procure the data itself from all three sources and thereby operate as its own data broker.

Alternatively the data broker could supply the SPI with data:

- owned by the SPI, held and supplied by the data broker acting as a data processor;
- owned by a partner of the SPI, held and supplied by the data broker acting as a data processor;
- owned by the data broker as a data controller;
- obtained from a secondary data broker.

It is recognised that, for example, the DWP is constrained by law from disclosing to persons outside the Department whether or not a customer of theirs is on benefit. This currently has an impact on the extent to which data sharing could take place and under what conditions.

Should, however, the individual be able to request DWP to share such information, for example to confirm that they are in receipt of benefits and therefore have an income stream or that they should be given access to special prices/programmes which may have been agreed locally or with the private sector?

An existing example of a Principal Data Broker (PDB) would be a credit reference agency operating in the financial services sector.

In these circumstances the PDB allows data sharing to take place without the need for individual financial service providers directly having to service data access requests from the multitude of other service providers wishing to assemble a single view of the applicant's PI data.

The assembled single view is made up of data obtained from many reputable sources and it is this breadth of data emanating from different organisations, coupled with its quality and depth, that contributes significantly towards the data's strengths. It is essential that only data relevant to the individual and the associated transaction is utilised within this single view. Fundamentally, this strength of data needs to be inherent within any single view of PI data.

This type of benefit would be reflected in other sectors. For example if the UK Passport Service wanted to offer a Passport Verification Service then rather than having to cope with thousands of different organisations trying to connect to the UKPS databases, the services of one or more PDBs could be used to provide conduits into the UKPS. The onus would then be on the PDB to establish connectivity with the thousands of organisations, some of which may already link into the PDB for other purposes.

The PDB would be responsible for ensuring that it provided the individual's PI data only to bona fide SPIs and appropriate to the type of transaction being processed. The SPI may take advantage of other added value services offered by the PDB that may directly contribute towards the processing of the transaction.

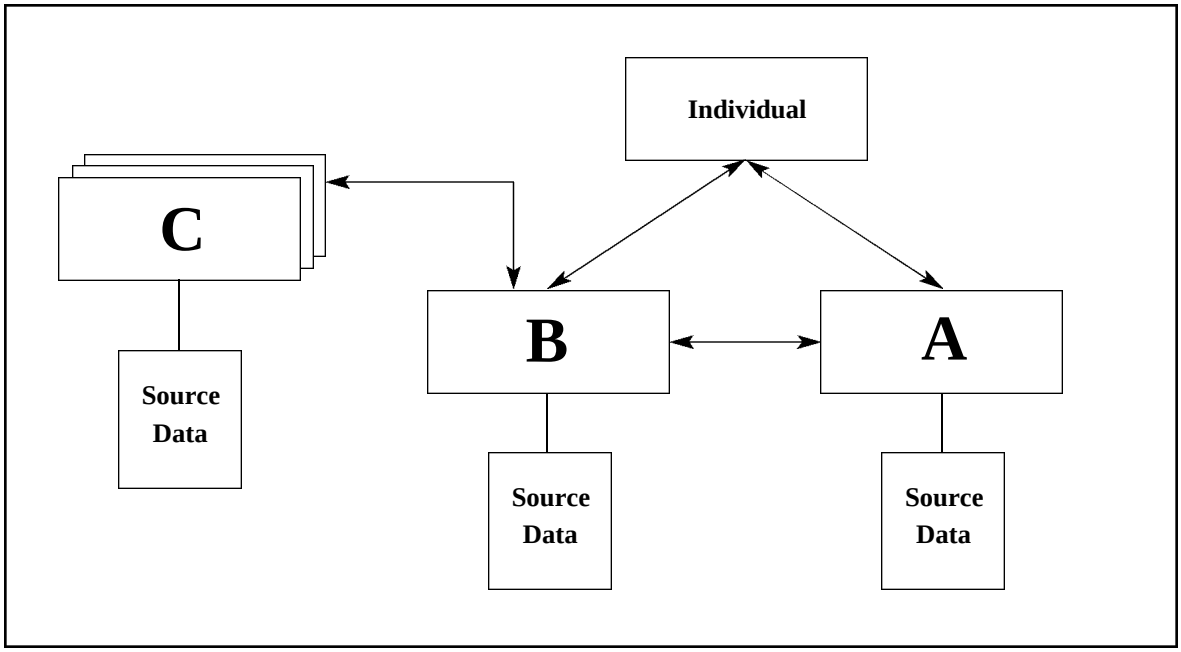
The PDB may elect to obtain some of its data from Secondary Data Brokers (SDB), some of whom could be Principal Data Brokers to other SPIs.

The PDB could be rewarded for services on a per transaction fee by the SPI. The PDB would be responsible for rewarding the SDB.

The PDB would, where the individual has elected to be advised of accesses to their PI data, provide the notification via the individual's channel of choice. The individual may, as an example, elect to receive notifications only when a new relationship is established or when a new transaction type is identified.

It is envisaged that the PDBs would come under the remit of the Data Services Authority. The DSA would ensure that the PI data is procured, maintained and processed in a compliant, efficient and effective manner. There should be proportionate penalties for any mis-use of the data. The ID Card draft legislation proposes such penalties.

Examples of the data sharing flow within the 'Circle of Trust'



Scenario 1 – Financial Services – application for credit
A = Bank ABC
B = Credit Reference Agency
C = Third Party Data Supplier

The individual, applying for credit, gives their consent to 'A' to allow the bank to access their credit data held by the Credit Reference Agency 'B'.

'A' requests the data from 'B'. 'B'checks the credentials of 'A' to ensure that it is a bona fide requestor. 'B'checks the type of transaction associated with the request. 'B'determines the level of data that 'A' is eligible to receive.

An element of the data that 'A' is eligible to receive is held by a third party 'C'. 'B' obtains the data from 'C'.

'B'assembles all the data and returns it to 'A' to a pre-defined standard.

The data held by the credit reference agency could include the bank's own data for use by the bank e.g. details of the individual's savings accounts held with the bank.

As part of the transaction the credit reference agency can provide added value services e.g. credit risk assessment, identity authentication check, application of the bank's own policy rules to define, for example, the credit limit to be offered.

The complete transaction from the initial request from the bank to the delivery of the data back to the bank by the credit reference agency is undertaken, on-line real time, within seconds.

If previously registered for the service, the individual can receive a notification from the credit reference agency that their credit data has been accessed.

Under the Consumer Credit Act the individual can request a copy of their credit data from the credit reference agency.

Scenario 2 – Passport Verification Service – verification of an individual's passport details

A = A service provider using a passport as part of their identity authentication process
e.g. an airport authority
B = Principal Data Broker
C = UK Passport Service

The individual presents their passport to the airport member of staff in order to check their identity credentials.

Utilising an on-line service provided by the Principal Data Broker 'B'on behalf of UKPS, the member of staff representing 'A' data captures specific details of the passport e.g. passport number, name.

'B' sends a data request to the UKPS 'C'to check the validity of the details captured by 'A'. The results of the check are returned to 'B' who in turn forwards them on to 'A'. 'A' utilises these results as part of their assessment of the individual.

'B'may provide added value services to 'A' in relation to the strength of confidence in the validity of the identity (i.e. that 'John Smith exists') and the verification of the identity(i.e. that 'this is John Smith presenting the passport').

Scenario 3 – Department for Work & Pensions - Benefit Application

A = DWP
B = Principal Data Broker
C = Inland Revenue

The individual applies for a DWP benefit. The individual gives their consent for their personal data to be accessed. The DWPapplication carries the PI Kite Mark.

'A' sends a request to 'B'. This request fulfils two objectives. Firstly to utilise the data held by 'B' to establish a virtual identity token to the appropriate authentication level, establishing the required level of confidence in the validity and verification of the identity for use in this benefit application. Secondly for 'B' to acquire on behalf of 'A', from the Inland Revenue, specific data that will subsequently be used in the benefit assessment.

The returned data will be utilised with the DWP's own data to contribute towards the assessment. The DWP may acquire data from other third party sources.

'B' may provide added value services to the DWP in terms of, for example, contributing towards the assessment of eligibility, utilising and applying the DWP's own rules.

4.5 Personal ID Management

The components of Personal ID Management include:

Notifications – As already discussed, the PDBs should provide the facility for individuals to opt in to a service that provides a notification via the individual's preferred channel, when pre-defined attributes of their PI data change. For example, when the data access request emanates from a new SPI or from an existing SPI but relates to a new type of transaction.

Access – The individual should be able to view their own PI data in order to be aware of the data values used by the SPI and thereby identify any perceived anomalies. The individual should be able to access this data via the PDB. This would be a specific type of data access in addition to the individual's right of subject access under the Data Protection Act. Clearly the PDB would need to employ robust identity authentication routines to ensure that the PI data are not accessed by an unauthorised person (e.g. a potential identity impersonation fraudster).

Recourse – When the individual identifies an anomaly, this would be reported to the PDB, resulting in the offending data item being 'suspended'with a 'notice of suspension'. The individual would resolve the offending data item with the originating organisation via the PDB.

Legitimate Aliases – where individuals wish to use alternative names there is a need to make the process more formal to enforce registration of the new name, with the ability to link the individual's aliases and create the ability to provide a (consent driven) single view of the individual's data associated with the aliases. It is recognised that certain services benefit from offering anonymity and this is consistent with the consent driven model.

Accountability – in addition to the SPIs and PDBs, the individual themselves have an obligation to protect their own identity through taking steps to ensure that, as far as they can, they:

- deal only with bona fide organisations;
- do not reveal unnecessary amounts of personal data;
- do not compromise or reveal security measures e.g. PIN;
- securely dispose of unwanted documents containing personal details;
- take the opportunity to review their PI data regularly;
- elect to receive notifications of accesses to their own data.

Individuals need to be educated in PI awareness.

Data Services Authority – it is envisaged that Personal Identity Management would come under the remit of the DSA.

4.6 Benefits

Individual – The individual will be able to exercise more control over their PI data and be aware of how their information is being used through the consent process, the ability to receive notifications of access and being able to access a copy of their PI data.

The PI Kite Mark will give confidence to the individual that only the appropriate levels of data will be accessed for a particular transaction.

Personal choice in the area of identity tokens will provide reassurance to those that do not wish to put 'all their eggs in one basket'on the one hand but also allowing an individual to minimise the number of tokens and passwords etc, that they have to carry and remember. Individuals will be able to re-use existing tokens with third party SPIs.

Individuals will experience an improvement in the cost, speed, effectiveness, and efficiency of the service provision and be able to access their chosen service through a wider choice of channels selecting their own preferred method.

SPI – The SPI will be able to reduce their data acquisition and data processing costs through an efficient data sharing process. The service provision will be quicker and be less costly. The SPI will be able to utilise more cost effective delivery channels.

The adoption of the PI Kite scheme will make the SPI's service provision more prestigious.

The SPI will have more confidence in the identity of the person they are dealing with.

The SPI can take advantage of third party identity tokens in the knowledge that they have been issued under robust conditions, conform to the appropriate authentication standards and have a secure method of token holder verification.

The SPI will have a more effective method of obtaining a single view of their customer. The SPI will have more confidence that the single view is comprehensive and thereby be in a position to manage the risk of service provision more effectively, resulting in additional financial benefits.

UK PLC – Overall levels of PI related fraud will, it is hoped, be reduced within the UK.

Individuals will naturally want to carry their identity token(s) in order to benefit from the improvements in service and, potentially, from financial incentives (e.g. 'price'reductions). This will provide the carrot to encourage individuals to acquire a National ID Card rather than adopting the stick approach.

This will make a significant contribution towards enabling e-Government to work.

Public Services will be improved through reductions in cost, increased speed and convenience of delivery, extension of delivery channels, and the introduction of new and innovative products and services.

5. Further Considerations

Whilst the 'Circle of Trust'is based upon a consent driven model there are many situations where government departments and agencies (not just conventional law enforcement), have the legislative authority to demand information. Here there need to be explicit routines for public accountability for those routines where not only is consent not required but also where revealing knowledge of the request (e.g. for law enforcement purposes) may itself be an offence (tipping off).

This problem has already occurred in the debate over the position of communications data under the Regulation of Investigatory Powers Act. That debate revealed widespread ignorance of the degree to which a wide range of government departments and agencies had legacy powers to demand and hold information with neither third party supervision nor public accountability.

It is believed that in moving such powers to fully regulated models, liberty groups that consider data sharing to be contrary to the interests of individuals, should see the benefit of extending the consent driven approach across public sector applications wherever practical and may even see a role in assisting the governance of the PI Kite Mark scheme. This is so even where the "consent" is "given" by those publicly accountable for the supervision of the process (e.g. the Interception Commissioner, perhaps with a much wider remit, visibility and resources).

The appendix shows a large number of PI related initiatives. It would appear that many of these initiatives are each likely to create new, unique, reference numbers (URNs) associated with the individual. The desirability of the proliferation of URNs versus the benefits of having an individual's PI data connected to a single URN is a debate that needs to take place as a matter of urgency.

It can be argued that the confusion caused by current proliferation gives more opportunities for criminal exploitation than the opportunities for additional security offered by compartmentalisation.

To enable data to be 'instantly'available when the individual provides their consent will require data to be already 'in place'ready for retrieval and assimilation and delivery to the SPI. This may generate concern over the potential for inappropriate use and needs further consideration.

The ID Card draft legislation recognises the value of electronic data as a means of validating and verifying an individual's identity. This is seen as a positive step as it recognises the weaknesses of documentary evidence as an identity measure and the disadvantages in terms of costs and customer service.

For example, the Home Office leaflet to employers on 'Amendments to document checks under section 8 of the Asylum & Immigration Act 1996'which came into force on 1st May 2004, refers to the extent to which documents containing NINOs should be relied upon.

Additionally, in relation to Anti Money Laundering controls, an example of the process for confirming identity when opening a current account is where documentary evidence is required to be presented to and countersigned at a Post Office.

6. Next Steps

The Personal Identity and Data Sharing group should be tasked to consider the following issues:

- how to allow the express consent of the individual to open up data sharing, perhaps over-riding current legislative/organisational barriers if appropriate;
- the third party governance of statutory data sharing (e.g. extension of the "Regulation of Investigatory Powers" to cover legacy investigatory powers and not just communications and covert surveillance);
- the linkages between data sharing and personal identity initiatives e.g. CIP and National ID databases (Medical Records, NINO, Tax , Child protection etc.);
- the need for a possible overarching strategy relating to the growing number of personal identity related initiatives (public and private). Does the proliferation of public sector "unique reference numbers" give additional protection and avoid dis-economies of scale or an expensive and wasteful illusion of protection?
- the desirability and/or means of co-ordinating, managing, rationalising the many initiatives, given that different applications may benefit from different approaches;
- enforcement, including the vetting and monitoring of staff and contractors (permanent or temporary) at every level and penalties for abuse, so as to increase confidence in that personal data is indeed handled in accordance with agreed procedures and that abuses will be deterred, detected and punished;

- assessment of the risks and liabilities entailed with the various trust and governance models (current and proposed), how these vary with changing business requirements and technical processes and the effects of volume and required response time. This may well lead to a recommendation for the application of formal risk assessment procedures to public sector proposals;

- establishing a working group to create a ‘working’model for the ‘Circle of Trust’, incorporating a service provider and citizen representation in order to ‘test’the practical issues of what is being proposed;

The other main activity of the EURIM Personal Identity and Data Sharing group relates to the issues around the need for practical, application-oriented guidance to staff, both public and private, who need to distinguish between those with whom information can and should be shared (legal requirements, customer/citizen wishes etc.) and those with whom it should not.

---

7. Appendix – sources of further information

PI Related Initiatives / Reports / Research / Information

Initiatives

Acacia programme – national infrastructure of property addresses
http://www.ordnancesurvey.co.uk/oswebsite/media/news/2004/june/acacia.html

Deaths Register
http://www.computing.co.uk/News/1153565

Child Bill
http://www.publications.parliament.uk/pa/ld200304/ldbills/035/2004035.pdf
http://www.kablenet.com/kd.nsf/Frontpage/A9E31138A028463380256E4D00436973?OpenDocument

Directgov
http://ukonline.direct.gov.uk/Homepage/fs/en

Government Gateway
http://www.gateway.gov.uk/

Smart Cards
http://www.govtalk.gov.uk/policydocs/consult_subject.asp?topics=62&order=publishdate&I1.x=19&I1.y-9
http://www.scnf.org.uk/

Office of National Statistics - Modernising Civil Registration
http://www.statistics.gov.uk/registration/whitepaper/default.asp

DfES and LASocial Services - National Child Database
http://www.computerweekly.com/Article126324.htm

DfES – Connexions card – 16 to 19 year olds – monitor & reward attendance at a place of learning
http://www.capita.co.uk/TextOnly/Sustainability/Social/ConnexionsCard.htm

Citizen Card – Age verification card
http://www.citizencard.com/

Immigration & Nationality Directorate – IND card
http://www.ind.homeoffice.gov.uk/default.asp?PageId=3168

Criminal Justice Information Technology
http://www.cjit.gov.uk/bpm/index1.html

Criminal Records Bureau – Identity authentication
http://www.crb.gov.uk/downloads/Corp_and_bus_plan_2003-2004.pdf

UKPS
http://www.ukpa.gov.uk/identity.asp
http://www.ukpa.gov.uk/images/UKPS_plans_03-08.pdf
http://www.passport.gov.uk/news/news.asp?intElement=738
http://news.bbc.co.uk/1/hi/uk/3493388.stm

National Benefits Project – One stop shop

NHS – Access to medical records
http://www.nhsia.nhs.uk/text/pages/pr/06032001.asp
http://www.kablenet.com/kd.nsf/Frontpage/7D34F73108166EB180256E54003A374F?OpenDocument

Home Office – ID Card
http://www.homeoffice.gov.uk/comrace/identitycards/
http://www.computing.co.uk/news/1153041
http://www.computing.co.uk/news/1153044
http://www.computing.co.uk/News/1152725
http://www.kablenet.com/kd.nsf/Frontpage/2A04F82E5540EE0B80256E5500592935?OpenDocument
www.homeoffice.gov.uk/docs3/identitycardsconsult.pdf

Office of National Statistics - Citizen Information Project
http://www.statistics.gov.uk/registration/cip.asp

Security Industry Authority – Identity authentication
http://www.the-sia.org.uk/sia-at-a-glance/what-is-the-sia.asp

Reports & Research

EU FIDIS Network of Excellence
http://cybersecurity.jrc.es/pages/projectsfidis.htm

IDEA comments re: Performance & Innovation Unit Privacy & Data sharing Report
http://www.idea.gov.uk/transformation/piu-datasharing.pdf

Cabinet Office – Better use of personal data
http://www.strategy.gov.uk/output/page3897.asp

NCIS – Role of identity fraud underpinning serious and organised crime
http://www.ncis.gov.uk/briefing/270203.asp

Metropolitan Police – Exchange of information
http://www.met.police.uk/publications/crime_disorder/cad1.htm

Department for Constitutional Affairs – Data Sharing
http://www.dca.gov.uk/foi/sharing/index.htm
http://www.dca.gov.uk/foi/sharing/toolkit/infosharing.htm
http://www.dca.gov.uk/consult/datasharing/datashareresp.htm

The Electoral Fraud (Northern Ireland) Act 2002
http://www.ipf.co.uk/Governance/signpostview.asp?id=6066
http://www.electoralcommission.gov.uk/files/dms/ElectoralFraudActFinalpdf_112668891__E__N__S__W__.pdf

Bichard Enquiry
http://www.kablenet.com/kd.nsf/Frontpage/B21306AB71F3D5DF80256E53004108A2?OpenDocument
http://news.bbc.co.uk/1/hi/uk/3573509.stm
http://www.bichardinquiry.org.uk/

Information

NS&I – Money Laundering risk
http://www.timesonline.co.uk/article/0,,5-939844,00.html

California Office of Privacy Protection
http://www.privacy.ca.gov/cover/identitytheft.htm

No finger prints –no entry (into Chelmsford nightclub)
http://www.kablenet.com/kd.nsf/Frontpage/84B5BA72FE95E36D80256E1C0060A488?OpenDocument

Talbot House
Talbot Street
Nottingham
NG80 1TH
United Kingdom