House of Lords Science & Technology Committee

Investigation into Personal Internet Security, chaired by Lord Broers

Submission of evidence by **Edentity Ltd**, November 2006

(Abridged by Edentity, Nov 2007, for Gateway Product Steering Group)

With support from the following individuals, all acting in a personal capacity:

Jean Bacon, Professor of Distributed Systems, Computing Lab, University of Cambridge
Brian Collins, Professor of Information Systems, Cranfield University
Matthew J. Dovey, Programme Director, JISC
Paul Hopkins, Director of Information Systems and Services, Newcastle University
Stuart Jones, Assistant Director (Policy, Learning & Skills), BECTA
John Madelin, Head of UK Security Practice, BT Group plc
Mike Martin, visiting Professor, Centre for Social and Business Informatics, Newcastle University
Fred Piper, Emeritus Prof. of Mathematics / Information Security, Royal Holloway, Univ. of London
Gwyn Roberts, Head of Corporate Development, Virgin Mobile (part of the ntl Group)
Rob Ward, Director, The Centre for Recording Achievement
Steve Williams, Head of ICT, Sunderland City Council

Edentity Ltd
The Millers House
Church Road, Shaw
Newbury RG14 2DL

Contact : John Harrison
E-mail: john.harrison@edentity.co.uk
Telephone: 07801 231 693

About Edentity

Edentity is a tiny development company that specialises in the emerging field of personal information brokerage (PIB), and - particularly - in those PIB applications that have the potential to straddle public and private sectors. We seek to be a catalyst in the creation of infrastructure that will:

- enable individuals to interact with organisations, and other people, in a way that is both more convenient and offers enhanced protection of their security and privacy; and
- help organisations move towards better ways of authenticating, and maintaining accurate information about, their customers.

Edentity was founded in 2000. In a first phase of work, we carried out a feasibility study of our ideas in collaboration with the Computer Lab at the University of Cambridge, with partial funding provided by the DTI. We then led three near-miss bids for research funding to the EU and HMG, with the likes of Experian, Ericsson, Sun Microsystems and the DfES as partners. More recently we have turned our hand to consultancy work, carrying out projects for local authorities, for the Office of National Statistics, for Eduserv (a charity) and for BECTA (a body that advises DfES on IT strategy in secondary education). Our attention is now turning to the running of a pilot, focused on the education sector, as a step towards critical mass.

Introduction & Summary

1. The internet sprang out of work funded by the US Advanced Research Projects Agency (ARPA) back in the 1960s. It was designed primarily for resilience, and scaleability. Little thought was devoted to the areas of security and identity, in part because those involved in the project did not anticipate the invention of the consumer-friendly web in 1993, the explosion in usage that followed, and the richness of applications that we now take for granted. As a consequence, there are real problems in the area of personal security over the internet, and these are linked inextricably with the broader problem of identity.

2. In this submission, we: describe a number of linked problem areas, outline a possible solution that we call Personal Information Brokerage[1] (PIB), explain how initiatives in user-centric identity management (such as PIB) differ from organisation-centric approaches (such as the Home Office's ID card), review earlier attempts to solve the network identity problem, give more details about the PIB technology, applications, and organisation/ business model, and finally explain why we believe that critical mass can be attained by working in partnership with the education sector.

3. We also explain that our plans to run a pilot of PIB are winning broad support, but may yet be frustrated by the Department of Education and Skills' current preference for building yet another (virtual) national database, this time of qualification data. We maintain that such data is positive in nature, and is best aggregated by the individual, and then shown to selected third parties, using an e-portfolio application provided by an information broker.

The problems

4. In the absence of any infrastructural approach, every organisation must devise its own means for identifying and authenticating individuals over the internet. Most opt for variants of username / password, in which the username serves as the identifier, and the password as a shared secret, knowledge of which authenticates the individual.

5. Criminals exploit the weak security offered by passwords, typically to steal money from online bank accounts. In a common attack, known as 'phishing', criminals send out mass e-mails in the name of a well known website, typically belonging to a financial institution. The recipients who follow instructions in the e-mail will visit a fake website, enter their usernames and passwords, and soon find that their accounts have been emptied.

6. The magnitude of the financial losses suffered as a result of phishing is hard to quantify, in part because consumers are often recompensed quickly by the service provider in an effort to avoid publicity. However, most of the harm may be indirect: many consumers now refuse to use online services because of the perceived security risk, and – in consequence – the operational costs of organisations are not falling as quickly as they might.

7. A second issue is the insecurity of e-mail. Because conventional e-mail can be read at any server through which it passes, the e-mail system is generally not used for messages of any sensitivity or value. Instead some service providers persist in using conventional paper-based mail. Others send electronic messages to personal mailboxes held on their own servers, and require an individual to log-in before they can read them. If this latter solution becomes widespread, individuals will find that the task of authenticating separately to every possible correspondent becomes burdensome.

8. A third, related, issue is the inability of the individual to transmit personal information recorded by one third party to another electronically, and convince the recipient that the information is genuine. As examples, consider a paper medical prescription, or a paper exam certificate. These are tamper-proof copies of information recorded about an individual by qualified counterparties, and can be shown by the holder to other counterparties to effect transactions for her own benefit. An individual cannot replicate this functionality over the internet. Although it is possible for an individual to send, say, details of exam results to a counterparty by e-mail, what she cannot do is convince the counterparty that the results are genuine.

9. A fourth issue is the lack of infrastructure that would enable an individual to update common personal attributes – such as name, contact details, and preferences – held by multiple different third parties in an easy and secure manner. One good illustration is the fact that anyone who

[1] In the past, we have used other names, i.e. 'Personal Digital Identity' and 'Virtual Home', a trade-mark.

moves house must still spend many hours informing counterparties manually of their new address. Although various proprietary solutions to this problem do exist, such as Plaxo, Linked-In and Iammoving, they all lack interoperability and can thus neither be scaled into an infrastructural solution, nor accepted as a primary means of delivering public-sector applications.

10. These problems are experienced across all sectors of the economy: in education, commerce, health, local government, and finance. In each sector, there is increasing recognition that the delivery of complex services requires personalisation, and that personalisation in turn requires that there be a secure and convenient electronic method to convey sensitive personal information between the individual and *multiple* distinct service providers.

Solutions & barriers

11. The weakness of passwords as an authentication mechanism has long been realised, and better methods are available. One example is One-Time Password (OTP). Here a service provider issues an individual with a small electronic device, equipped with a single button and a display, often in the form of a key-ring fob. To authenticate to the service provider, the individual browses to its website, and enters both his username, and a multi-digit number obtained by pressing the button on the device. Software on the server is synchronised with the device, and thus recognises the number even though it changes on every button press. OTP eliminates the risk of phishing.

12. Technically, there is no reason why OTP functionality cannot be delivered using a mobile phone, rather than a special-purpose device. Indeed, one company in the UK - Monitise - has already signed contracts with all the mobile network operators to deliver such a service under the brand name Accode. See http://www.monitise.com/products-and-services/accode.

13. Other forms of strong authentication are available. BT is said to be developing a service that uses voice recognition to authenticate an individual who makes contact by 'phone. Some manufacturers offer small card-reading devices that can be combined with a standard chip-and-pin payment card to deliver OTP functionality. And there remains the classic PKI[2] private key, which can be stored on any personal electronic device, such as a smart card, a PDA, or a computer.

14. While all these forms of strong authentication work technically, there remain significant barriers to take up:

    - Cost. Implementing OTP, or another form of strong authentication, costs much more than conventional username/ password, and many service providers find it difficult to justify the expenditure. They prefer, instead, to tolerate modest levels of fraud, and reimburse the victims.
    - Convenience. While it is not hard to persuade an individual to carry one OTP device as a key-ring fob, it seems unlikely that anyone would be willing to carry a separate fob for every service provider with which they deal.

15. The way to overcome these barriers is, conceptually, simple. There is a need for a new kind of service provider, one that we call an information broker. An individual will commission one or more such brokers to intermediate in his network relationships. To transact, the individual authenticates to his broker, who then passes on details of the authentication process to the relevant service provider. Because one broker acts as intermediary for many relationships, it becomes practical to spend a reasonable amount of money to ensure that the authentication process itself is secure.

16. An information broker could also provide the individual with a secure 'permission hub', with which he can control the transmission of personal attributes to, and between, third parties. Such a hub could enable many useful applications, in addition to secure single-sign-on. They range from secure messaging and voice-over-IP to single-point-change-of-contact-details, from intelligent redirection of conventional mail to permissioned marketing, from person-centric record aggregation to transfer of attendance data, and from parental access to storage of accessibility preferences.

17. Edentity has been developing this approach, which we now call Personal Information Brokerage (PIB), for several years. PIB can be seen as one initiative in a field that has come to be known as

[2] PKI = Public Key Infrastructure, a security technology.

'*user-centric identity management'*. We will give more details about PIB, and its possible initial implementation in partnership with the education sector, later in this submission. But first we will contrast *user-centric* identity management with the alternative, *organisation-centric*, approach; and then review the history of earlier attempts to crack the network identity problem.

User-centric vs. organisation-centric identity management ?

18. User-centric identity management recognises that an individual has a distinct e-identity for each service provider with which he deals, and seeks ways to provide him with the means to: (i) sign-on securely and conveniently to multiple services providers, and (ii) give explicit transaction-based permission for the transfer of personal information to, and between, service providers.

19. Because of the importance placed on individual privacy, user-centric designs tend to employ relationship-specific identifiers. The alternative, a globally unique identifier, would make it too easy for untrustworthy service providers to exchange personal information without the individual's permission.

20. The emphasis on privacy and permission also means that user-centricity is only suitable where the individual has a choice between service providers, and where the net outcome of a transaction is likely to be perceived as beneficial. Thus the private sector would be fertile ground for user-centric identity management, were it not for the difficulty of developing the consensus necessary to attain critical mass. The answer may be to work *initially* with those parts of the public sector where individuals: (i) have a choice between service providers; and (ii) are, or can easily become, IT-literate. More on this later.

21. Looking now at organisation-centric identity management, here a closely-linked group of entities seeks to reduce the multiple e-identities by which a particular customer or employee may be known to a single instance, typically represented by a single identification number. The individual then has little control over the transmission of personal information between the entities, and must rely on their internal authorisation policies to protect his privacy.

22. The Home Office's Identity Card Project is clearly an organisation-centric approach, and seems appropriate for the central government organisations which already share personal data between their back-offices, and with which an individual has no choice but to maintain a life-long relationship, i.e. the Home Office (Passport, Criminal Records), the DVLA, the DWP, and HMRC.

23. The NHS 'Connecting for Health' programme is also organisation-centric, being based on a perception of the NHS as a single, massive organisation, with which an individual will have a single relationship and a single health record. The benefit is that an individual's health records can be viewed by NHS staff throughout the country. But there are drawbacks:

    - Privacy. Celebrities can opt for private health care, and thus are able to prevent personal information appearing in the NHS's systems. But there has been complaint that DfES's compulsory IS Index project, which is designed to improve child protection and springs from the same conceptual family as 'Connecting for Health', offers insufficient protection for the privacy of celebrities' children. To which the inevitable rejoinder must be, 'If it isn't good enough for celebrities, why is it supposed to be good enough for the rest of us ?'
    - Authentication. There is no provision in 'Connecting for Health' to authenticate individuals to a level high enough to allow them to inspect their own health records on line.
    - Interoperability. There is no provision in 'Connecting for Health' to enable an individual to show her own health records to medical professionals in the private sector, or abroad.

Earlier attempts to crack the network identity problem

24. Efforts to fix the problems with personal security over the internet have been pursued, sporadically, ever since the medium really became popular back in the 1990s. The roll call starts with Microsoft's Passport and Hailstorm, and then progresses to the Liberty Alliance, Shibboleth, Microsoft Cardspace, and OASIS SAML.

Microsoft

25. Network intermediation is an old idea. The first major initiative started in 1999, when Microsoft bought out a start-up, Firefly, and commenced efforts to transform its single-sign-on (SSO) service, Passport, into a utility for the web. In 2004, the company finally admitted that Passport

had not achieved its take-up targets, and that in the future would be used only as a SSO service for its own web properties.

26. In 2001, midway through its attempts to roll-out Passport, Microsoft announced an even more ambitious project, Hailstorm, that would store all kinds of personal information, and intermediate between the individual and service providers. Unsurprisingly, few service providers were willing to contemplate a future in which Microsoft interfered with their customer relationships, and so Hailstorm never made it to market, foreshadowing the eventual change of direction for Passport. However, the threat of Hailstorm existed for long enough to provoke the formation, in late 2001, of a new standards body for digital identity, the Liberty Alliance, of which more later.

27. After the setbacks with Hailstorm and Passport, Microsoft went quiet about digital identity. Then, in 2004, one Kim Cameron emerged as the company's architect for identity and access and provoked a flurry of discussion in the identity community by blogging about seven 'laws', to which - he maintained - any emerging identity system must conform. See www.identityblog.com.

28. In early 2005, Cameron began to speak about Microsoft's next identity initiative, an 'identity meta-system' coupled with a desktop interface, now called 'Cardspace', which is to be bundled with the next release of Windows, Vista. Cardspace is built around a business-card metaphor, and invites an individual to select which 'card' of attributes he wishes to disclose in which contexts. Each card is a representation of, and pointer to, personal attributes held on a counterparty's database.

29. Cardspace is, clearly, a user-centric approach to identity management. But Microsoft has learned from experience that service providers will not allow it to be a mass-market server-side intermediary, and so was obliged to make Cardspace into a desk-top solution, building on its Windows monopoly. But the decision can not have been an easy one, for several reasons:

    - using Cardspace, an individual's computer itself becomes the second factor required for secure authentication, despite the fact personal computers are insecure and, even in the lap-top form-factor, are rather bulky;
    - the data held within Cardspace will need to be backed-up, and synchronised across multiple devices, indicating the need for a (costly) server-side implementation;
    - there are applications for which it is convenient for an individual's identity nexus to be permanently online; and
    - Cardspace lacks any form of business model, and thus there is scant incentive for service providers to participate.

The Liberty Alliance

30. In 2001, at about the time that Microsoft was trying to win support for its Hailstorm initiative, a number of technology and consumer-facing companies came together in order to establish 'an open-standard for federated network identity through open technical specifications'. The grouping is called the Liberty Alliance (www.projectliberty.org) and now counts Sun Microsystems, HP, Intel, Nokia, Ericsson, Amex, NTT, Vodafone and a number of public bodies among its members.

31. Liberty has chosen to divide its task into three main areas: a federation framework, a web-services framework, and service interface specifications. Work in the first of these areas has already been donated to OASIS, and will inform the development of the SAML standard (of which more below). It seems likely that standards in the remaining two areas will follow the same path, although no announcements have been made.

32. As yet there have been few large-scale consumer deployments of the Liberty standards. Many in the identity community believe that this is because the Liberty members are generally large organisations who are unwilling, for commercial reasons, to cede control of personal data to the data subject. Their mindset appears to be primarily one of 'organisation-centric identity management', as defined earlier. Note, however, that Liberty now emphasises that its standards can also be used to enable user-centric implementations.

33. In a much-cited Liberty use-case, an airline acts as an 'Identity Provider (IdP)' and leads a 'Circle of Trust (CoT)' in which car-hire and hotel companies act as 'Service Providers (SPs)'. Instead of maintaining separate username-passwords for each entity, an individual can choose to 'federate' his identities, and enjoy single-sign-on (SSO) – using the IdP username-password – to all entities within the CoT. In this example, it is clear that the CoT is under control of the IdP, and that the individual is constrained to use SSO, and related attribute transfer services, only for SPs that have some form of marketing agreement with the IdP.

Shibboleth

34. Shibboleth is a further example of organisation-centric identity management. It emerged from the Internet2 (http://shibboleth.internet2.edu/) grouping of universities in the USA as a solution to the problem of how students and academics of one university could be given easy access to web resources belonging to other organisations – such as other academic institutions and publishers of academic journals.

35. Using Liberty terminology, a student's home university acts as the Identity Provider, and resource providers are the Service Providers. All the parties negotiate trust agreements within a Circle of Trust, which is sometimes called a federation.

36. Shibboleth is now being implemented in the UK education sector. Following a number of pilots and studies, JISC[3] has decided to replace the Athens access management service, used in higher education, with the Shibboleth approach. UKERNA[4] is to provide the necessary central services, and Eduserv[5], the provider of Athens, has developed various inter-system gateways to help HE institutions make the transition. In a parallel exercise, BECTA[6] as also opted to implement Shibboleth at the secondary level, and again has commissioned UKERNA to provide the necessary central services.

OASIS SAML

37. A standards group, OASIS (www.oasis-open.org), has developed the Security Assertion Mark-up Language, known as SAML. The Liberty Alliance donated significant chunks of it work to OASIS, and Internet2 have done likewise. In consequence, the second release of the SAML – 2.0 – is a generalisation of the Liberty and Shibboleth approaches, and is broadly applicable.

PIB - technology, business model, applications, and implementation.

38. Microsoft's idea of Passport / Hailstorm as a user-centric intermediary for network transactions was, in many ways, correct. The initiatives failed for a number of reasons, primarily: (i) an individual must be able to choose between a number of competing intermediaries, and not be forced to use a monopoly provider; (ii) Microsoft was not trusted; (iii) there was insufficient buy-in from service providers; and (iv) certain necessary technical innovations and standards were not then in place. If the public and private sectors in the UK can work together, there is now a possibility of revisiting the topic of intermediation, and getting it right. Edentity calls the project Personal Information Brokerage (PIB).

How PIB works

39. Central to PIB is the idea that an individual will use one or more points in the network space – which we call permission hubs – to give explicit, transaction-based, consent for the sharing of personal attributes between counterparties. Since these attributes may include descriptors of an authentication process, a further tenet of PIB is that authentication is, potentially, a pure web service that counterparties will outsource to the organisations that host individuals' permission hubs.

40. We call these organisations identity or information brokers. Logically, an information broker is an individual's agent, and thus must be commissioned by the individual rather than by any counterparty that will consume its services. Further, a broker may choose to provide authentication in-house, or may outsource the requirement to a specialist counterparty, an authentication service provider.

41. The likely candidates for the authentication role are the mobile network operators, and possibly the banks, who can provide secure authentication at low cost as a result of their existing activities. In time, these organisations may also assume the broker role. In the nearer term, brokers may be public or third sector organisations, possibly from the education sector or local government sectors.

[3] The Joint Information Systems Committee (JISC) is funded by HEFCE to develop strategy, and fund development, of IT systems for the Higher Education (HE) sector. See www.jisc.ac.uk

[4] UKERNA is the publicly owned organisation that delivers IT infrastructure for the HE sector. See www.ukerna.ac.uk

[5] Eduserv is a charity that provides IT services to the education sector. See www.eduserv.org.uk.

[6] The British Education Communications & Technology Agency (BECTA), a non-departmental public body, supports all four national government education departments to develop ICT for the secondary and primary sectors. See www.becta.org.uk

42. An important feature of PIB is the use of a counterparty's role, allocated either by an individual or by a supervisory body, to engender trust and to help the individual control – in a simply and intuitive way – which counterparty sees which attributes. As examples, only an organisation certified by DfES to fulfil the role of awarding body would be entitled to assert public qualifications, and only prospective employers and learning providers would – by default – be given access to an individual's qualification record.

Business model

43. Turning now to the commercial model, service providers will pay brokers for: (i) the provision of a secure relationship with an individual, and for updates on attributes that the individual has chosen to disclose; and /or (ii) the chance to supply marketing material to an individual who has chosen to disclose certain profile attributes, using a combination of a pseudonymity and forwarding to protect privacy. (The use of a PO Box number for conventional mail is a close analogy.) Other individuals, with whom the individual chooses to maintain personal relationships, will pay nothing.

44. Since any one service provider will have to deal with multiple information brokers, and could not negotiate separate tariffs with each, there is need for collaboration. Specifically, we envisage that service providers and brokers will negotiate contractual and commercial relationships under the auspices of a new body, one that we call an eXtensible Circle of Trust (XCOT). Small service providers may choose to be represented jointly within XCOT, either by direct collaboration, or by hiring an agent commercially. There are clear parallels here with the organisational models developed by the credit card networks.

Applications

45. There are many applications for PIB, over and above secure single-sign-on. Generally, they all derive from the capacity of the infrastructure to enable secure communication between the individual and multiple counterparties, and – in some cases – the use of pseudonymous identifiers to protect privacy. The initial application groupings are:

46. Access control. An individual will use a PIB broker account as the means to gain access to his learning provider's systems; and (ii) to web resources, provided by other organisations, to which he is granted access as a consequence of his relationship with the learning provider. This second point means that the Shibboleth functionality, described earlier, will be subsumed within PIB.

47. *Communication.* Most large-scale Instant Messaging and Voice-over-IP applications (e.g. AOL, Skype, and MSN) lack interoperability, and thus can only be used between individuals who maintain accounts with the same service provider. To use a banking analogy, this is equivalent to insisting that everyone maintain accounts with the Bank of England, rather than with interoperable retail banks. PIB should crack this problem, providing both interoperable instant messaging / voice communication, and a secure equivalent of e-mail.

48. *Record Aggregation*. PIB enables the individual to aggregate records of transactions with counterparties in a particular sector, and then show the composite record to chosen third parties. In the near-term, one obvious application is to create a learner-centric qualification record (of which more below). In the longer term, the principles could be applied in other sectors, provided that the records are generally positive in nature.

49. *Location & attendance.* An individual will be able to use his permission-hub to control the transfer of data about his physical presence to third parties. Such data may be provided:

    a) by a mobile network operator, using triangulation to locate a handset between transmitter masts. One obvious application is for concerned parents to keep an eye on the whereabouts of their children

    b) by a school or college that records a student's attendance manually. This could be used to improve the administration of the DfES's Education Maintenance Allowance Scheme, which pays students, who are between the ages of 16-19 and from low-income families, up to £30 a week provided that they attend college regularly.

50. *Mail Redirection.* Shopping over the internet is increasing, in part because people are becoming busier. But the very fact that people are busier means that they are often not at home to accept the parcels when delivered. Using PIB, a sender could append an address for the recipient's permission hub to a conventional street address. Then, if nobody is at home to accept a parcel, the delivery agent could – by virtue of his employer's role as certified by Postcomm – interrogate the recipient's permission hub for a standby address, deliver accordingly, and inform the recipient

by secure mail. Later on, a permission-hub address could be used as replacement for a street address, enabling a delivery company to look-up the recipient's desired delivery address as the parcel passes through the sorting office.

51. *Marketing.* In the prevalent internet marketing model, merchants post public advertisements, often on search engine listings, in order to persuade customers to *visit* their sites. But there remains untapped potential for:

    a) merchants to *send* marketing material – either in paper or electronic form – to individuals in response to a specific request. Here, an individual will browse an enhanced yellow-pages type directory, and then instruct his information broker to send a 'special' permission-hub address to merchants of interest, requesting marketing material to be provided within, say, a two-week window; and

    b) merchants to *send* unsolicited marketing material, again either in paper or electronic form, to individuals. Here, an individual will give his broker permission to (i) disclose a pseudonymous profile, probably aggregated with that of others; and then (ii) invite merchants to bid for the right to send unsolicited material, at a rate (say 5 – 10 a month) specified by each individual.

52. In both these marketing applications, the individual's privacy is protected by the fact that the permission-hub address divulged to a merchant will be a one-time pseudonym. Marketing material sent to the pseudonymous address will be forwarded by the information broker, provided that the merchant has observed the time or volume constraint. Merchants will pay information brokers for each lead, possibly at rate high enough to offset a significant proportion of the infrastructure's overall cost.

Route to critical mass

53. Information brokers are intermediaries, and can only reach critical mass if a sizeable grouping of service providers believes that the benefits of secure intermediation exceed the risks from interference in their direct relationships with customers, and have the capacity to act in concert to adopt common infrastructure. It is hard to identify such a grouping in the private sector.

54. In the public sector, central government needs infrastructure for data sharing, and has (rightly) chosen an organisation-centric model. Health has also chosen an organisation-centric model. Local authorities are uncertain as to whether they are independent entities, or extensions of central government, but for data-sharing purposes tend to the latter view.

55. Which brings us to the education sector. Schools and universities are autonomous organisations, and most desire to retain distinct relationships with their students rather than being subsumed with a 'national education service'. And the sector also meets two other requirements for PIB: (i) most of the data to be shared – such as qualifications – is positive in nature, and thus suitable for a learner-permissioned approach; and (ii) schools and universities can act in concert to adopt common infrastructure when given the right signals.

56. Note also that individuals in the education sector tend to be young and technically literate, and so most should be able master the use of a permission hub easily. For those who encounter difficulty, their learning provider will be able to provide support. Also, the design for PIB provides for a parent, carer or guardian to maintain a permission hub on behalf of someone who is unable to do so herself.

57. In a 2005 strategy paper, entitled 'Harnessing Technology. . ', the Department for Education and Skills committed to the roll-out of a national approach to what is called an 'e-portfolio', essentially an on-line space in which learners can store validated qualifications, samples of their own work, and reflections about their progress. In time, it is expected that a learner will use her e-portfolio to make applications, from school to university, and then from university into the workplace.

58. There are clear advantages in delivering the qualification record element of e-portfolio using a learner-centric, rather than an organisation-centric, approach to system design and identity management. Specifically the learner-centric approach can: (i) scale indefinitely, allowing the individual to collect qualifications from anywhere, rather than just from a national silo; (ii) allocate cost and benefits fairly by use of transaction payments – thus avoiding the need for sizeable Treasury subventions; (iii) enhance learner privacy; (iv) reduce total cost per application by creating infrastructure that can be used for many user-centric data-sharing applications; and (v) fix the issue of how to authenticate a learner securely prior to giving him access to his qualification record. Thus e-portfolio may present an opportunity to drive PIB to critical mass.

A pilot

59. PIB has now been the subject of paper-based development for several years. Functional specifications for the various software components are nearing completion; and the next stage is to work-up and cost technical specifications. But the project cannot proceed further until there is a clear prospect of running a pilot, which will focus on (a component of) e-portfolio, and learner transition between institutions.

60. The likely participants in the pilot would be: a grouping of universities; a grouping of secondary schools and FE colleges; UCAS, as the means to connect a learner's electronic identities at the secondary and tertiary levels; two or more of the principal public examination boards; and two or more potential information brokers / authentication service providers.

61. Given the diversity of the potential participants, we believe that the first step should be a scoping study. This would take 3-6 months, and result in a fully-worked up proposal for a 3+ year pilot. Edentity is now working hard to build support for the scoping study.

Support, and the lack of it

62. PIB has been discussed widely with academics in the field of computer science, with organisations in the education sector, and with potential information brokers and authentication service providers.

63. The approach now enjoys either support, or strong interest, from relevant individuals, all acting – for the moment – in their personal capacities:

    - Jean Bacon, Professor of Distributed Systems, University of Cambridge Computer Laboratory.
    - Brian Collins, Professor of Information Systems, Cranfield University. He is also Vice President of the British Computer Society, and was specialist adviser to the Home Office Select Committee's work on Identity cards.
    - Matthew J. Dovey, Programme Director, JISC. Matthew is responsible for JISC's e-Infrastructure development programme.
    - Paul Hopkins, Director of Information Systems and Services, Newcastle University. Paul is keen that Newcastle should participate in a PIB pilot, probably leading a consortium of the 5 NE universities.
    - Stuart Jones, Assistant Director (Policy, Learning & Skills), BECTA. Stuart is responsible for BECTA's work on e-portfolio.
    - John Madelin, Head of UK Security Practice, BT Group plc
    - Mike Martin, visiting professor, Centre for Social & Business Informatics, Newcastle University
    - Fred Piper, Emeritus Professor of Mathematics / Information Security, Information Security Group, Royal Holloway, University of London.
    - Gwyn Roberts, Head of Corporate Development, Virgin Mobile (part of the ntl Group). Virgin Mobile may be interested in the role of information broker.
    - Rob Ward, Director, The Centre for Recording Achievement. The CRA exists to promote good practice in recording achievement, and thus has a strong pedagogical interest in e-portfolio infrastructure.
    - Steve Williams, Head of ICT, Sunderland City Council. Sunderland has pioneered the usage of smart cards and Liberty Alliance standards for digital ID in the public sector, and currently provides secure-single-sign-on for 8,500 students at the local university. They see the information broker role as a logical next step, and are keen to experiment.

64. Organisations, by their nature, move more slowly. Some indication of the emergent positions of relevant organisations is given above, by virtue of the willingness of individuals to express a personal interest. Further comments follow:

    - BECTA has responsibility for both the implementation of Shibboleth (see earlier) in the secondary sector, and for work on e-portfolio. The leaders of both teams are interested in PIB, and one is pursuing discussions about a corporate approach with senior management colleagues. Progress has been delayed by the fact that DfES has reserved the area of identity management in education to itself.
    - JISC is governed by a number of fairly autonomous sub-committees, and now recognises that – since PIB cuts across the remit of at least three committees, but falls squarely within the

remit of none – there is a risk that it will attract neither funding nor support. Discussions are now underway to correct this problem, but we have yet to see the results.

- UCAS has been aware of PIB since August this year. Senior individuals there now recognise the potential importance of the project to the organisation's future role, and discussions about a corporate response are underway.
- The Royal Mail Group has been aware of the PIB mail redirection and marketing applications for some years, and individuals have expressed support, but the 'timing has never been right' for work to be taken forward on a corporate basis. Fortunately there is now renewed interest, and progress may soon be possible.
- Edentity is in discussion with one other mobile network operator, in addition to Virgin Mobile, about the broker and authentication service provider roles. While there is interest from individuals, there is as yet no movement at the corporate level.

65. Individual users, en masse, form a significant stakeholder group. Edentity has carried out a small formal market research study, and has spoken about the PIB concept informally to many people. On the basis of this work, we are confident that the great majority of individuals would prefer personal control over the use of their personal information, rather than surrendering it to another national database. Also, they are tired of the inconvenience and insecurity of the username/ password approach to authentication for the web, and would welcome progress.
