Empowering individuals to control their personal information

The report of the Work Group on User-Centric Identity (and Personal Information) Management

sponsored by:

The Information Commissioner's Office,
The Technology Strategy Board,
and The Cyber Security Knowledge Transfer Network.

December 2008

Information Commissioner's Office

Technology Strategy Board
Driving Innovation

Cyber Security
Knowledge Transfer Network

Contents

Preface by the sponsors

For several years now, there has been much debate in the UK about the linked subjects of identity management, identity assurance, and personal information sharing. Some believe that improved information systems in these areas are necessary in order to safeguard national security, deliver better 'joined-up' services, and even reduce costs. But others fear that the linked trend towards ever more centralised systems will impair the individual's privacy and autonomy.

This document is the report of the Work Group on User-Centric Identity & Personal Information Management, which was sponsored by three organisations:

- the Information Commissioner's Office, which is the UK public body with the responsibility for promoting the protection of personal information;
- the Technology Strategy Board, which seeks to stimulate technology-enabled innovation in the areas which offer the greatest scope for boosting UK growth and productivity; and
- the Cyber Security Knowledge Transfer Network, which exists to bring together the cyber-security community in the UK in order to identify new challenges, influence UK investment strategy and government policy, and accelerate innovation.

As sponsors, we agreed to support the Work Group because we believe that – when organisations consider identity management and personal information sharing – insufficient attention has been paid to new user-centric architectures that seek to put the individual in charge of the flow of their personal information, and so allow the delivery of joined-up services and the reduction of costs and, at the same time, enhance personal privacy.

The report represents an overview of discussions at a number of facilitated work-group meetings. It has been written by John Harrison of Edentity with the help of other participants in the group. Note, however, that the report cannot be said to represent a consensus of all participants. Rather it is an illustration of thinking about user-centric identity and personal information management, written with a view to informing – rather than necessarily persuading – the reader about the new approaches.

We suggest that the report is worth reading carefully. Although there is no conventional summary, the main body of the document is just nine pages long, and conveys a multi-stranded argument in clear terms, touching not just on technical issues (at a suitably high-level), but also on the need for clear thinking about organisational boundaries and for fresh approaches to the business and liability models that underpin information system design. Matters of detail have been relegated to the annexes.

Jonathan Bamford
Assistant Information Commissioner

Andrew Tyrer
Network Security Innovation Platform Manager, the Technology Strategy Board

Nigel Jones
Director, the Cyber Security Knowledge Transfer Network

Introduction

1 In March 2008 the Information Commissioner published a paper [ICO] entitled 'New approaches to identity management and privacy'. This explained how work in a new field, known as user-centric identity management, offers the potential to give individuals control over the initial sharing of their identity and other personal information, and so could provide a privacy-friendly alternative to the more traditional approaches. The paper also reviewed existing user-centric initiatives, a summary of which is provided as Annex A.

2 A month or so later, and being aware that further work was required to develop understanding of the new approaches, the Commissioner agreed to join the Technology Strategy Board and the Cyber Security Knowledge Transfer Network as a co-sponsor of a Work Group (WG) on User-Centric Identity (and Personal Information) Management[1] (UC-IPIM).

3 The remit of the Work Group is to: "determine where the field of user-centric identity and personal information management now stands and, if appropriate: (i) attempt to reach a common view on the need for, and shape and scope of, one or more UK pilots; and (ii) summarise our views in a brief report, and go on to organise one or more education events designed for politicians, senior civil servants and think tanks". This document is the report foreseen in the remit.

4 The Work Group was well supported. A total of 46 individuals, representing organisations from across the public and private sectors, participated in the face-to-face meetings, and in the linked online discussions. Their names, and affiliations, are given in Annex G. Note, however, that the views expressed in this paper cannot be said to represent a consensus of all participants. Rather they are intended to provide a broad overview of the discussions, and are presented with a view to informing, rather than necessarily persuading, the reader as they participate in the identity and information management debate.

5 In parallel with the launch of the Work Group, and in response to a commission in 2006 from the (then) chancellor Gordon Brown, Sir James Crosby published the report [CRO] of his Public-Private Forum on Identity Management. The report stated that "It's the consumer's identity", and "To realise the greatest economic and social benefit every aspect of an ID card scheme should be designed from the consumer's perspective". Few would disagree. However, the report's recommendations were limited to the best use of currently deployed technology. This report considers how new technology can give the consumer better control of their own identity and other personal information.

6 In the following paragraphs, we look at the differences between the traditional organisation-centric and the proposed user-centric approaches to identity and personal information management, and explain why user-centric architectures protect privacy by design. We go on to state that, while it can be argued that some form of unique national register of 'legal identities' may be necessary, the user-centric approach appears better suited to many applications. Next we look briefly at some implementation issues, describe the scope for convergence with other infrastructure, and finally discuss next steps.

Traditional organisation-centric IPIM is necessary, but imperfect . . . .

7 The advent of high-speed networks is making it easier for organisations to share information about individuals, using common fields – such as name and address, or a cross-organisational

[1] At inception, the Work Group's subject was referred to as User-Centric Identity Management. On writing the report, the words Personal Information were added to the title to make it clear that the subject extended beyond the narrow definition of identity to include many types of personal information.

identifier – to match up their records. Such *organisation-centric* or *back-office* identity management and personal information sharing can be carried out without an individual's consent and thus can impair individual privacy.

8 But it is recognised that privacy is not an absolute right. In the absence of consent, back-office information sharing can be justified where the needs of society outweigh the rights of the individual; or where an individual is incapable of giving consent. Obvious applications include crime prevention and detection, national security, and the care of the young and the vulnerable. And there is little overt public concern about such sharing, especially where the organisations concerned, although legally distinct, are seen by the public as being merely different facets of the central government monolith.

9 Nevertheless, the traditional back-office approach to identity management and personal information sharing is far from perfect. There are two concerns, of which the first is privacy. Although some individuals support back-office sharing, saying they have 'nothing to hide', many others dislike the practice for fear of scope-creep leading to a society in which organisations hold comprehensive files, and privacy and autonomy are eroded. Thus, in the interests of privacy, it is generally accepted that organisations should – wherever it makes sense – enable individuals to exercise choice over the sharing of their personal information. Often obtaining consent can be to an organisation's advantage because it broadens the range of purposes for which personal information can be fairly – and transparently – used.

10 The idea of consent is a simple one. But the practice of obtaining consent for back-office information sharing is problematic. Use of the common mechanisms – either 'tick-boxes' at the foot of an application form or a mandatory clause in the small-print – is unsatisfactory, either because the consent sought is too broad-brush; or because the individual has no choice but to give consent if he wishes to obtain a service; or because (given that the sharing takes place out of sight in the back-office) he has no confidence that his wishes will be respected. The frequency of data breaches, which can be considered as an extreme form of non-consensual information sharing, suggest that individuals are right to be sceptical.

11 The second concern about back-office information sharing is simple: it is a poor fit with the complexity and mobility of modern society. The approach only works well when the number of organisations sharing information is relatively small, and / or the organisations are linked together closely by common ownership or common interests. But as the distance between organisations grows, their degree of mutual awareness diminishes, and it becomes increasingly hard to determine which organisations have the information that is required, which organisations should be told when the information changes, and whether any of the organisations can trust each other as information originators or recipients. There are thus many information sharing applications that cannot easily be addressed by the back-office model, and – if an alternative can be found – there is ample scope for further reducing transactions costs for organisations, and enhancing convenience for individuals, while also protecting privacy.

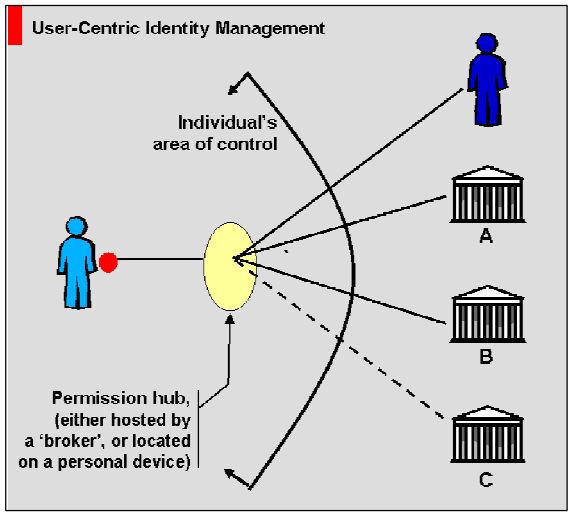
User-centric IPIM addresses the weaknesses of the organisation-centric model . . .

12 *User-centric identity and personal information management* (UC-IPIM) can be seen as a way of addressing the concerns about the organisation-centric model, and it seems likely that a mature identity/information management infrastructure will comprise both user-centric and organisation-centric elements. The term *front-office information sharing* is sometimes used as a metaphor for the user-centric approach.

13 The principle of UC-IPIM is simple: an organisation gives an individual access to a tamper-resistant record of certain personal information, and the individual can then show the record – and /or information recorded by himself – to other organisations, or other individuals, when required for the purposes of a transaction.

14 In one sense, UC-IPIM is not a new idea: in the paper-based world, individuals often carried personal information, on a paper-certificate or plastic card, from one organisation to another. Examples include showing a medical prescription to a pharmacist; a driving license when hiring

a car; an exam certificate when looking for work; a passport when opening a new bank account; and a proof-of-age card to buy age-restricted goods and services.



15 Replicating this front-office approach electronically is possible now that the internet is approaching ubiquity, but requires a new kind of infrastructure. In most proposals, an individual uses a digital '*permission-hub*'[2] to give explicit permissions for the transmission of relevant personal information to and between such counterparties. The information shown electronically to a particular counterparty is referred to as a *profile.* Note that a permission-hub can be carried on a personal device (such as a smart-card, a mobile 'phone, or a laptop computer), or can be provided as a service by a broker commissioned for the purpose. Each alternative has pros and cons, which we discuss later.

. . and protects privacy by design.

16 To protect privacy, it makes sense for an individual to limit the information contained in a profile – as disclosed through a permission-hub to a counterparty – to that which is relevant to, and thus necessary for, a particular transaction. This is the idea of data minimisation. Think about the common need of young person to prove that they are old enough to buy a drink. Bad practice would be for a retailer to demand a full identity card, since the purchaser's name, precise date-of-birth, home address, and card number are all irrelevant. What is needed, following the idea of data minimisation, is just a statement from a trusted source that the young person is above the minimum age, and some means – say a photograph – to link the statement to the individual. This need could be met with a minimalist tamper-resistant plastic card, or by online electronic means.

17 The idea of data minimisation reflects the way in which normal relationships (whether between two individuals, or an individual and an organisation) develop. The two parties start by knowing relatively little about each other, and then progressively reveal more information when it is in their interest to do so. Frequently a legal identifier – such as an ID card number – is neither relevant nor needed.

18 This means that – if it is to be successful – a user-centric infrastructure cannot be built on the basis that a national ID card number will be automatically disclosed in every profile. Doing so

[2] The term 'identity selector' is also used in this context, having been popularised by Kim Cameron of Microsoft. But it is thought by some to be misleading, since UC-IPIM can be used to transmit many different kinds of personal attributes, not just those that form part of a person's (narrowly defined) identity.

would contradict the principle of data minimisation, and enable unfriendly organisations to use the identifier to join-up records in the back-office, thus destroying privacy.

19 Instead, in UC-IPIM, each counterparty knows the individual by a different underlying identifier, a bit like a customer reference number. Only the individual, or software working on the individual's behalf, knows all the different reference numbers and can allow links to be made between them. Then, using his permission-hub, an individual can choose to transmit particular pieces of information (such as a national ID number, a date of birth, or just a nickname for use in a relationship) if requested by the counterparty. It is as though an individual gets to carry a piece of 'psychic paper'[3] in his wallet that shows whatever (true) information is required by a counterparty fulfilling a particular role with respect to that individual, and nothing more.

A national record of each citizen's legal identity is probably inevitable . . .

20 Having described the two approaches to identity and personal information management, it is time now to discuss where each should be applied. A good starting point is to recognise that – in the paper-based world – society evolved a mixed approach to information sharing, using the cheaper and easier user-centric approach whenever possible, and the back-office organisation-centric approach where necessary. In the networked world, this mixed approach will be repeated, although it is likely that the balance between the two styles will shift to reflect the differing characteristics of the paper and electronic media.

21 Looking first at those areas where organisation-centric IPIM is inescapable, it is clear that:

- every citizen already has a de-facto '*legal identity*' (comprising records of name, date-of-birth, address, etc) by which they are known to those departments of central government with which they must maintain a near lifelong relationship (HMRC, DWP, DVLA[4], and the parts of local authorities that act as agents for DWP in the administration of the welfare system);
- and that these central government departments already share information via the back-office where necessary for reasons of national security, border control, welfare, and crime prevention / detection.

22 Thus the creation of a minimalist Unique National Register (UNR) as a single centralised store for such information can be seen as little more than a tidying-up exercise, with the goal of ensuring that the back-office information sharing that already takes place is accurate, i.e. that sharing departments can match up their records correctly. Note, however, that this acceptance of the likelihood of a UNR should not be taken to imply that the Work Group supports the National Identity Scheme as currently designed.

23 Going further, it would make sense for a UNR to notify an inner circle of public-sector organisations automatically – again via the back-office – whenever it is informed by a citizen of a change-of-address. Quite which organisations should be included within this inner circle is a matter for debate: HMRC and DWP would seem to be near certainties; the DVLA a possibility. In effect, the individual would come to have a single relationship with the central government monolith, rather than distinct relationships with the constituent departments; and departments within the monolith would use internal authorisation policies to ensure that any given public servant only saw personal information relevant to his role.

24 And there will be other information monoliths, outside of central government and mostly separate from it. The obvious examples are the groups of organisations responsible for the

[3] The 'psychic paper' metaphor was first used by Dave Birch of Consult Hyperion in 2008, but the technical idea of limiting electronic data disclosure according to the role of a counterparty with respect to an individual dates back much further, e.g. UK Patent GB2365721, filed by Edentity in 2000.

[4] Her Majesty's Revenue and Customs; the Department of Work and Pensions; and the Driver and Vehicle Licensing Agency respectively.

delivery of social and mental-health care, since their clients are often unable to care for themselves or look after their own information. But it is uncertain whether the credit-reference system in financial services, and the NHS's centralised approach to health records, will persist in their present form as large, central databases, or will evolve slowly towards user-centric architectures.

. . . but user-centric approaches work better for many applications …

25 Outside the three areas (central government, social care, and mental-health care) that are naturally monopolistic and organisation-centric, individuals can choose with which organisations and people they wish to deal. They can choose where they, and their children, are educated; they can choose suppliers of groceries, books, and music; and they can choose their employers and their friends. These are the sectors where user-centric applications are likely to develop and flourish.

26 The likely foundation UC-IPIM application is a **Common Authentication Service** (CASe) – which enables an individual to sign-on to multiple distinct organisations using a single authentication process, but avoids the use of a common identifier[5]. Although many experts believe that the combination of a permission-hub with a CASe is inevitable, and can be made sufficiently secure by the use of better authentication methods, critics maintain that common authentication creates too great a risk of a serious identity theft. Instead they suggest that an individual should use a permission-hub only when registering with a new service provider, or when altering permissions, and that subsequent authentications should remain service-provider specific, despite the tedium of multiple usernames and passwords.

27 Anyone who has moved house or changed mobile number is familiar with the **change-of-contact-details** problem, and longs for a good solution. Certain social networking sites, such as Plaxo [PLA], are user-centric to a degree, and show the sort of change-of-address functionality that would be useful. But they cannot become general infrastructure, accepted by both pubic and private sectors, because they are proprietary and seek to lock their users in. (What is needed are business and trust models that encourage interoperability between sites, so allowing an individual to choose his social networking provider, and then port his information to a different one at a later date.)

28 In education, where there is increasing emphasis on **personalised & work-based learning**, there has long been interest in the idea of giving every learner a personal area in the network space – called an e-portfolio – that can be used for the storage of qualifications, for reflection about progress, and for assessment. Since an e-portfolio must travel with an individual, from school to college / university and then on into the myriad forms of work, a conventional organisation-centric design – such as the current MIAP[6] project – is likely to struggle to capture the complexity and richness of an individual's lifelong experience. A user-centric approach would seem to merit investigation.

29 Should a user-centric e-portfolio prove successful, other applications in education could be added. As one example, young people between the ages of 16 and 19 from low income families who choose to stay in full-time education are eligible for a **maintenance allowance** of up to £30 per week. The administration of this scheme is complex, requiring that attendance data, possibly from more than one learning provider, be sent to a payment authority, and then matched with

[5] Note that common authentication does not breach the principle of data minimisation since – when communicating with a CASe – each service provider uses its own local identifiers, and receives back authentication assertions linked to such identifiers. Only the CASe, acting ideally under the control of the individual, knows the different identifiers used by each service provider, and can link authentication assertions to them.

[6] MIAP is a programme, commissioned by the Department of Children Schools & Families, to give every learner in the UK a 'Unique Learner Number' and create a single national database of educational qualifications.

the learner's account and bank details. UC-IPIM would enable the individual to examine their own attendance data online, have any errors corrected, and then submit the data to the payment authority every week or so, together with bank details.

30 Then there are the common problems of proof-of-age and status. Once a user-centric infrastructure is in place, it would be possible to set-up **safe online chat-rooms** that only allow entry to users who can prove their age is below the threshold. Or only allow online **purchase of adult goods and services** by those who can show that they are over the minimum age. Or enable students and senior citizens to prove their entitlement to discounts.

31 Individuals working with children or vulnerable adults are currently required to subject themselves to **CRB**[7] **checks**. This is a lengthy paper-bound process that must be repeated for every new job. From October 2009, the Independent Safeguarding Authority [ISA] will introduce a new scheme. Each worker will register with ISA just once and – if found suitable – will have their name added to a 'approved-list', one that is updated frequently. Then, when applying for a new job, a worker will invite a potential employer to confirm their suitability by checking her ISA number against the ISA database. Initially the ISA process is likely to use conventional technology but there is no reason why – in time – the process could not become one application of the UC-IPIM infrastructure.

32 Some people are concerned that the NHS's 'Connecting for Health' IT programme will allow all medical professionals in the country access to everyone's **health records**, with professional ethics and their terms of employment the only real constraint on unjustified curiosity. UC-IPIM would offer individuals online access to their own records[8], and also allow them to (i) restrict access to only those medics, primary care practices, or hospital teams, with which they have some form of relationship; (ii) confirm their default consent for their records, when suitably anonymised, to be used for research purposes; and (iii) grant access – on a once-only basis – to a life-insurance company, prior to taking out a policy. They could also choose to disclose emergency information[9] – such as drug allergies – to any medically-qualified person, either within or without the NHS.

33 There are many further applications of UC-IPIM infrastructure. To give just a few more headlines: certain proposals can enable **secure electronic mail** that – unlike today's insecure e-mail or its secure but little-used variants – can be used easily, and by everyone, for sensitive personal information; there are **reverse marketing** (sometimes called permissioned marketing) applications that could reduce commercial spam, and make direct mail relevant and controllable; there is the potential for **remote proof of legal identity**, which would allow individuals to open new financial accounts without sending paper proofs of identity by conventional mail; and there is scope to provide for **delegation** and **power-of-attorney**, so allowing individuals to seek help in managing their affairs online. But by now the message should be clear, and it's time to look at the next topic: that of how infrastructure for UC-IPIM can actually be built.

Implementation issues

34 Building new infrastructure is tricky, particularly when there is no direct precedent, and when subject experts have conflicting ideas. In the following paragraphs we discuss some of the key issues, starting with the dilemma of where an individual's permission-hub should be located,

---

[7] Criminal Record Bureau

[8] Caspar Bowden of Microsoft has made the point – in various public fora – that UC-IPIM infrastructure would not only protect privacy, but also enable individuals to exercise their subject access rights (to personal records held by organisations) online, rather than relying upon the existing paper bound process, which requires payment of a fee and takes far too long. Indeed, eventually legislation could mandate online access . . . .

[9] International services for emergency health care records already exist, e.g. World Medical Card (www.wmc-card.co.uk in the UK). This requires the individual to carry a printed card showing a membership number, which a medic then uses to access an online database. Reliance on manual methods means that security is low.

and examples of both possibilities. We go on to discuss business model, authentication, links to legal identity, and governance.

Device-based or broker-mediated ?

35 Some experts take the view that perfect privacy can only by attained by giving the user complete control, and so believe that a permission-hub should be located wholly on an individual's personal device (such as a mobile 'phone or laptop computer), rather than on a server in the internet 'cloud'. This can be called: 'device-based UC-IPIM'.

36 The principle example of device-based UC-IPIM is the 'InfoCard'[INF] interface, an open-standard first proposed by Microsoft as one element of its 'identity meta-system', and now also implemented by others for non-Microsoft operating systems. However, the actual use of Info-Cards remains at a low-level. Some suggest that this is because the approach lacks scaleable business, liability, and governance models.

37 Other UC-IPIM experts believe that the requirements for back-up, synchronisation across personal devices, and (eventually) multi-factor authentication, all indicate the need for a mediated UC-IPIM service, in which the individual will use software on a personal device to control a permission-hub hosted on a server in the internet 'cloud'. More detail on these points is provided in Annex B. The organisation commissioned by the individual to provide such a service is called a 'broker', whence the term 'broker-mediated UC-IPIM'.

38 The backers of broker-mediated UC-IPIM maintain that the control / privacy deficit caused by the presence of a broker can be mitigated by: (i) good software design to ensure that the individual has near total control over his broker account; (ii) a competitive market, giving individuals a choice of brokers; (iii) account portability, so that the individual can move his account to another broker without difficulty; and (iv) a strict governance regime to which brokers must adhere.

39 OpenID [OPE] is an early technical standard for broker-mediated UC-IPIM, and has attracted significant support. Organisations such as Google, IBM, Microsoft, and Verisign are members of the OpenID Foundation's corporate board., and many organisations – both large and small – act as OpenID 'providers', i.e. an early form of broker. However the willingness of large organisations to act as OpenID providers is generally not matched by their readiness to allow individuals to use OpenID accounts provided by others to log-in to their own sites.

40 This asymmetry in adoption can be explained by the fact that OpenID is purely a technical standard, and lacks any coherent business, liability or governance models. Becoming an OpenID provider costs little, and – despite the lack of business case – can be justified as a gesture towards interoperability. But becoming an OpenID counterparty requires an organisation to rely upon ID providers with whom they have no contract, and who accept no liability towards them. It is not surprising that few large organisations have taken this step.

41 Returning to the question of where an individual's permission-hub should be located, the likely result is a mixed economy in which: (i) individuals can choose to use a single permission-hub for all relationships, or to use different permission-hubs for sets of relationships in different parts of their lives; and (ii) some hubs may be provided by brokers, and others may be entirely local, according to the preferences of both parties to a relationship.

Authentication, identification, and legal identity

42 As a purely technical standard, OpenID does not specify the means by which an individual should authenticate to his permission-hub, and – in most cases – providers / brokers default to the cheapest, but least secure, option, i.e. user-name password. As for Infocards, its design does permit a particular counterparty to require a higher level of authentication, say a smartcard, but there is no straightforward means by which the associated benefits and costs can be shared between counterparties.

43 It is likely that future UC-IPIM schemes will provide both a stepped approach to authentication, and the means by which the benefits and costs associated with secure authentication can be shared between the counterparties. Higher levels of security, above username-password, can be achieved by requiring the individual to have a particular thing (such as a smart card, a SIM card in a 'phone, or the kind of one-time password device now issued by some banks); and/ or by requiring a biometric (i.e. something that an individual is, e.g. finger-print or a voice-print).

44 Turning now to identification, future UC-IPIM schemes will again provide a stepped approach. OpenID and Infocards already enable an individual to use a different *pseudonym* for every counterparty, or even a different pseudonym for different transactions with the same counterparty. This maintains privacy, and is the proper default position. A good current example is the way in which many people choose to use pseudonyms or 'screen-names' when posting a comment online, or when participating in online games.

45 In the future, parties will be able to require, as a condition of completing a transaction, that their counterparty disclose information recorded about them by one or more third parties. For example, if the transaction concerns the purchase of goods online, the purchaser might wish to see the individual's reputation as a seller, as recorded by previous customers; and the seller might require to see proof of the buyer's age before agreeing to supply age-restricted goods or services. And if the transaction is the opening of a new bank-account, then the bank will require sight of the individual's legal identity, as recorded on a Unique National Register or by a proxy.

46 This raises the more general issue of how UC-IPIM infrastructure should be linked to the system of legal identities by which individuals are known to the state. The various possibilities are described in Annex D. In summary one party to a transaction may – for various reasons, such as self-protection or when required by law – require the counterparty to disclose verified legal identity attributes. The counterparty could obtain electronic access to such verified attributes in a number of ways: a broker (if present) could check his legal identity when he signs-up; or he could set up a relationship from his permission-hub to a specialised registrar of legal identities (such as a UNR, described earlier); or he could rely upon a check of legal identity carried out by a third-party for its own purposes.

Who pays ?

47 As purely technical standards, neither OpenID nor Infocards say anything about who should bear the costs of UC-IPIM infrastructure and who should pay for the associated benefits. The issue is important because, as experience with both schemes has shown, a coherent business model is a necessary driver of take-up.

48 That said, the question may seem less acute for device-based UC-IPIM schemes, such as Infocards, because they rely on software that is likely to be bundled with a personal device's operating system and thus can be used by the individual without incurring extra cost. But, nevertheless, device-based schemes do impose costs, both those that must be met by the counterparties who integrate with the system, and those centred on the individual if secure authentication is required.

49 The Work Group discussed 5 possible business models for the UC-IPIM infrastructure: no-one pays; the State pays; the individual pays; service providers pay; and advertisers pay. The arguments for and against each are reviewed in Annex C. In summary, the likely business model for a broker-mediated scheme would seem to be 'service provider pays', with the possibilities that: (i) brokers may receive some contribution to revenue from reversed or permissioned marketing; and (ii) some individuals may choose to pay extra, either by an annual fee for enhancements to a basic 'free' service.

Governance

50 Neither OpenID or Infocards say much about the need for a UC-IPIM infrastructure to have a governance structure. In the case of OpenID, the reasons for this are bound-up with the origin's of the scheme: it grew out of the need felt by bloggers to find a single-sign-on solution for

multiple blog sites, for which security – and thus governance – was of little importance. In the case of Infocards, the lack of brokers to represent the individual makes it hard to see how a governance community can be formed, or how its regulations could be enforced.

51 Future UC-IPIM schemes are only likely to prosper if adequate attention is paid to governance. Issues that would need to be addressed include: equivalence of different authentication mechanism; business model; structures for exchange of payment and liability, co-branding; and account portability.

Convergence with other infrastructure.

52 By the time that the case for new infrastructure is accepted, there have often been many attempts to attack the problem piecemeal. UC-IPIM is a case in point, and we may well see convergence between UC-IPIM schemes – particularly those that are broker-mediated – and a number of existing services.

53 The leading candidates are the Common Authentication Services (CASe), which enable an individual to use a single authentication process (such as username-password) to gain access to accounts held with multiple distinct service providers. Currently there are two large scale CASe services in the UK: Gateway [GAT] enables the individual to sign on to multiple distinct service providers in the public sector; while the UK Access Management Federation [UKF], in the education sector, enables a student or academic to gain access to remote resources – such as online academic journals – using his home institution's sign-on. Potentially broker-mediated UC-IPIM could provide a convergence path for both Gateway and the UK Access Management Federation.

54 Going further, communication and low-value payment applications could be bundled with broker-mediated UC-IPIM infrastructure. As well as providing a secure alternative to e-mail, broker-mediated UC-IPIM could offer a distributed /infrastructural replacement for the proprietary online services that currently dominate the markets for instant messaging, web-enabled telephony, and low-value internet payments.

55 Then there is electronic ticketing. Sunderland City Council has developed infrastructure for electronic remote ticketing, with which a young person can purchase (using funds provided by the local authority) electronic tickets for 'constructive activities'. He then downloads the tickets from the web to a smart card, and gains access to the activity by presenting the card at the venue. ITSO [ITS] and its member organisations are developing similar functionality for transport ticketing. Both are natural applications for a general-purpose UC-IPIM infrastructure.

56 Finally there is the distant possibility that an individual could manage his 'account' on a Unique National Register through his permission hub. He would then be able to inform the State of, say, a change of address at the same time as he informs other counterparties.

Next steps / the Future.

57 UC-IPIM is a fast developing field, in which a number of overlapping groupings are trying to make headway. Notable initiatives that have not yet been mentioned include:

- VRM, led by the Berkman Centre for Internet & Society at Harvard University
- Project Higgins, led by Parity Inc., a US start-up.
- Mydex, a new UK community-interest company;
- TAS^3, a research project financed by the European Commission;
- PAOGA Ltd, a UK start-up;
- Personal Information Brokerage, a UK proposal led by Edentity Ltd;

And there may well be more. Brief details of each of these projects are given in Annex A.

58 This level of activity suggests that progress may soon be made. But there remains a risk. Unlike conventional packaged software, UC-IPIM cannot be created in the laboratory, and then foisted

directly upon unwary service providers. Rather its development must be a collaborative venture between service providers, and (in the case of mediated UC-IPIM) potential brokers, so that each gets a chance to influence the design, and will commit to running a pilot at an early stage in a project's life. Thus rapid development of UC-IPIM requires that groups of service providers come together to work with potential brokers (for broker-mediated schemes) and technology vendors. As yet there is little evidence of a will to work in this way among service provider groups. Perhaps this report, if it does nothing else, will influence thinking about this issue among relevant decision makers.

Annex A Existing UC-IPIM initiatives

A1 UC-IPIM has been a live topic for the last 10 years or so, ever since the internet took-off. In that time there have been a number of initiatives and standards efforts. The more significant were described in some detail in the original ICO [ICO] paper, and are summarised below – together with some more recent additions.

A2 **OpenID**[OPE] is an open specification for user-centric IdM. It provides a distributed server-side registration and single-sign-on utility for the web. As such, it is lightweight and well-suited for the blogging community from which it sprang, and which it mainly serves. However, as the OpenID community have added additional functionality for OpenID 2.0, they have encountered problems familiar to those who have been active in the field for some years, i.e. any scheme that seeks to go beyond light-weight applications requires not only technical standards but also a governance structure, a business model, and a trust / liability model.

A3 **Information Cards** [INF] In 2005 Microsoft launched its current IdM initiative, an 'identity meta-system' coupled with an interface, called generically 'Information Cards' or 'InfoCards', for use on a personal client device (e.g. a mobile 'phone or laptop PC). Microsoft's own implementation of InfoCards is bundled with the current release of Windows for PCs, Vista. As its name suggests, InfoCards is built around a card metaphor, and invites an individual to select which 'card' of attributes she wishes to disclose in which contexts. Attributes can either be asserted by the individual, or by a third party. In the latter case, the InfoCards software on the personal device holds pointers to the attributes on the third party's servers, rather than the attributes themselves. While more technically sophisticated than OpenID, Infocards suffers similar weaknesses: it too lacks either a business model or a governance structure.

A4 **Project Higgins** [HIG] is an open-source, user-centric, IdM project that will enable 'individuals to store their digital identities and profile information in places of their choice (i.e. on a server or on a personal device) and to share the stored information with companies and other parties in a controlled fashion.' Higgins has adopted the InfoCard metaphor proposed by Microsoft for its client-side architecture. The project is led by a US start-up, Parity Communications. IBM and Novell are contributing code.

A5 **The UK Access Management Federation** [UKF] was created to enable members of one learning provider (such as a school, FE college, or university) to gain easy access – using their home learning provider's authentication process – to web resources belonging to other organisations, such as other learning providers and publishers of academic journals. Originally piloted using the Shibboleth software (which has been adopted by many learning providers), the federation works to the SAML standards (of which more below), and enables the protection of individual privacy by the use of one-time pseudonyms for identification, rather than permanent identifiers. Thus an individual can show attributes (such as 'I am a student of this university') to a third party anonymously, i.e. without also disclosing any permanent identifier. Privacy protecting features of this kind are likely to be a key feature of future user-centric systems.

A6 **Government Gateway** [GAT] is the Common Authentication System for the UK public sector, and allows individuals to log-in to their accounts with multiple public sector service providers using a single authentication process. Since each service provider continues to use its own system of identifiers, Gateway has no need of a common identification system, offers some protection of privacy, and can be seen as a step towards UC-IPIM.

A7 **The Liberty Alliance [LIB]** and the work of the **OASIS SAML [SAM]** technical committee are well-supported initiatives that have developed technical standards applicable to both styles of identity management, i.e. organisation-centric and user-centric.

A8 **Project VRM [VRM]** VRM, or Vendor Relationship Management, is the reciprocal of CRM or Customer Relationship Management. It provides customers with tools for engaging with vendors in ways that work for both parties. Project VRM is a community-driven effort to support the creation and building of VRM tools. It is headquartered at the Berkman Center for Internet and Society at Harvard University and headed by Doc Searls, a fellow with the Center.

A9 **Mydex [MYD]** is UK-based community-interest company, formed in 2008 with support from the Young Foundation – which is a 'centre for social innovation based in London, with a 50 year track record of success in creating new organizations - public, private and non-profit - as well as influencing ideas and policies'. Mydex intends to research and pilot new approaches to user-centric architectures, starting probably with a house-move / change-of-contact details applications.

A10 **TAS^3 [TAS]** is a research project in the UC-IPIM field, funded by the European Commission and led by a Belgium company, Synergetics.

A11 **PAOGA [PAO]** is a UK-based start-up company that has developed and demonstrated software for UC-IPIM applications.

A12 **Personal Information Brokerage [PIB]** is a proposal for UC-IPIM infrastructure in the UK, led by a start-up company, Edentity Ltd. The likely lead application is e-portfolio in the higher and further education sectors.

Annex B Location of permission hubs

B1 The Work Group spent some time debating whether an individual's permission-hub – which he uses to manage relationships with multiple different counterparties – should be: (i) wholly located on a personal device, such as a laptop computer or a mobile phone; or (ii) hosted on a server by a broker, and controlled by the individual using specialised software on a personal device.

B2 The principal argument for 'personal device only' is that of privacy. Some experts maintain that, since no other party can be trusted to act wholly in the individual's interest, an individual must be self-sufficient. He must maintain total control by locating his permission hub solely on a personal device (such as a laptop or mobile).

B3 Other experts understand the privacy arguments for a 'personal device only' architecture, but believe that – for many people, and when other factors are taken into account – a solution combining software on a local device with a managed service, provided by a broker, is likely to prove optimal. The factors are that:

- Control over a permission hub need not rely upon physical possession of the device on which the hub software resides. It should be possible to design software and governance policies to give an individual control over a server-based permission hub that is as close to total as makes no practical difference.
- An individual would find it catastrophic were his permission-hub to be lost, stolen or otherwise become unusable. But individuals are notoriously bad at arranging for back-ups. A hosted service would effect back-ups regularly and reliably.
- An individual may wish to access his permission-hub from multiple personal devices, and / or arrange for synchronisation of personal information between personal devices. Both tasks are easier if the master copy of the hub is located on a server.
- For certain permissioned attribute transfer transactions, the individual may wish to grant permission sometime ahead of the actual transaction. Direct debits or standing orders are good examples from the finance sector. In such cases, there is a clear need for the individual's permission hub to be permanently online, i.e. as a hosted service on a server.
- Since dishonest individuals can tamper with personal devices, it is probable that some relying parties will be unwilling to accept authentication assertions made directly by such devices, particularly for transactions that involve sensitive or valuable information. Rather they would prefer the greater assurance provided by the involvement of an independent broker – who is beyond the individual's reach, and can make authentication judgements based on the aggregation of a number of factors, including network location (IP address), shared secret (password), possession of token (such as a one-time-password device), and biometric (such as voice).
- Finally, locating a permission-hub on a server allows for the possibility that – for reasons of national security or crime prevention – the state may wish to examine an individual's permission hub. It is likely that some form of warrant, issued by the judiciary, would be required for such examination, akin in some ways to the search warrants that the police must obtain before entering a private house. Although no-one who values privacy likes to design systems in this way, it can be argued that UC-IPIM cannot be built without cooperation from the state, and allowing for lawful intercept may well be the price for such cooperation.

B4 All told, the Work Group's view on the issue of permission-hub location is that choice is paramount, both for the individual and for the various entities that may rely upon information received from the individual via his permission hub. In other words, some individuals may find

that, although they would prefer to maintain their permission-hub entirely on a local device, certain counterparties with whom they wish to establish a relationship insist on the use of a hosted service. The likely result is a mixed economy in which: (i) individuals can choose to use a single permission-hub for all relationships, or to use different permission-hubs for sets of relationships in different parts of their lives; and (ii) some hubs may be provided as a hosted service, and others may be entirely local, according to the preferences of both parties to a relationship.

Annex C Business model

C1 A UC-IPIM infrastructure can only be built on the foundation of a viable business model. The Work Group discussed 5 distinct possibilities: (i) no-one pays, i.e. the service is 'free' to all participants; (ii) the State pays; (iii) the individual pays; (iv) service providers pay; and (v) advertisers pay. Looking at each in turn:

C2 **No-one pays.** This can be ruled out. UC-IPIM can only be realised if: (i) one or more parties go to the effort and expense of creating the infrastructure; and (ii) other parties value the services that the infrastructure can deliver and are willing to pay enough to cover the costs. Various past initiatives have ignored this simple principle and – in consequence – have not succeeded. Even if the necessary code can be produced by open-source methods, other costs are inescapable – such as hosting, secure authentication, liability etc.

C3 **The State pays.** This also can be ruled out. It is hard to see how a service funded top-down by the Treasury could ever expand beyond a basic scope of facilitating interactions between the individual and the public sector. And such a restriction would defeat the purpose of UC-IPIM infrastructure – which is to facilitate interactions between the individual and many different counterparties, both organisational and individual, and from both public and private sectors.

C4 **The individual pays.** Theoretically, it would be possible to build a UC-IPIM infrastructure in which each individual is required, as a condition of participation, to purchase a local device (on which to carry his permission hub) that would be trusted by all likely counterparties as an issuer of acceptable authentication assertions. There would be a need for (i) a certification scheme to inform the individual, prior to purchase, which devices would be so trusted; and (ii) an insurance scheme whereby device manufacturers could indemnify relying parties against fraud, with – presumably – the associated costs being built into the device's purchase price. But, in practice, it seems unlikely that such schemes could ever succeed. Smart cards and mobile handsets are the nearest things we have at the moment to trusted personal devices, and – in the vast majority of cases – these are not bought outright by the individual; rather they are issued by a bank or a mobile network provider as one element of a service bundle. It is difficult to believe that this aspect of commercial and consumer behaviour will change as permission-hub services are introduced, although there may well be scope for the individual to pay for enhancements to a basic 'free' service.

C5 **Service providers pay.** If it is accepted that there is a need for at least a basic UC-IPIM service to be available free of charge to individuals, but that nevertheless there will be costs that have to be met, then service providers are the only likely source of funds. Arguably they will, or at least should, be glad to pay for outsourced authentication, and for automatic update of whatever details – such as home address, or seating preference for air travel, or contact details – that the individual chooses to disclose. The end result is likely to be something close to the banking/ credit card model, in which merchants pay for the costs of payment systems by way of transaction fees, and pass on such costs to their customers by way of higher prices.

C6 **Advertisers pay**. Conventional advertising would seem to run against the spirit of UC-IPIM because of its intrusive nature, beyond the control of the individual. It may be, however that advertisers can be regarded as simply potential service providers who do not yet have, but would like, a relationship with the individual, and are willing to pay for the chance to be considered. This is the world of reverse or permissioned marketing, and is a step towards the VRM [VRM] idea of using software tools to empower the individual to deal more effectively with multiple distinct vendors while protecting privacy. VRM is also defined, rather neatly, as the reciprocal of CRM, or customer relationship management.

C7 All told, the likely business model for a ubiquitous UC-IPIM infrastructure would seem to be 'service provider pays', with the possibility of some contribution to revenue from reversed or permissioned marketing, and some direct payments by individuals for additional services. Note that the model of 'service provider pays' has already been adopted by Government Gateway, where central government departments and local authorities pay the costs of the service in rough proportion to their usage of it.

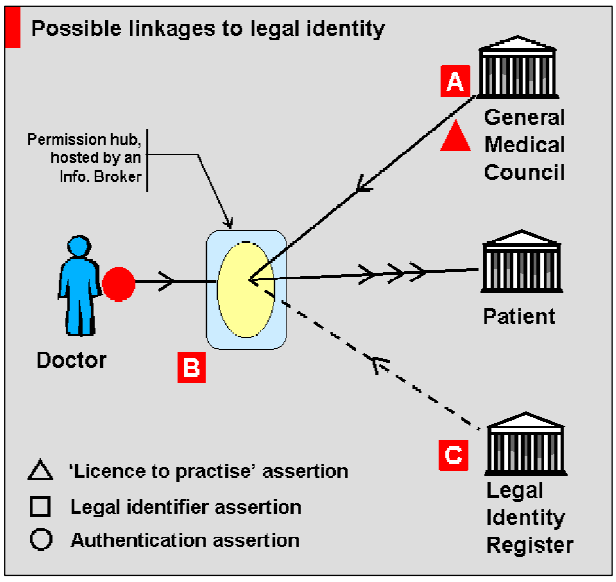
Annex D Touch points between UC-IPIM and 'legal identity'

D1 UC-IPIM infrastructure could be designed to enable an individual to transact anonymously, or pseudonymously, in all circumstances. Such a design would permit near perfect privacy, and make it very difficult for a counterparty – acting without the individual's consent – to link their records to those held by others, whether the state (i.e. legal identity) or any other organisation.

D2 But the privacy requirement must be balanced against legitimate requirements for transparency and auditability. In the real world, transactions can go wrong, and cause harm to an individual's reputation, health, or wealth. In consequence, a UC-IPIM infrastructure must enable an individual to require that any party requesting sight of sensitive personal information first disclose either his 'legal identity', or at least a credential indicating that he is acting on behalf of a legitimate authority. The requesting party can, of course, refuse to disclose his legal identity or credential, and so drop the request.

D3 To look at a simple example, suppose that – in response to an online request from someone purporting to be a doctor – an individual is considering whether to disclose his medical records. Before agreeing, he might reasonably require that the 'doctor' provide him with electronic proof of both her license to practise medicine (as granted by the General Medical Council, GMC) and her legal identity. There are various ways in which this could be arranged:

D4 **Scenario A1: GMC asserts self-issued identity.** GMC deems the doctor's training records to be satisfactory, and inscribes his self-issued identity (i.e. whatever name the doctor chooses to call himself) – along with the licence to practise medicine – on an electronic certificate. As a result, the doctor could find that his electronic CV comprises qualifications issued in different variations of the same name. If the variation is extreme, she may well have difficulty in convincing a patient of her bona-fides.



D5 **Scenario A2: GMC asserts legal identity.** Here the GMC requires the doctor to provide proof of his legal identity at the time of registration, perhaps by showing a paper passport, driving licence, or ID Card. Then, as in scenario A1, the GMC 'mints' a degree certificate showing both legal identity and degree details, and the doctor can use his permission-hub to show the certificate, and any others that may be relevant, to a patient.

D6 **Scenario B: Information Broker asserts legal identity.** Here the doctor's information broker requires that he prove his legal identity, perhaps by showing a paper passport or an ID card, prior to registering with the GMC. Then the student instructs the broker to pass details of his legal identity to the GMC as required for the registration process. Subsequently, the GMC can either

(i) mint an anonymous degree certificate, which the individual can combine with a legal identity certificate minted by the broker, and then show both to the employer; or

(ii) mint a degree certificate that shows both legal identity and license to practise, which the individual can then show to the potential patient, either alone, or backed up by a further certificate confirming legal identity issued by the broker.

D7 **Scenario C: Another entity asserts legal identity.** Here the doctor chooses to set-up a relationship between his information broker and a provider of legal identity attributes, perhaps a Unique National Register, or some online proxy. Subsequent steps are as Scenario B. The main difference between B and C is that, in the latter the broker only asserts authentication attributes, and thus accepts no responsibility / liability for the assertion of legal identity. This clear delineation of roles may well be desirable.

D8 It seems unnecessary – at this early stage – to specify which of the above scenarios is likely to prevail. We may, in fact, see a progression, from A1 through A2, and B all the way to C, as experience with UC-IPIM infrastructures develops.

Annex E Glossary & abbreviations

E1 The identity management field is plagued with ambiguous definitions and competing terminologies. This glossary does not attempt to set the world to rights in this area: rather it merely explains the meaning of various specialist terms and abbreviations as they have been used in the Work Group's discussions and are used in this document.

E2 Note also that glossary, like the paper itself, is concerned not with the entire field of identity management, but principally with the specific topic of user-centric identity and personal information management. Terms and alternative meanings, of relevance only to other topics, have been omitted.

Glossary & Abbreviations

Assertion	A statement made by an entity about one or more attributes.
Attribute	A fact recorded about an individual by a counterparty, or by the individual himself.
Authentication	The process by which an individual proves, to the satisfaction of a counterparty, that he or she is the rightful user of an identifier issued by that counterparty. May require that the individual demonstrate knowledge of a shared secret (e.g. password), possession of a token (e.g. smart card, one-time password generator), or some biometric characteristic (voice, face, etc).
Back-office information-sharing	See organisation-centric identity management.
Back-office identity management	See organisation-centric identity management
Broker	An organisation that may be commissioned by the individual to provide a hosted, server-side, permission-hub service
Common Authentication SErvice (CASe)	A method by which an individual can authenticate over electronic networks to multiple different counterparties using a single authentication process. Note that the counterparties may or may not use the same identifier for the individual. If they do not, CASe requires the use of trusted intermediary software (which may be located either on a personal device or a server) that permits authentication assertions to be transferred from one identifier to another.
Counterparty	Any entity, either individual or organisational, with whom an individual transacts and/or has a relationship
Entity	An individual or an organisation

Front-office information-sharing	See user-centric identity and personal information management.
Front-office identity-management	See user-centric identity and personal information management.
Identification	The process by which an entity distinguishes between another entity and all other entities in that other entity's peer group, and/ or the process of matching that other entity to a record created previously. Note that, in contrast to authentication, identification (i) does not necessarily require any action on the part of the individual; and (ii) does not presuppose a relationship, or likelihood of any future transaction, between the entity and the individual.
Legal identifier	A string, probably of letters and numbers, issued by the government of a nation state to distinguish an individual's record from the records of all other individuals with whom that state transacts.
Legal identity	That group of attributes recorded about an individual by the state prior to the issue of a legal identifier, together with the legal identifier itself. Usually comprises, as a minimum: name, date-of-birth, address, legal identifier, etc.
Organisation-centric identity-management.	The process by which two or more entities, typically organisations, create an aggregate record about an individual by direct sharing of information. Requires that the organisations match up their records, generally by comparison of certain key attributes of the individual, such as those that make-up legal identity. The individual may or may not be asked to consent to this process. If consent is sought, the request is typically made once only at the outset of a relationship between individual and counterparty, and is broad-brush in nature.
Permission-hub	Software, which may be located either on a personal device or a server, that enables an individual to select which attributes should be disclosed to which counterparty. Fulfils a necessary function in all UC-IPIM schemes.
Profile	That set of attributes which the individual decides should be disclosed to a particular counterparty, or group of counterparties. The terms *persona* and *partial identity* are also used to convey much the same meaning.
Pseudonym	An artificial / fictitious name used by an individual as an alternative to their legal name.
Self-issued identity	A profile comprised of attributes whose value has been asserted by the individual himself, without reference to any verifying entity.

Unique National Register (UNR)	The single register of 'legal identities', held by Government, in a mature identity management infrastructure in which user-centric and organisation-centric components are balanced. The Work Group makes no comment as to the similarities, or otherwise, between a UNR and the current National Identity Scheme.
User-centric identity and personal information management. (UC-IPIM)	A process in which an individual is given, either in paper or electronic form, a tamper-resistant copy of information recorded about him by a counterparty, such that he can then elect to show such information to any other counterparty of his choice. Or, put another way: "UC-IPIM is a technical and regulatory system designed to improve control and convenience of individuals in their dealing with service providers with regard to authentication and disclosure of information that is considered private"
Verification	The process by which an entity confirms that an attribute pertaining to another entity is true. Can be regarded as a superset of, but should not be confused with, authentication
Work Group	This Work Group on User-Centric Identity (and Personal Information) Management.

Annex F References

CRO. ‘Challenges and opportunities in *identity* assurance', the report of a review led commissioned by Gordon Brown, and led by Sir James Crosby. Available at http://www.hm-treasury.gov.uk/independent_reviews/identity_management/identity_management_index.cfm

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

HIG Project Higgins. See http://www.eclipse.org/higgins/

ICO ‘New approaches to identity management and privacy’, published by the Information Commissioner’s Office and available at : http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx

INF Information Cards. See http://www.microsoft.com/net/windowscardspace.aspx. Cardspace is the Microsoft trademark for Information Cards, which is an open standard.

ISA The Independent Safeguarding Authority. See http://www.isa-gov.org.uk/

ITS ITSO. A UK organisation that seeks to create standards for interoperable smart card ticketing in the transport sector. See http://www.itso.org.uk

LIB Liberty Alliance. See http://www.projectliberty.org/

MIAP ‘Managing Information Across Partners’, a project funded by DCSF. See http://www.miap.gov.uk/

MYD Mydex. See http://mydex.org/

OPE OpenID. See http://openid.net/

PAO PAOGA Ltd. See http:// www.paoga.com/

PIB Personal Information Brokerage. See http://www.edentity.co.uk

PLA Plaxo. See http://www.plaxo.com

SAM OASIS Security Services (SAML) Technical Committee. See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

TAS TAS^3. See http://tas3.eu

UKF The UK Access Management Federation. See http://www.**uk**federation.org.**uk**/

VRM Vendor Relationship Management. See http://cyber.law.harvard.edu/projectvrm/Main_Page

---

Annex G Contributors to the Work Group

The following individuals contributed to the Work Group, either by attending one or more of the face-to-face meetings, or by contributing to the online discussions. As already stated, the views expressed in this report merely represent an overview of discussions in the Work Group, and do not necessarily reflect the views of every participant or the organisations they represent.

This report was written by John Harrison of Edentity with the help of other participants in the group.

Name	Organisation
Paul Hodgson	BT
Piotr Cofta	BT
Andy Clark	Detica
John Harrison	Edentity
Paul Hopkins	Edentity
Simon Enefer	Equifax
Dave Wright	EURIM
Patrick Maynard	Giesecke & Devrient
Adrian Johnston	Government Gateway
Jim Purves	Government Gateway
Pete Bramhall	Hewlett Packard Labs
William Heath	Mydex
Andy Smith	Identity & Passport Service
John Leach	Information Assurance Advisory Council (IAAC)
Peter Tomlinson	Iosis Associates
Julian Jones	IST44
Josh Howlett	JANET
James Farnhill	JISC
Matthew Dovey	JISC
John Larmouth	Larmouth T&PDS
Andy Waters	Metropolitan Police
Clive Gerrard	University of Newcastle
Fred Piper	Royal Holloway, University of London

…./continued on next page

Geoff Llewellyn	RPM
John Walker	Secure-Bastion
Phil Steeples	StartLok
Robin Wilton	Sun Microsystems
Conn Crawford	Sunderland City Council
David Rennie	
Andrew Churchill.	Telsecure
Iain Henderson	Mydex
Richard Trevorah	tScheme
Angela Sasse	University College London
Andy Voysey	UK Council for Electronic Business
Johnnes Arreymbi	University of East London
Bruce Christianson	University of Hertfordshire
David Chadwick	University of Kent
George Inman	University of Kent
Simon Cotterill	University of Newcastle
Nick Hopkins	Virgin Media
Martin Pickford	VocaLink
Peter Seymour	VocaLink
Steve Babbage	Vodafone
Dylan Evans	Vox Generation Ltd (Voxgen)
Richard Walton	Walton-Mackenzie
Simon Willison	
