

Putting the user *back in charge* over his *identity*

Linking web-service identities to real world
identity (if the individual so desires)

A proposal for trusted user-centric infrastructure:
Personal Information Brokerage (PIB)

LSEC conference
3-4 December 2009

John Harrison



About Eidentity

- Various granted patents
- But a **market-maker**, not a typical tech start-up
- 3 staff, privately funded

Advisory Board

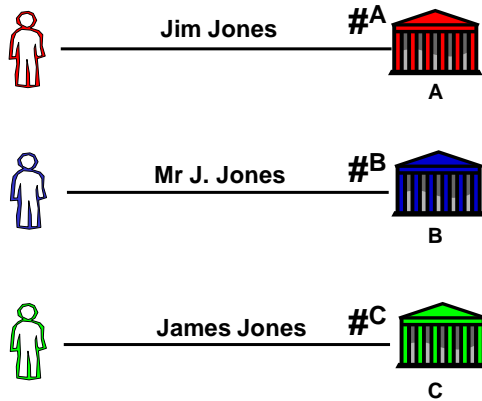
- **Prof Jim Norton**
e-gov expert, Institute of Directors
- **Prof Fred Piper**
security expert, Royal Holloway
- **Dr Nick Spencer**
former head of innovation, Vodafone

- 2008**
 - Led the Work Group on UC-IdM, as sponsored by:
 - UK Information Commissioner; &
 - UK's Technology Strategy Board

- 2007**
 - Advice to UK Info. Commissioner
 - Discussions with UK IPS
 - Led conference re IdM
 - focused on public sector
 - at Oxford Internet Institute
 - sponsored by JISC, ICO, etc



Problems



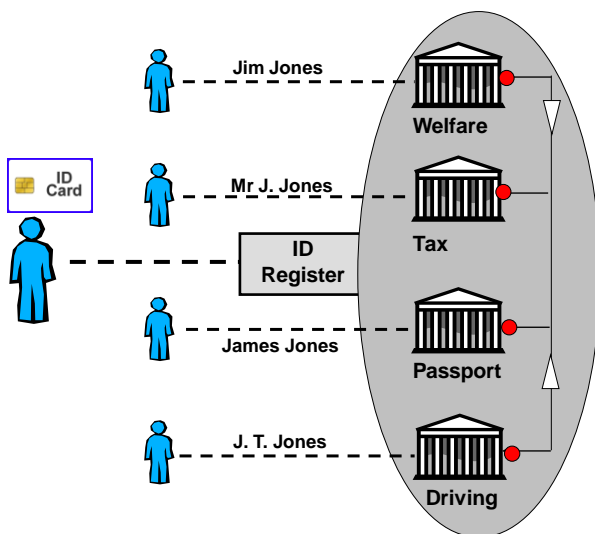
Issues

- Too many usernames & passwords
- Can't do one-to-many transactions, e.g. social stuff, updating contact details
- Can't transmit validated data
- Un-met desire to share data about individuals
- Low security or high authentication costs
- Data breaches

3



Central databases are not the inevitable answer . .



A single e-relationship with **central** government

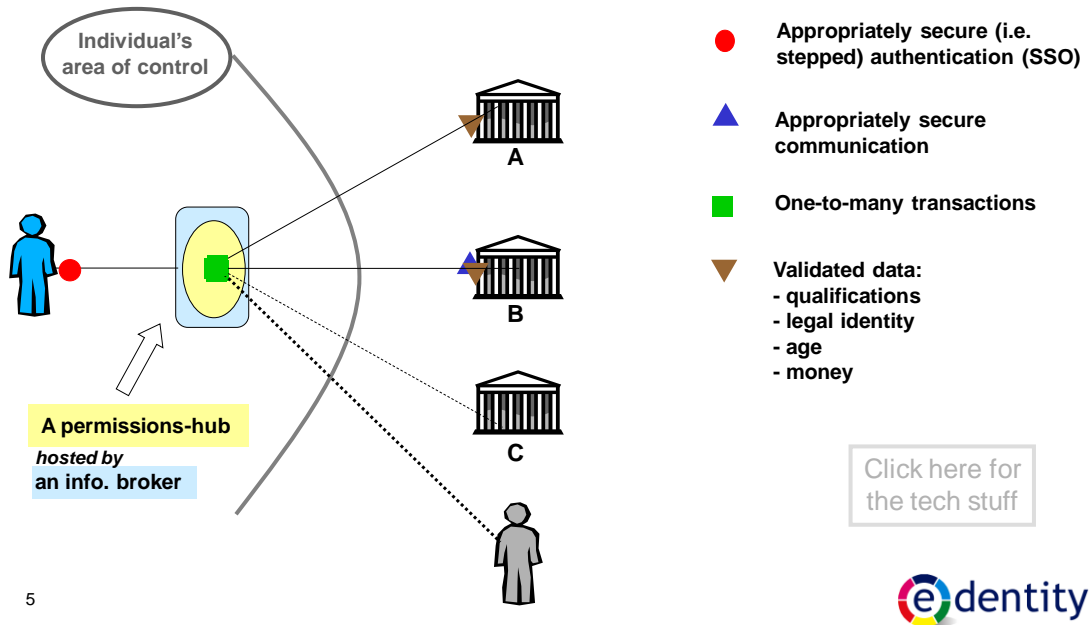
Issues

- Privacy / extensibility (beyond central gov.)
- Remote authentication
- Massive authorisation problem
- Data breaches
- Cost

4



Individual transacts on-line with multiple, distinct entities



5



Application route-map

Education
= { recruitment ownership base revenue }

- E-Portfolio
- Transitions
- Child protection
- Proof of attendance
- Group access to resources

• Delegation

- Dynamic contact book
- Payments
- Calendar
- IM & VOIP
- S-S-O Secure mail

Better interoperable web services



- Intelligent mail redirection
- Permitted direct mail
- Active yellow pages

Delivery & (reverse) marketing
= significant revenue

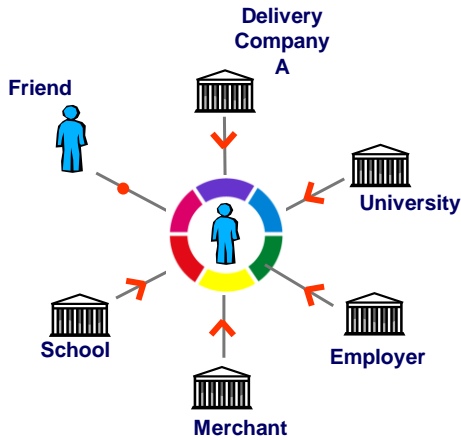
- Agent Services
- Proof of legal ID
- Health

Longer term

6



Organisations pay info-brokers for . .



Organisations pay an information broker on a per-capita basis for:

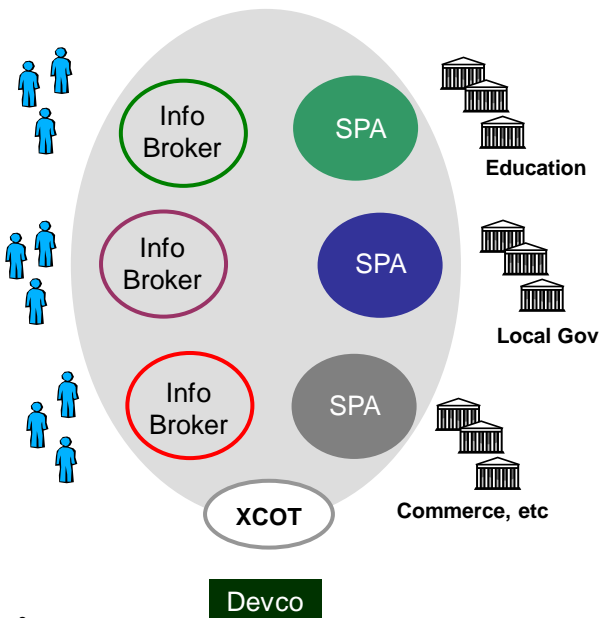
- (i) the provision of a secure authenticated relationship with the individual + update of disclosed attributes; or
- (ii) the chance to enter into a relationship with the individual, i.e. permissioned marketing.

Individuals (friends, parent etc) pay nothing

7



The mature industry structure resembles a payment system . . .



Information Brokers
- compete to serve individuals

Service Provider Acquirers
- compete to serve organisations

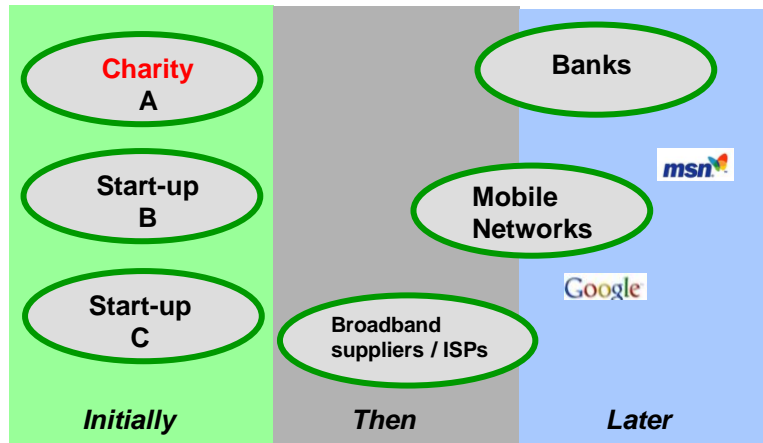
eXtensible Circle of Trust
- Visa-like industry body

Devco- supply of software and services in a competitive market

8



In time, established organisations may enter the broker market



The individual should be able to choose,
AND change her mind !

9



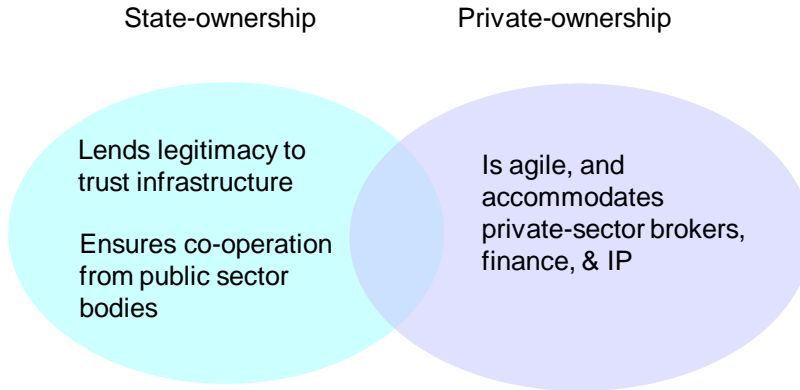
Rough outline of potential pilot

- **Lead application = e-portfolio / personalised learning**
- **Two / three brokers ?**
- **Brokers compete to enrol students**
 - commencing academic year 2011/ 2012
- **Method of authentication to be discussed:**
 - ideally students 'kiss' NFC-enabled mobiles to (i) sign-on to learning-provider systems; and (ii) exchange contact details
 - Otherwise 'Poken' type tokens / smart-cards / username-password

10



Development of PIB requires – probably # – a special x-sector entity



Alternatively, contractual undertakings by the public-sector might just suffice

11



Where are we now ?

Eidentity
BT
VocaLink
Universities of:
- Hertfordshire
- Surrey
- Bristol

✓ Form lead consortium

? Persuade the UK education establishment to provide seed funding

2010 ? { Conduct feasibility study: business cases, design, mock-ups, etc
Raise funds for pilot

2011? Run pilot

Scale to ubiquity

12



An invitation . . .

INFRASTRUCTURE projects – such as PIB - are difficult

- o Many stakeholders to manage
- o Cost-benefit analysis discounts future applications severely

BUT

- o Current e-infrastructure (such as e-mail) was designed 40 years ago, in the era of very thin pipes
- o We need something better, suited to the broadband era.

IF

- o Your company / university / telco / payment system / government would like to contribute, then please get in touch

13



Any questions ?

John Harrison

e-mail : john.harrison@edentity.co.uk

mobile: + 44 7801 231 693

14

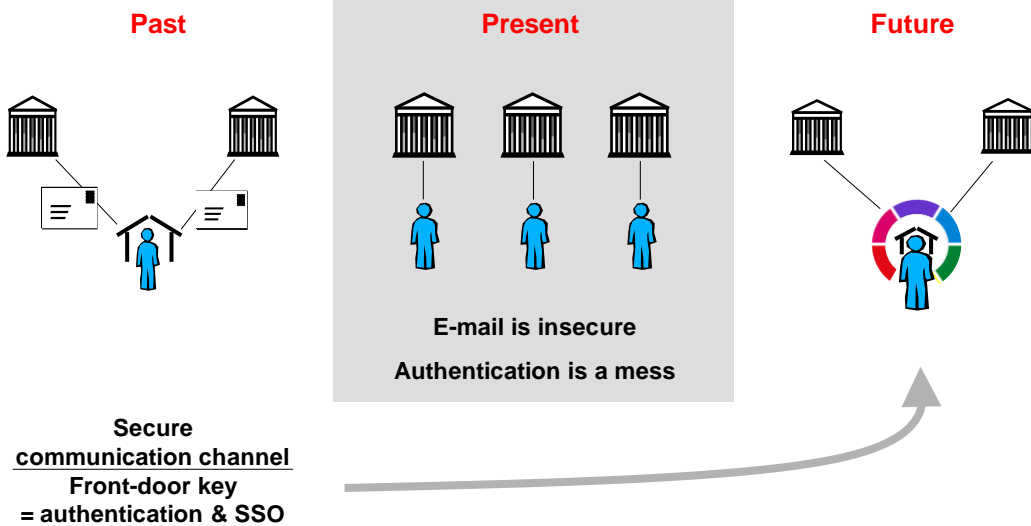


Slides describing the various
PIB applications follow

15



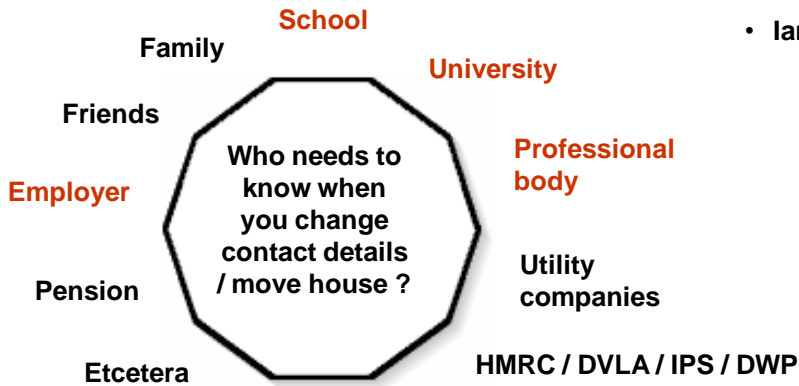
Single-sign-on and secure mail




16



Dynamic contact book



For example:

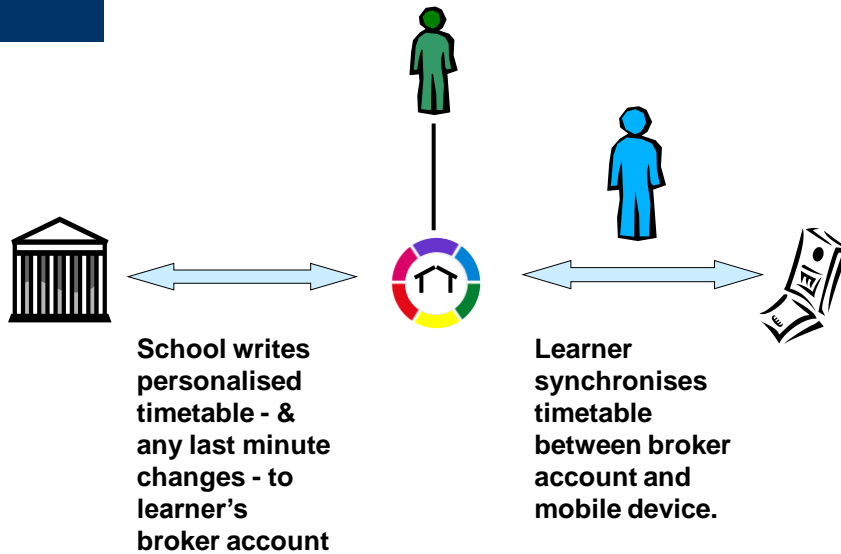
- Plaxo
- Linked_in
- lammoving 



17



Calendar



18



Payments

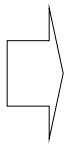
Compare

Traditional electronic payment systems, e.g. Switch / Maestro

- o Payment made from account to account

Internet-based payment systems e.g. Paypal

- o Payment made from person to person
- o Sender decides which account to take payment from
- o Recipient decides in which account to place payment



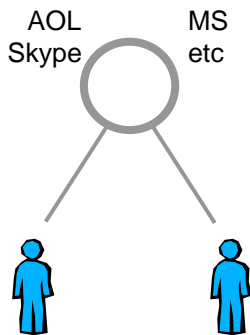
PIB could result in broader take-up of internet-based payment systems

- o Brokers begin to act as payment hubs
- o Constraints imposed by Paypal, as single supplier, overcome

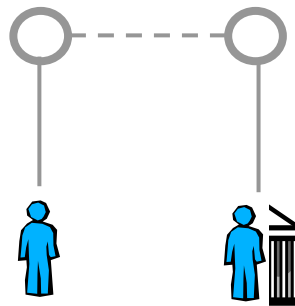
19



Instant messaging / VOIP



Current approaches rely upon a single provider, and "lock" the user in



Info-brokers have the potential to offer a distributed approach, for use by individuals **and** institutions

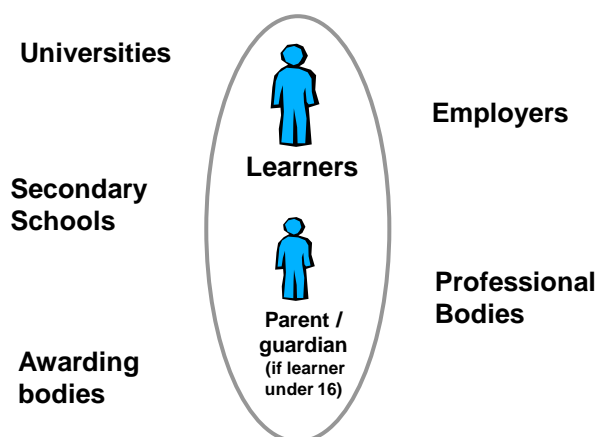
20



E-portfolio

A **learner-centric** system that **is meant** to facilitate:

+ Reflection + Assessment + Transitions
(validated CV)



21



Proof of attendance

Young people aged 16-19 from low-income families are entitled to payment of an allowance provided they remain in full-time education

1 Schools / teachers

- 'write' attendance data to an appropriate page within a young person's permissions hub
- data possibly obtained direct from smart-card readers in class-rooms

3 Payment Authority

- responds immediately to data
- makes payment to account details sourced through permissions hub

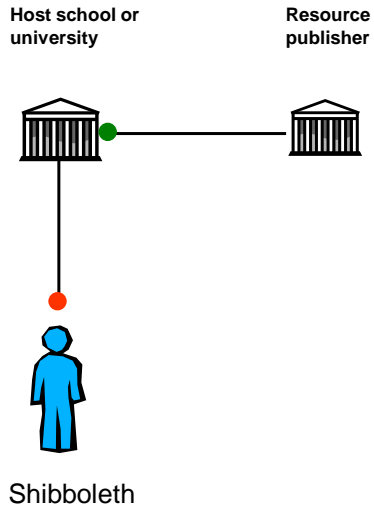
2 Every week, the young person

- checks that attendance data is correct
- arranges for the school to correct any errors
- submits corrected data to the EMA Payment Authority

22



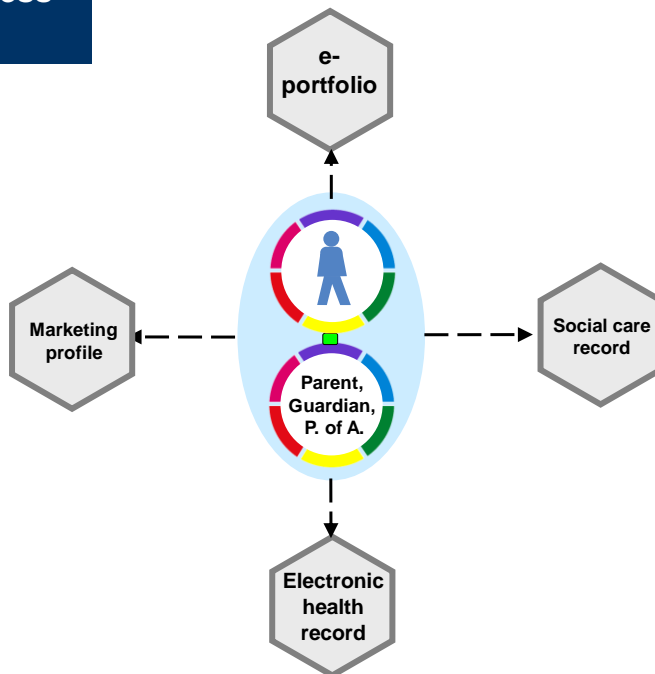
Access management



23



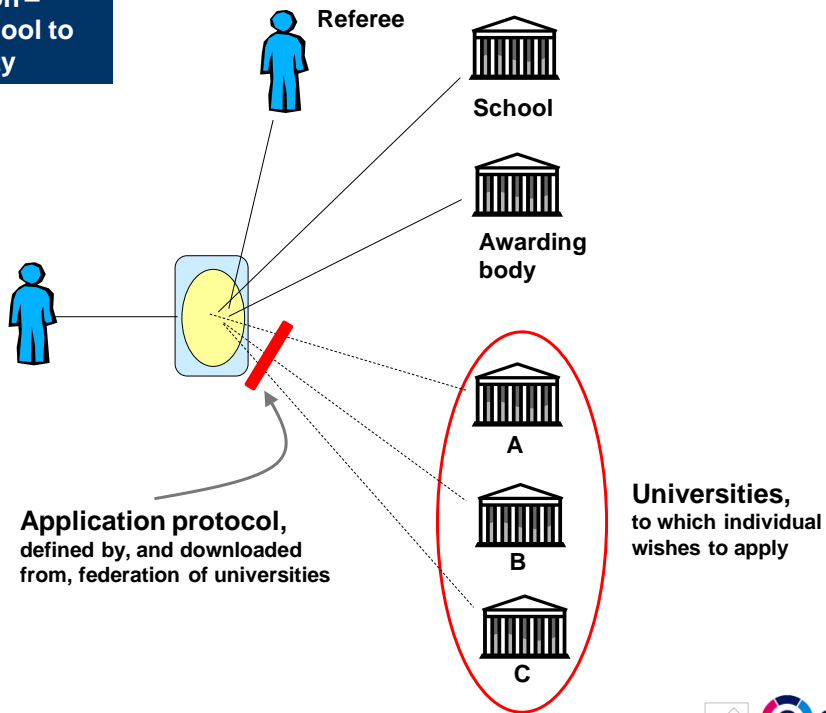
Parental access to records



24



Transition – from school to university



25



Intelligent Mail Redirection (IMR)

- Home shopping is growing
- But no one is at home to accept the parcels

⇒ Delivery Failure

- ‘Weak’ IMR
 - ⇒ Address of an individual's permissions hub complements normal street address
 - ⇒ If delivery fails, permissions hub gives standby street address
 - such as “deliver to No 24”
- ‘Strong’ IMR
 - ⇒ Packets addressed to J Bloggs c/o address of permissions hub
 - ⇒ Courier adds street address at sorting office
 - ⇒ J Bloggs has control of hub
 - deliveries M to F to work address etc

26



Active Yellow Pages

- Remote shopping is growing
- Predominant model:
 - first Google
 - then **VISIT** merchant site
- But merchants still wish to **SEND** product info by:
 - by electronic message
 - by paper catalogue
 - by telephone

27

1. An individual wants, say, a sofa.
2. He clicks on:
 - “household goods > furniture > sofa”
3. He selects:
 - preferred merchants
 - an ‘interested period’, say 1 month
 - preferred medium
4. Broker sends to each merchant :
 - a time-limited pseudonymous address for the individual’s permission hub
 - other information, such as wide-area postcode
5. Material is readdressed en-route



Permissioned Direct Mail

- Some individuals are willing to accept unsolicited marketing material
 - especially if relevant
- Relevance can be increased by:
 - targeting by profile
- But consumer profiles are often:
 - inaccurate
 - used without consent

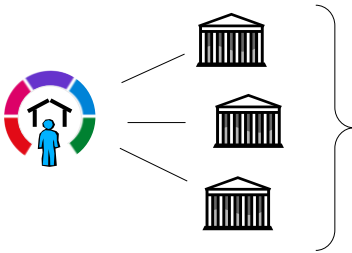
28

1. Individual:
 - makes accurate profile available through permissions hub
 - indicates frequency with which she is willing to accept unsolicited marketing material
2. Aggregator:
 - auctions off willingness (together with that of others) to merchants
 - prevents abuse by use of pseudonymous, time-limited hub addresses
 - pays bulk of fee to individual / info-broker



Agency services

- Acting as agent, info-brokers can empower the individual to deal more efficiently with multiple third parties:



- **Insurance** – enter data once to receive many quotes; use broker account to transfer evidence of no claims.
- **Gas, electricity, telcos** – enter usage data through, and store within, broker account. Use data to obtain future quotes.
- **Cardwise** – store card numbers on line, and cancel all in one transaction if necessary.
- **Opt-outs** – use broker account to opt out from unsolicited mail, phone calls, and faxes

- But critical mass is a pre-requisite

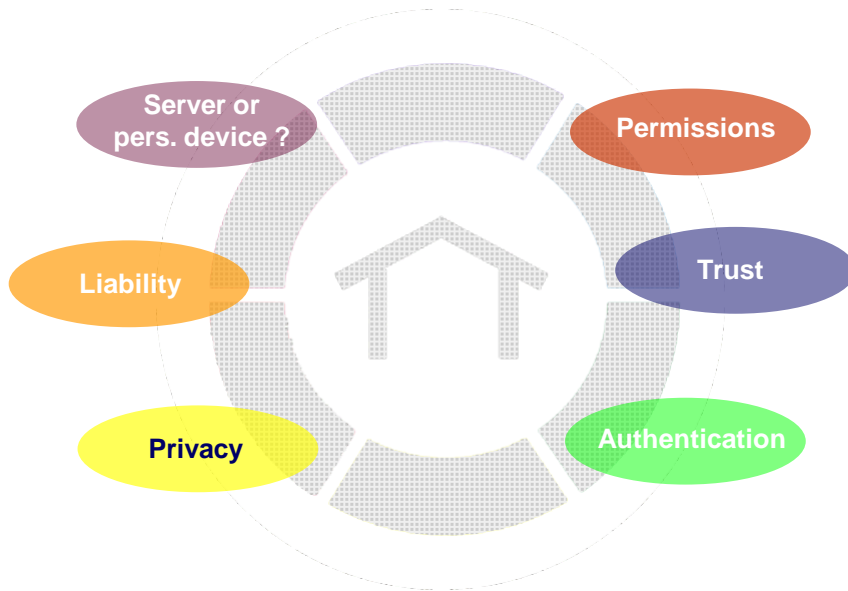
29



Slides describing technical aspects of PIB begin here

30

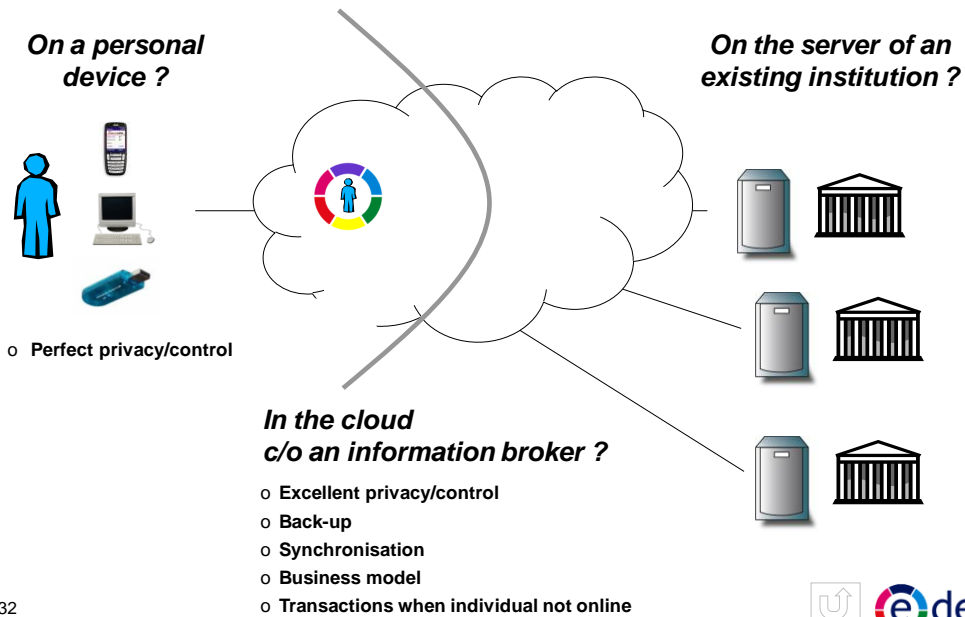




31



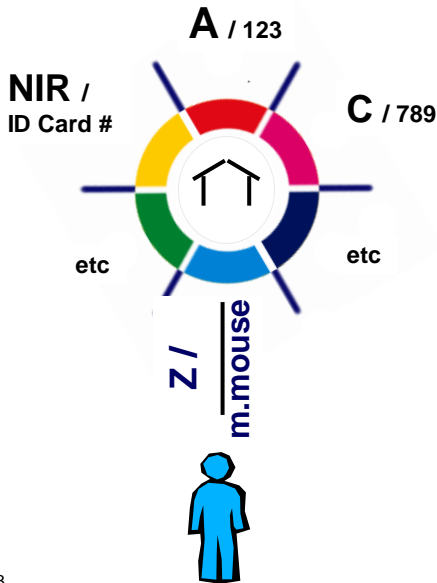
Where should a 'permissions-hub' be held ?



32



Privacy . . . requires pair-wise identifiers

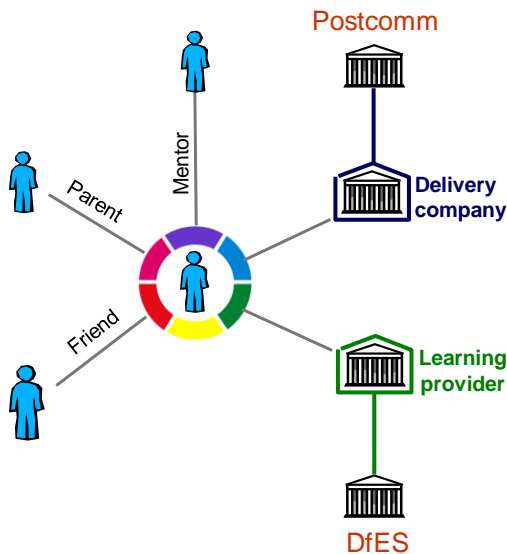


1. Relationship *identifiers* are pair-wise & private
2. An individual may choose to maintain a quasi-public *address* (e.g. Z/m.mouse) to point new contacts, encountered of-line, to his permissions-hub
3. Omni-directional addresses / identifiers (e.g. phone #, ID card #) may be transmitted over the infrastructure with the consent of the individual, but are not required by it.

33



Permissions granted according to roles



The individual sets up relationships with other entities from his permissions-hub (as in Skype or MS IM)

Default access permissions are determined by the *role* of an entity, but can be modified by the individual

Roles are allocated either:

- by the individual; or
- by a *certifying body*

34



Any token & multiple security levels

Authentication mechanism



- **Username & password**
- **2 factor authentication**
 - One-time password (on key-fob or 'phone)
 - Smart card (requires secure accepting network)
- **3 factor authentication** – to prevent impersonation by consent
 - e.g. BT launch of voice biometric service
 - Possible use of Home Office (ID Card) as authentication service provider

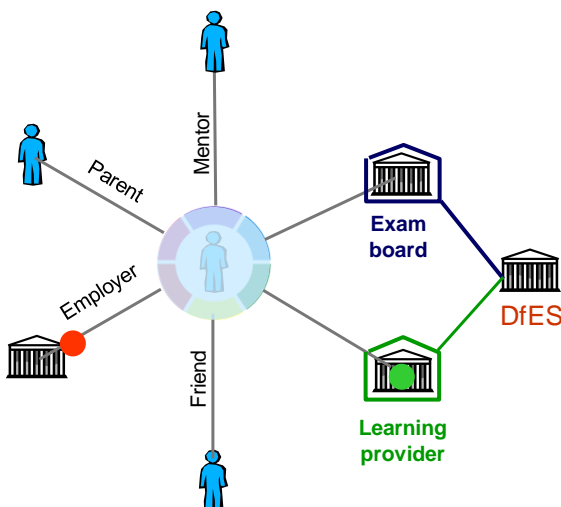
NB

1. Partial shift of responsibility from organisation to individual
2. Divorce of authentication and identification
3. No privacy issues because data (inc biometrics) under individual control

35



Why should relying parties trust information received ?



Relying parties can:

- trace attributes back through a learner's e-portfolio to the attribute provider;

and, if necessary:

- trace an attribute provider's credentials back to the certifying body.

A network trust infrastructure that mirrors the real world

36



Liability

**A complex problem,
but not a show-stopper.**

Needs further study.

One possibility:

- Relying parties specify authentication level etc
- Broker and authentication providers:
 - are responsible for correct execution of their tasks
 - are liable, up to cap (depending on authentication level), **only** if their tasks have been incorrectly executed