Personal Data Services Model

Outline of possible standards-based approach

DRAFT FOR DISCUSSION

December 2006

Peter F Brown
Founder, Pensive

This particular printout is from a document that is **not currently stable** and is being updated on no particular schedule

Comments are welcome and should be sent to Peter F Brown at: peter@pensive.eu

File History

Date	Summary of evolution
26/09/2006	File created (FileID:134)
26/09/2006	Initial notes and outline
21/11/2006	Content and editing
26/11/2006	Comments and revisions
04/12/2006	Completed
05/12/2006	Released

Information Associations

Association Type	Value	Comment
IsRepresentationOf	eu.pensive:uid:0081	Document uid
HasEquivalentContent	eu.pensive:file:154	PDF version

Table of Contents

1 Introduction

This document is a first attempt to assess the desirability, feasibility and acceptability of developing and normalising a “Personal Data Services Model”.

It attempts to address the often very thorny issue of personal data management by firstly “unbundling” many assumptions and presumptions about what “personal data” actually means before going on to highlight the problems and issues involved when attempting to identify, authenticate, use and manage “personal data”.

It then looks at some common preoccupations regarding personal data privacy and public policy concerns before looking in detail at how a model for the encapsulation and servicing of personal data might be achieved that is consistent with political and social imperatives as well as data protection concerns.

2 Context

The wide range of assumptions about what constitutes personal data makes it difficult to establish a common model: all too often the creation, use and management of “personal data” is based exclusively on the needs of the particular process in hand. Current emphasis in interoperability is between systems managed by business and services and thus on how data can be most easily shunted between heterogeneous systems. When it comes to personal data, how those transactions take place should be centred on the needs of the citizen.

Even when the citizen does interface with electronic, web-based, services:

- Personal data is seem merely as a set of data, like many others, rather than something with intrinsic value that belongs to someone;
- information architecture is still based around needs of the service, not of the individual;
- service still manages and maintains the data on citizens;
- still multiple instances and overlaps in that data;

eGovernment should be about more than simply “digitising older paper-based processes.
Why then – in the domain of personal identity – is there still so much preoccupation with electronic identity ***cards*** rather than about identity ***management*** ? A “Personal Data Services Model” should attempt to build a model for identity and data management that goes beyond digitising paper.

- citizen has little direct access to or control over that data, its quality or its use;
- when data quality standards are used, there are often service or sector specific: multiple, conflicting and overlapping data standards exist and are used to manage citizen data based upon specific service - rather than citizen – needs;
- exchange of citizen data between services and agencies is often done without any mediation or control by the citizen;
- these exchanges still require substantial investment in harmonising exchange standards;
- increasingly, business-process driven systems use personal data as part of automated processes with little or no scope for the citizen to refuse that their data be used;
- data is rarely available beyond the bounds of an explicitly defined and established context
- there is no public-agreed standard by which citizens can assert their "personal electronic identity" (for example, beyond simple digital signature and encryption): standards exist but "authorities" are often associated with particular roles (a person can have a digital signature by the fact that they are, for example, an employee of a firm that has registration authority), rather than being available directly and authentically to the citizen.

3 Policy concerns

Politicians and public policy makers have so far bought into a scenario for identity management that is essentially little more that a digitized version of an essentially paper-based paradigm, that of the identity **card**. As such, the debate has often been conducted in an environment shaped by our understanding and acceptance of the limits of the physical ID card.

Legitimately voiced concerns about protection of privacy are often simplistically countered by arguments over security. Security services should be able to access and use data than in any other context would be considered private and confidential and often – as part of their mission – in a way that is unknown to the person(s) concerned. However, even those activities should be properly authorised, audited and accountable. Indeed, it is in the interests of those services themselves to be able to defend their actions (for example in a court of law).

Alongside heightened political concerns about electronic identity, there is increased public fear about the use and abuse of private data. As well as concerns about who has access to personal data and how they store, use and distribute it, there are questions about liability when data is wrong and/or misleading and the rights of citizens to legitimately withhold data when they believe it compromises their rights to privacy.

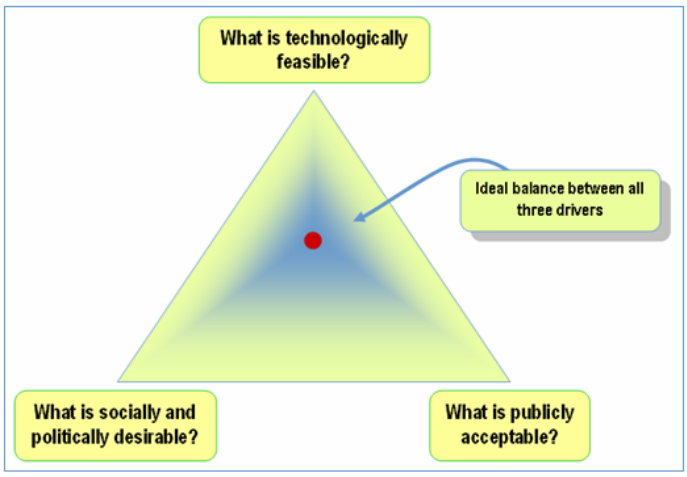
There is very little understanding that the technologies available today permit an entirely different approach to identity management that can allow otherwise contradictory concerns – such as what is politically or socially desirable alongside what is publicly acceptable – to co-exist. For example, that the political and social imperatives of security can still be achieved, somewhat paradoxically, in an environment that rigidly defends and enforces privacy.

It is worrying that large parts of the debate have been conducted without an explicit unbundling of the issues, political, social, cultural, legal as well as technological.

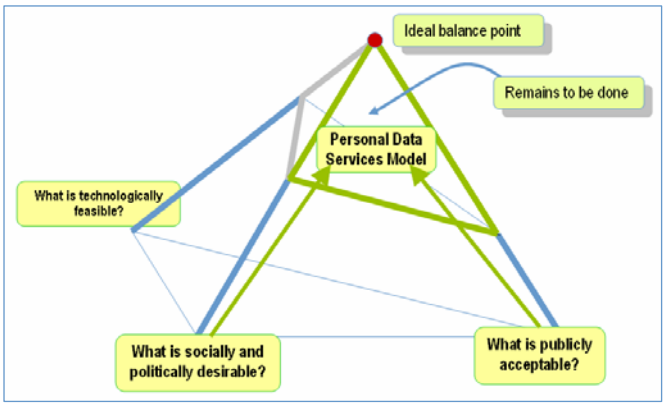
One valuable tool to help do exactly this, firstly identifies the main drivers:

As with many major technological debates, the discussions around electronic identity management have tended to held along one or other of the three outside axes of this triangle. Either:

- What is technologically feasible and publicly acceptable, without any reference to political or social concerns (the so-called "libertarian" or anarchic model);
- What is technologically feasible and politically desirable, but in this case without reference to what is publicly acceptable (the more "totalitarian" or "Big Brother" model); or – to a lesser extent, the third:
- Balancing what is politically/socially desirable with what is publicly acceptable, but without any account taken of what is technologically feasible.



The domain of electronic identity demands however that all three concerns are taken properly on board: it is important to firstly assess the current situation regarding all three factors:



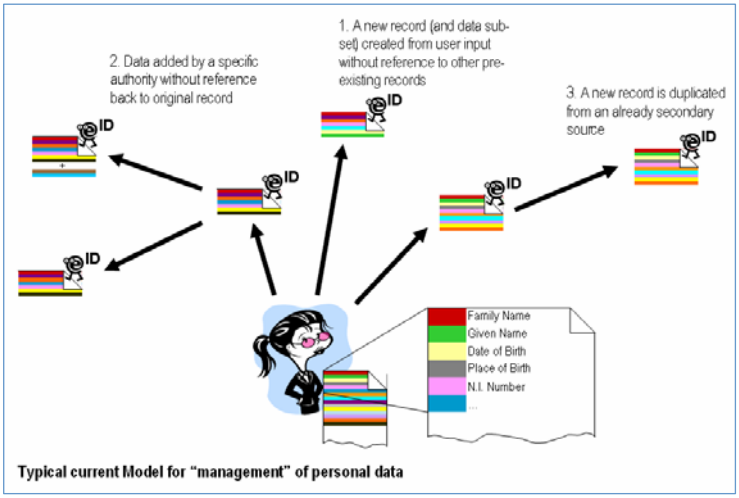
All three of them fall short of reaching the "ideal" apex point. The nature of the issue however demands that we start with consideration of what is desirable and acceptable, in order to create a reference model that can serve as a template upon which technological solutions can then be developed. This will also involve a very clear and detailed examination of key terminology used in this domain, in order to eliminate ambiguity and misunderstanding in discussions over the key concepts.

4 Why isn't personal data "personal"?

Citizens today are faced with an ever increasing need for tools and mechanisms that will allow them to manage their own data, whether that be in the form of:

- Data sets held by various services (often demanded as pre-requisites to access to online services);
- electronic documents
- e-mail archives
- transactions management (from use of bank & credit cards; to tracking web sites visited, people called, correspondents/contacts management, tax and government related forms management);
- audit trails of how/where their personal data is accessed/used

To complicate matters, the same data-sets are repeatedly requested by multiple services or agencies (mailing lists, registrations, forms management, etc) and it is often difficult for the citizen to assess whether their data is used in accordance with data protection legislation and use of some services is often refused if the citizen does not unilaterally give up their right to data privacy ("consent under duress").



Typical current Model for "management" of personal data

Furthermore, personal data is often locked into proprietary systems that:

- make it difficult or impossible to transfer the data from one environment to another;
- make it practically impossible to control who accesses what;

There is only limited legal protection against misuse of private data: even when a user is aware and able to enforce their rights, data protection legislation seems firmly anchored to a view based simply upon a digitized version of the traditional management of paper-based data records and transactions.

It is hardly surprising therefore that citizens feel powerless. To make matters worse, every day they are forced into using forms of authentication that they know to be often vulnerable and are yet held responsible for their use.

At the heart of these concerns are two related questions:

- Who or what do you trust to "identify" someone?
- Who or what do you trust to manage your personal data?

Related to these questions are implicitly concerns about liability: if my trust is abused and/or my personal data s compromised in some way, what can be done to make good any harm done? Data protection legislation in force in some countries only goes some way to addressing this, as the onus is always on the individual to track down uses and misuses of their data, irrespective of whether they have knowledge of or access to data that might be held by different third parties. Ultimately, you can only manage what you can identify.

5 What can the financial services sector teach us?

It is useful to look at an analogy – that of money management – in order to understand some of the processes. It is perfectly possible to look after your own money by keeping "under the mattress" but you are then entirely liable for its management. The alternative is to have someone to look after it for you: citizens choose a service provider that offers the best match to their needs (and pick and mix particular services if necessary).

After pharmaceuticals, the banking and financial services sector is the most heavily regulated business and with reason: citizens want to be sure that the services they use are trustworthy, are accountable and are held liable for the transactions that are undertaken in their name. As such, there are strong public policy rules, detailed regulation and a clear model for financial liability.

Furthermore, the financial services sector have developed highly sophisticated identity and authentication systems – largely because of issues of liability – as a means to ensuring secure, reliable and trustworthy transactions.

In terms of personal data management, we can see parallels:

- We manage our own piles of paperwork (forms, certificates, diplomas, licenses, statements, bills, etc)
- We "employ" our home PCs, PDAs, mobile phones, web-mail accounts, etc. to manage more and more information resources;
- Publicly-available services emerge to manage some of those resources on our behalf (web-mail services, social-networking sites, personal web-sites, document and photo repositories, etc.).

The big difference is that there is no legislative framework in which such services operate; there is no effective user control; nor any set of underlying standards that dictate how personal data should be managed, stored, authenticated, shared and used; nor yet any agreed standard or enforcement of liability or conformance.

6 The Personal Data Services Model

However, what if:

- There were a public standard governing the information architecture for personal and citizen data?;
- Each citizen were able to have a personal information repository[1], with the same legal protections and inter-operability that we have come to expect from banking?;
- Such repositories were architectured and run as services, according to an agreed underlying model?;
- Different vendors and solution providers were to offer the IT-infrastructure for these repositories, according to agreed, certified standards?;
- Each citizen could decide whether to manage the repository themselves via a service provider (cf online banking), or use the services of a trusted "information broker" who manages the repository on their behalf (cf traditional banking, with personal interaction, ink signatures to provide authorisation and audit trail, etc.) ?

Such information brokers could be banks, post offices, libraries, employers, government agencies: anyone that met certain service provision criteria and guaranteed conformance with an agreed service model. Alternatively, personal data services could be managed directly by the user on their own infrastructure.

Now imagine further that:

- There were a public standard governing citizen electronic identity, and more particularly authentication and subsequent assertions of the validity of that identity (to govern, for example, legitimate access to and management of information repositories);
- Instead of citizen data being entered into, managed and stored in multiple repositories in public and private sector services, those services instead simply accessed personal repositories as needed and authorised;
- There were a "double key" mechanism requiring both the citizen (or their agent) and a service to digitally sign requests to access information;
- The citizen part of the double key were available in different authentication tokens of the citizen's choosing (whether using a mobile phone, personal music player, bank card, computer or other infrastructure);
- That, irrespective of its physical location, the personal data store were permanently reachable and programmatically accessible;
- That critical and reference data were stored according to a standard model and that standard mechanisms (covering accessibility and authorisation) were available for accessing such data;
- That, even if certain data were accessed in an emergency with a public "override key", the citizen would still have an audit trail of who accessed what, making it easier for the citizen to spot abuses and errors;
- The citizen could receive information transaction statements detailing who has accessed what data, in the same way that we receive bank statements today?
- Citizens could choose among personal repository service providers, in the same way that we choose among banks;
- That such service providers would be authenticated and certified by a recognised public authority

[1] Such a repository does not need to be a single physical entity but rather a single "logical" entity which could be made up of various subsets of information provided and managed by different parties.

- The basic service and core information were provided free to the citizen, with the service provider subsidised from the public purse;
- Key reference data would be modifiable only by a double key process involving both the citizen and respective public authority; other reference data would be modifiable by the citizen alone, or in tandem with an appropriate authority, and done according to a standardised process;
- Citizens could buy in to additional services (document storage, encryption and digital certification, credit and charge cards, fidelity cards, mailing lists, e-mail archives, blogs, personal web sites, transaction/audit trails, etc.);
- Citizens could "trade" certain items of personal data for an agreed price (countering the current trend where retailers and services trade that information in exchange for certain privileges/benefits); this trading would involve agreed access and use of certain data, which the citizen could terminate at any time; this trade could subsidise the cost of running an individual's information repository;
- Citizens could individually decide what part of their information repository they wanted to make available, to whom, and on what conditions; and "publish" an ontology of their own information store allowing programmatically accessible virtual communities to be established;
- Citizens could make legally binding assertions regarding the ownership of digital “belongings” (whether MP3 files, films, documents from a birth certificate, a university diploma through to the Deeds to their home) as well termination and transfer of such ownership.

7 Implications

Implicit in the above approaches is that management of personal data – however widely defined – should be carried out as a service. This would:

- Eliminate the (need for) duplication of personal data;
- Create a simple and single point of access (at least a single ***virtual*** point of access - need to avoid single points of failure);
- Ensure referential integrity of data;
- "Outsource" at a stroke large parts of the data storage needs of many agencies, public and private alike;
- Allay and disperse fears about electronic ID cards and management of personal data;
- Put the citizen at the centre of the "information model" regarding their own data;
- Ensure transparency on the use of personal data;
- Force service providers to create and maintain data access interfaces that respect the integrity and “use-rules” of the reference data;
- Would force a serious maturing of the Internet and web service technologies and web security standards;
- Would require a public agency to determine the data standards to be used, as well as the information architecture and service model, as well as conformance criteria and certification processes;
- Would allow the private sector to compete to develop and provide both IT-infrastructure (repositories, registries as well as software and tools) and repository services.

The “Reference Model for Service-Oriented Architectures”[2] provides an adequate model upon which to base any proposed Personal Data Services Model, from the moment that “personal data” is understood as having inherent value, and thus its management,

[2] An OASIS Standard, see http://docs.oasis-open.org/soa-rm/v1.0/

provisioning and use are seen as part of a transactional service rather than just the manipulation of passive data objects.

Understanding "personal data" in this manner also underlines an important conceptual point, that of the important difference between "data" and "information": information is best understood as "data in context". Personal data is nearly always data in context, and as such will always be information for someone or some agent. Whereas data can be seen as merely "passive" objects, information always has value and as such should always be managed, this itself implying both ownership and custodianship.

8 Possible approaches

A number of issues need to be addressed if this model is to be realised.

Firstly, it would be necessary to be more explicit about **what is understood by "identity"** and "personally identifying data". From the point of view of formal logic, "identity" is nothing more than the assertion that two things *x* and *y* are equal and takes the form:

$$\forall x \forall y [\forall P (Px \leftrightarrow Py) \rightarrow x = y]$$

"for any x *and* y*, if* x *and* y *have all the same properties, then* x *is identical to* y*"*

The electronic identity, the objective of "identifying" some person is often not to actually "know" who the person is but rather to identify some selected set of properties needed for some particular purpose. For example, having verified that some group of properties presented to a service (a name and a credit card number; a user name and password; etc.) match an identical group of properties held by that service "on file", a service is able to assert – because the set of properties is identical – that they must indicate or "identify" the same person. Most service are completely indifferent to the particular "identity" of the person: *in extremis*, an online service doesn't actually care whether the "person" exists at all, provided that the service is paid for by some entity.

What is important here is that the group of properties used to "identify" does not need to be – indeed, cannot be – exhaustive but is rather aimed at being sufficient for the assertion of identity to be made in the particular context. However – whether because of poor and/or lazy interface design and programming or an overzealous interest in farming personal information – many services collect more data elements than are strictly necessary for the completion of the particular service. Whether intentional or not, this leads to a dispersion of personal information in a way over which citizens have little control.

Even if there is a single set of characteristics or properties that are always sufficient to identify someone uniquely, the questions arises whether that is necessary or acceptable: there will be public policy reasons in some contexts, but in most situations, comprehensive identification of an in individual – for example by requiring a biometric-enabled identity card in order to order a book online – will simply be overkill or too expensive and complicated to deploy as well as compromise issues of legitimate protection of personal privacy.

The first approach therefore underlines the principle that identity should be provided by a set of properties necessary per context, nothing more, nothing less.

Secondly, it would be necessary to **make a distinction between a "formal identity"** – such as provided by a government issued identity card, passport or other token – **and "functional**

identities" that consist of a set of data necessary for a particular function, service or context – such a company staff card, a user account, etc.

In "classic" Western bureaucracies, formal identity was asserted through possession of identity papers: possession of the papers, together with human verification of some characteristics carried on the papers – photograph, signature – constituted a formal and legally acceptable assertion of identity. A limited number of known authorities (often only one per country or administrative area) could issue such papers; and a limited number of public agencies knew or needed to know what valid papers looked like.

If a publicly-issued identity card carries **biometric** data – such as digitized encapsulations of fingerprint, iris, facial patterns or even DNA – that incontrovertibly provide unique identity, why do all identity cards also carry **biographic** data (name, address, date of brith, etc)?
Surely biometric data is enough to provide a formal "root" identity and providing anything more should be a matter of personal choice?

Today however, a wide range of "authorities" – both public and private – issue forms of identity and it is increasingly difficult to make assertions (especially legally-binding assertions) about identity in any comprehensive fashion. Some countries are deliberately making their latest-generation electronic identity cards available as a token for asserting identity also in private transactions (such as online eServices and eCommerce) but which might be considered as unnecessarily heavy-handed for many transactions. On the other hand, in countries where the "formal identity" is limited to being used for public sector transactions, there is no mechanism for making any formalized and legally-binding assertion between the identity established for a particular service and a person's formal or "root" identity.

In both situations however it is possible to accumulate data that – taken together – is sufficient to identify a person: this is the most common vector used in identity theft and spoofing: providing sufficient identifying elements to satisfy a particular service's need, without any reference back to an authentic – and authenticated – root source.

Thirdly, in order to provide both a protection against identity theft and a reassurance as to the legitimacy of a claim of identity being made, there should be a standard, formalised mechanism that allows any identity assertion – or indeed any data element associated with a particular person – to be tied to a "root identity" (even if this root identity is "anonymized") through a signed and verifiable association. An extension of this principle – to link an unambiguous identity with any digital artefact – would allow citizens to make assertions of ownership in a manner that would reduce or eliminate the need for current "sledgehammer" approaches to digital rights management.

Fourthly, personal data should no longer be understood as stand-alone, passive data objects but rather as information assets. To treat them as such would introduce both the concepts of personal data ownership and custodianship and stimulate a clearer debate around the responsibilities of both.

Fifthly, and as a consequence of this, the management, provisioning and use of personal data should be architected as a distinct service model. Whether personal data is managed by the individual, by a government authority, by one or more private services (or any combination thereof), such a "personal data service" should be seen as a logically unique point of access to such data. This would conform to the principles of the Reference Model for Service-Oriented Architectures and open up a series of benefits for citizens, public authorities and the private sector alike:

- Personal data and personal data service capabilities would be "exposed" only according to need (principle of "service opacity");
- Data would be accessed and used transactionally;

- Transactions would be idempotent, ensuring that data is used only once for a particular purpose, however many times it might be requested;
- All transactions would have an "execution context", ensuring that the citizen is able to manage and track the interactions with their data;
- Transactions can be fully audited – even in a situation where a citizen may not be aware of their data being accessed (for a defined public safety or security issue, for example), a transaction audit provides a means for all parties to ensure that data is accessed according to legitimate rules.

> "The Council of the European Union…invites the Member States to…
> - ensure an appropriate legal and organisational environment which stimulates the creation of accessible, inclusive, user-centred ad seamless electronic services of public administrations across the European Union and wider ICT take-up in the public and private sectors;
> …
> invites the Commission to…
> - put in place the necessary mechanisms to stimulate pilot projects and other necessary support activities…"
>
> ***Council Conclusions on eGovernment for all Europeans, 9 June 2006***

With this approach, the perennial problem of interoperability between heterogeneous systems with differing identity requirements can also be addressed: even if different systems require different data elements or tokens in order to authenticate a user, the availability of a single, logical, personal data service would be able to "customise" the authentication transaction according to a specific service's needs.

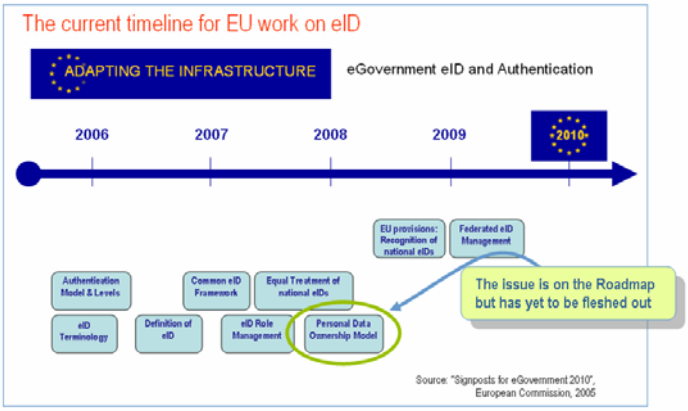
Some steps have been taken in this direction already, by both public and private sector initiatives: what is missing however is a common personal data "reference model" that could include common agreement on definitions of personal data and related terminology as well as on rules and procedures for access and on ownership and custodianship.

Such a model should be both simple and extensible and should be a matter of public policy, but supported by solution providers.

9 European Union context

The European Commission's "eGovernment Action Plan 2006-2010" lays out a policy framework for detailed work to be carried out together with the European Union Member States, as part of its mid-term work plan up to 2010 on the Information and Knowledge Society.

In the specific field of electronic identity management, a "Road Map" has been elaborated which identifies a series of work areas that need to be pursued in order to achieve certain defined policy objectives regarding the interoperability of electronic identity systems across Europe. One of the items on the Road Map concerns the development of a "personal data ownership model" and should be understood as a placeholder for further work such as outlined in this document.



The eGovernment sub-Group – made up of representatives of the EU Member States and the Commission itself – is the main body advising on the overall strategy for eGovernment policy in the EU. It is currently in the process of updating and refining the various aspects of

the Roadmap, and will be deciding how each of the issues will be tackled - particularly as many of them are a mix of political, legal, organisational and technological challenges.

The timeline and milestones are only indicative: it is clear that any attempt to develop a reference model for personal data should ***precede*** any work on more substantial architecture and development.

The European Commission is intending to launch a series of preparatory and support activities, including "large-scale demonstrators", that will serve to support and validate the proposed policy work.

In common with many public policy makers, it is this author's belief that certain milestones indicated in the Roadmap are probably best achieved by standards bodies and/or industry consortia who have the membership and necessary expertise in these domains. This could be the case already for one early item – defining and agreeing a common terminology for electronic identity – as well as for the item concerning the "Personal Data Ownership Model": indeed, the objectives of this milestone coincide largely with those set out in this paper.

One obvious candidate for such work would be OASIS – the Organisation for the Advancement of Structured Information Systems – a global member-based industry consortium that has a proven track record in developing common, open, specifications, particularly in related areas concerning identity and security[3].

An OASIS specification on personal data services could serve then as a "deliverable" to the European Union's eID Roadmap as well as providing a sound basis for any public or private agency that wished to develop user-centred conformant models for managing personal data.

Industry would certainly have an important role to play, both in validating any personal data services model but also in promoting technologies and solutions that conform to the model's public policy goals.

10 Next steps

Following initial discussions with a series of public and private sector bodies, there is a growing consensus both to act on the issues outlined in this paper and to aim for some early, pragmatic results. The following steps could be envisaged if the creation of an OASIS Technical Committee is accepted as the best avenue through which to pursue this work. Initial steps could therefore consist of:

- Initiate a discussion list within OASIS for the purpose of forming a new Technical Committee – this requires a minimum of three OASIS members;
- This would trigger a "Call for Participation" to the entire OASIS membership, in order to solicit views on the value of such a new Committee.

Alternatively – if, for example, there is enough support already for the idea – and in any case after the initial discussion list, the following steps would be:

- Submitting to the OASIS administration a formalised proposal to start a new Technical Committee – this requires support from a minimum of five OASIS members (and including at least two member organisations)

[3] Such as the Security Assertion Markup Language (SAML) and Extensible Access Control Markup Language (XACML).

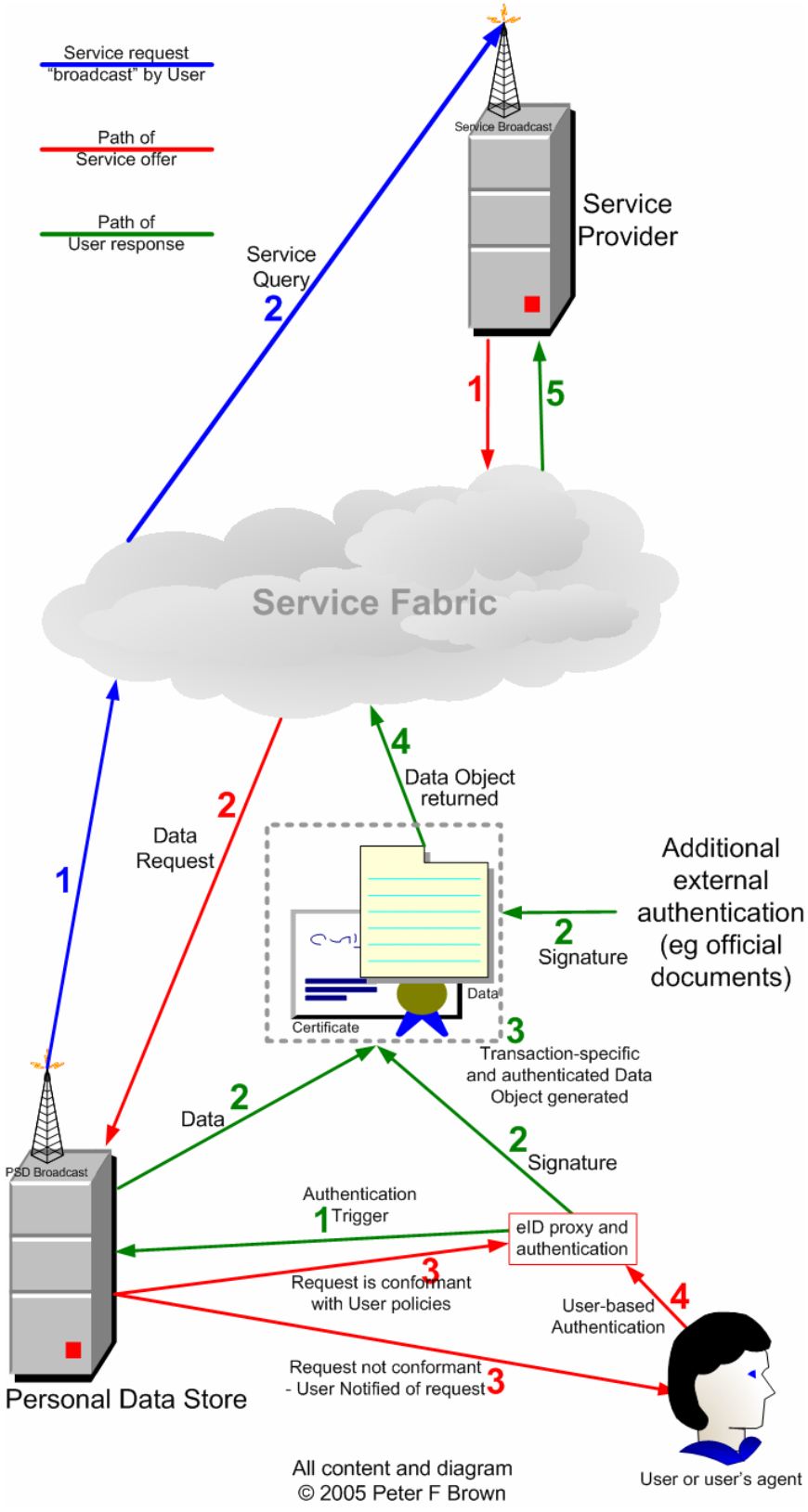
- Such a proposal would contain a draft Charter for the new Committee, including its proposed name, purpose, deliverables, IPR mode to be used, intended audience and working language[4];
- After an initial 2-week comment period, OASIS will organise a first meeting among the "proposer group" to discuss and refine the proposal and react to comments from the OASIS membership;
- The initial "sponsors" would proceed to agree the timing and practicalities of a first kick-off meeting – this can be done via conference call but a face-to-face meeting is often valuable as a first meeting on a new project. Whatever the formula used, the first meeting needs to be sponsored by one of the proposing members. The first meeting must be held after a minimum of 30 days (for a telephone or other virtual meeting) or 45 days (for a face-to-face meeting) following the announcement by OASIS of the committee being established;
- Members can submit at the outset existing technical or other work that they feel could contribute to the committee's work.

Depending on how this work proceeds, output from the Technical Committee could also serve as valuable input to the European Commission's work on its "eID Roadmap"; the ongoing work of any other public authorities; to the OASIS eGovernment technical committee; or indeed any other related work.

[4] See section 2 of the OASIS "process document" at http://www.oasis-open.org/committees/process.php

11 Typical model

Below is a conceptual model demonstrating how personal data could be used transactionally:



12 References

The Identity Landscape of 2006, http://netmesh.info/jernst/Digital_Identity/three-standards.html

Identity, Reference and the Web, W3C 2006, http://www.ibiblio.org/hhalpin/irw2006/

Privacy fear over Web's future, BBC News, 24 May 2006, http://news.bbc.co.uk/2/hi/technology/5009774.stm

Austrian Government Unique Object Identifier, http://www.cio.gv.at/it-infrastructure/oid/

On the Absurdity of Owning One's Identity, Bob Blakley, http://notabob.blogspot.com/2006/01/on-absurdity-of-owning-ones-identity.html

Identity Open Space and Higgins Trust Framework, http://www.eclipse.org/higgins/

The Laws of Identity, Kim Cameron's Identity Weblog, http://www.identityblog.com/?page_id=354

The Identity Metasystem, Kim Cameron's Identity Weblog, http://www.identityblog.com/?page_id=355

Robin Wilton's esoterica, http://blogs.sun.com/racingsnake

European Council Conclusions, 9 June 2006, http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/trans/89954.pdf

i2010 eGovernment Action Plan, European Commission, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

A Reference Model for Service-Oriented Architecture, OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

The Global supply chain: challenges for small and midsize enterprises, Economist Intelligence Unit, http://www.eiu.com/globalsupply

Motorists to give fingerprints

Drivers who get stopped by the police could have their fingerprints taken at the roadside, under a new plan to help officers check people's identities.

A hand-held device being tested by 10 forces in England and Wales is linked to a database of 6.5m prints.

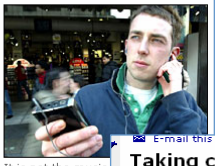
No two fingerprints ha
found to be identical

Police say they will save time because people will have to go to the station to prove their identity.

Officers promise prints will not be kept on file but have been raised about civil liberties.

Copying own CDs 'should be legal'

A think-tank has called for outdated copyright laws to be rewritten to take account of new ways people listen to music, watch films and read books.



The Institute for Public Policy Research (IPPR) is calling for a "private right to copy".

It is not the music
decide consumer ri

It would decriminalise millions of Britons who bre
each year by copying their CDs onto music play

Making copies of CDs and DVDs for personal use
little impact on copyright holders, the IPPR argu

Officials falsely labelled 1,500 as criminals

ologise yes-
1,500 inno-
se of errors
whether in-

ns of trust

E-mail this to a friend Printable version

Taking control of your digital ID

Jonathan Fildes
Science and technology reporter, BBC News

Most people know that you should not throw away letters or bills that contain your personal information.

If you do, an unscrupulous criminal might raid your bin in the middle of the night and steal your discarded details.

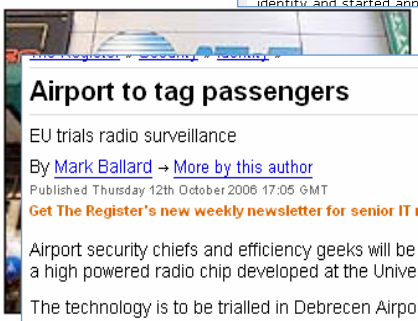
The government estimates that ID fraud cost £1.7 billion in 2005

By the time you sit down to breakfast, the midnight marauder will have assumed your identity and started applying for mortgages and credit cards

Hackers steal AT&T customer da

Hackers have obtained the credit card details of almost 19,000 online shoppers from telecoms giant AT&T.

The US company said it had notified shoppers at its online store of the security breach, which affected people buying high-speed DSL internet items.



Airport to tag passengers

EU trials radio surveillance

By Mark Ballard → More by this author

Published Thursday 12th October 2006 17:05 GMT

Get The Register's new weekly newsletter for senior IT managers delivered to your inbox, click here.

Airport security chiefs and efficiency geeks will be able to keep close tabs on airport passengers by tagg
a high powered radio chip developed at the University of Central London.

The technology is to be trialled in Debrecen Airport in Hungary after being in development for two-and-a
University College London as part of an EU-funded consortium called Optag.

Dr Paul Brennan, of UCL's antennas and radar group, said his team had developed a radio frequency
tag far in advance of any that had been used to now to label supermarket produce.

People will be told to wear radio tags round their necks when they get to the airport. The tag would notify
system of their identity and whereabouts. The system would then track their activities in the airport using

Home ▸ Justice & Security Policy Section

Belgian authorities knew of US sc
data[de]

Published: Monday 26 June 2006 | Updated: Tuesday 21 November 2006

The Belgian National Bank and the country's Finance Minister Didier Reynders knew of an agreement under which SWIFT, the company operating cross-border payments in the EU and elsewhere, forwarded data to the

Under the scheme, SWIFT granted the US intelligence agency acc
concerning millions of financial transactions involving six billion eu
reaction to a request from US authorities. The programme, which
the CIA, allegedly led to the arrest of high-rank terrorists.

The New York Times, which **revealed the practice**, quotes

The next phase of the web could face "big privacy" issues, a senior UK academic has warned.

Hugh Glaser of the University of Southampton made the comments at the WWW2006 conference in Edinburgh.

The web is full of personal information about all of us

He was describing the semantic web, an attempt to make the web more intelligent.

Privacy problems could occur, he said, because the semantic web deliberately combines multiple sources of information about people and places.

Thoughtful solutions

Pensive!