Identity Management (Technologies)

Workshop Report

24th January 2007

This report was commissioned by the Horizon Scanning Centre within the Foresight Directorate of the Office of Science and Innovation (OSI HSC). It was developed by Outsights-Ipsos MORI.

While OSI HSC commissioned this work, the views are those expressed by the participants, and are independent of Government and do not constitute Government policy.

The Outsights-Ipsos MORI Partnership has been established to develop the HSC online Sigma Scan database of drivers of change, maintain and refresh the Delta Scan overview of future science and technology issues and trends, and to design and run a series of cross-governmental and departmental engagements to consider future opportunities and risks. The partnership combines Outsights, a London-based strategic consultancy with a particular focus on future challenges, and Ipsos MORI Horizons, the international research consultancy.

Ipsos MORI

outsights
insights from the outside

Contents

Executive Summary

Her Majesty's Treasury worked with OSI HSC and Outsights-Ipsos MORI to review the key technologies and their societal context relevant to future identity management, in order to input to the work of the Public Private Forum on Identity (PPFI). The project brought together a cross-section of public and private sector perspectives in tandem with consumer and other expert views to inform the development of an analytical framework for the PPFI.

This workshop is the second of two workshops aimed at informing the consideration of identity management issues and cross cutting key themes of particular interest to the PPFI. The first workshop – held on 13 November, 2006 – examined the broad, key drivers behind identity management, and the uncertainties around these, before going on to assess their impact on the need for identity management, and how they shape management within the context of the PPFI's four Key Themes.

This workshop considered in more detail the scope and opportunities for technology to deliver viable and sustainable solutions to the future challenges of ID Management in a 2 - 10 year timeframe. The event also explored the potential roles of the public and private sectors and the societal context in which future identity management systems might be deployed.

Main conclusions

The key messages emerging at the end of the day were:

- PPFI should challenge the emphasis on biometrics. Currently biometrics underpin the national ID scheme, but is it necessary to make it work?
- Focus should be placed on architectural solutions to reduce the key problem of interoperability, which lends itself to solving many related issues such as indexing across different organisations.
- The idea of keeping NIR as a streamlined database is good, with core services being used primarily to assert identity, and secondary services possibly used for commercial application.
- Not many issues discussed during the day were new, but all the experts are still trying to guess why some historical decisions were made.

Introduction

Her Majesty's Treasury worked with OSI HSC and Outsights-Ipsos MORI to review the key technologies and their societal context relevant to future identity management, in order to input to the work of the PPFI. The Outsights-Ipsos MORI Partnership has been established to develop the HSC online Sigma Scan database of drivers of change, maintain and refresh the Delta Scan overview of future science and technology issues and trends, and to design and run a series of cross-governmental and departmental engagements to consider future opportunities and risks.

The workshop was attended by a cross-section of Government departments and participants from the private sector. (See Appendix One for participants)

This report records the output of that workshop – Identity Management (Technologies). It is presented in three main sections:

Section 1: Introduction and context for the day

Section 2: The technologies

- Biometrics
- Identity Management Systems and Architectures
- Directories & their Meta and Virtual Versions
- Role-based access control
- Digital Rights Management Systems
- Federated Identity: Risk/trust Management
- Anonymity (E-cash and E-Voting)
- Interoperability standards
- User-friendly solutions
- Pie in the Sky Technologies

Section 3: Technologies analysis against context

Appendices: Participants

Presentations

Section 1: Introduction and context for the day

The day started with an introduction to the project by Jon Parke of OSI HSC, followed by an outline of the framework to be used for analysis on the day by Richard O'Brien of Outsights-Ipsos MORI. Participants then suggested technologies and issues that are critical, ones that run the risk of being ignored (and thus should be on the radar screen) and ones that could be considered the "flavour of the month". These are summarised below:

Critical technologies/issues

- Radio Frequency Identification (RFID) technology
- Bar codes
- Data governance
    - How many data on an individual do you need?
- Coherence and consistency of language and definition
- Error rates and repair mechanisms
- Common sense
- Trusted credentials – federated use
- Proportionate measures

Technologies/issues that run the risk of being ignored

- Use of data offline
- Benefits to the individual
- What happens when technology fails?
- Threats of disruptive technology
- Multi-use of technology: is it appropriate?
- Quantum computing: possible threats
- Maturity of smart cards

Flavour of the month

- SOA: Service Oriented Architecture
- Technology itself (i.e. excessive attention to technology as opposed to the issues and context)
- Excessive use/disproportionate application of technology e.g. biometrics for the library

Section 2: The technologies

As preparation for the workshop, a paper entitled "Key technologies for identity management" was produced by Dr Michael Huth, Senior Lecturer, Quantitative Analysis and Decision Science at Imperial College, London. Dr Huth presented the key points of the paper (Appendix Two) and the morning session was devoted to a rigorous review of the ideas presented in the paper. Summaries of these comments follow:

Biometrics

Role of biometrics

- Substitute for a higher level of identity management, role-based access control
- Roles can be very dynamic
- What is the wider usage of biometrics?

General comments

- IKO standard has been put on a chip so the law/police can use their own reader technology
- There is an important distinction between the authentication of an object carrying credentials (for example, a passport) versus the authority of the carrier to make the assertion that he is the correct owner of the object
- Differentiate between Biometrics to identify somebody versus to validate a purported identity: negatives
- Distinguish between Identification (for example, a suspected hooligan in a football crowd) versus Verification (e.g. correct ownership of a passport)
- Distinguish between Automated versus what needs a lab (DNA)
- Security or a usability benefit
- Multifactor authentication (it was noted that that the government paper on multi-factoral identity should become the "set-text")
- Language and definition is critical e.g. in multifactor definition
- An additional adaptive behaviour
- Profiling, early wins – services to the right people
- How do systems adapt to crises e.g. avian flu?

Identity Management Systems and Architectures

- It may not be the system that is so important as understanding the ways in which components link into adjacent systems
- Large corporates are now implementing large IDM systems; the US is now doing it
- Field has not really matured so there is no common framework to build architecture
- More important for engineers than public sector

Directories & their Meta and Virtual Versions

- Databases and data – needs indexing standards
- Is a directory possible? In theory, but not in practice
- Large corporations and governments have good IMS
- Potentially the technology directory we are describing is the tail wagging the dog. The reality is that the IT specialists are pushing a directory scale, which by the time it is implemented, will be wrong. The concept in our heads doesn't map into directories. How do you map the world as it really is, taking into account the soft roles?

Role-based access control

- Not convinced this is a relevant technology for organisations
- It's a useful device but the question is how to get relationships within the organisation correct. The concept is good, but the discipline is not there
- How you manage role-based control to deviations in management is a major obstacle
- What's the proximity between this issue and identity management?
- Allows individuals to exploit identity management
- Needs a clear definition of roles for it to work
- Roles can be very dynamic, e.g. if there's an on call consultant at a hospital and a patient comes in, that consultant will need general access
- Can be used in proportionality to ID control – a soft form of IDM which is currently implemented in Belgium (log-in cards for teens to prevent

paedophilia) and Germany (chip & pin cards which tell the person's age to allow/disallow them to buy cigarettes)

- We need to know more about what we're carrying to assert identity, just because you own a chip or card does not mean you own that identity
- There can be a two-stage authentication: what you hold and who are you
- Need to get the terminology right, there's a danger of using ID management not as a collection of attributes but as a specialised attribute

Digital Rights Management Systems (DRM)

- What about the impact of reverse DRM? Consumer dictates this
- Different directories stored in different formats, so there's a standardisation issue
- PKI (public key infrastructure standard) should be critical

Federated identity: Risk/trust management

- All the people in a federated identity must have the same knowledge and use of the identity
- Question is do you trust the identities offered by other organisations? We have to make sure there is a clear understanding of the regulations/standards before engaging this kind of technology
- Mutual appreciation of the value of the identity
- Is this a technological solution or a business sense? Clarity is needed
- Reuse across departments/private sector
- Strong case for access, defined mechanisms
- Data sharing is less about technology problems but more question of politics and society

Anonymity

- Assertions: a key word
- Public and private sector using data for different purposes
- Public to follow the same rules as private
- Virtualised money e.g. the Linden in 2nd life

- Virtual worlds are a potential disruptive technology undermining identity: currencies in such as 2nd Life with their own exchange rate erodes people's idea of trust and experience of service; we also could see interesting effects of avatars on people's conception of their self in reality
- Any public system should allow people the right for uses they permit
- Definitions of e-cash need strengthening; in reality e-cash means stored value. Only one true system for e-cash in the world was Mondex which never took off in the UK
- E-transactions could undermine the use of identity going forward
- Trust comes in the branding of products and services: are people willing to trust e-cash?
- Related issue about anonymity is that any public scheme should give the consumer the right to expose only the attributes they want to. The whole nature of a beneficial identity scheme is that the consumer has control
- Most Government rhetoric about this is focussed on security - there's no debate about how the private sector is using these technologies
- The security structure should be the same for Government and private sector. At the moment this is ambiguous in the Act
- Have to design the ID system so that it starts with the question: is this person over 18?
- Not convinced that this is difficult to do; the issue is: don't muddle it.
- Defining attributes comes down to the design of the model: are we trying to read the attributes or interpret them?
- Using the term "assertions" is a very positive way of assessing what ID management wants to do
- There's an unfair exchange of value: government does not give anything in exchange for information whereas commerce does
- What business wants is continuity of identity; what government wants is uniqueness of identity, though the environments are gradually converging
- Commerce will eventually need to know more about your identity or Government can force commerce to get more information
- There aren't many areas in the public sector using uniqueness as a driver, that's more for border control and security

- One of the conundrums about this debate: it was actually bank systems that made Government realise the value of doing this
- Worth making the link between anonymity and the offline validity of the ID card
- E-Cash will never come in because it is direct challenge to the national float; this will never happen unless the monetary system changes

Interoperability Standards

- Government must set standard for NIR
- Deal with liabilities
- The Germans have a very different legal interpretation of passports to us (shaped by their nation's history)
- Although we have a Data Protection Act, it is applied differently
- The passport and ID are essentially different, is there a need to see the scheme as multi-platform?
- Linking the passport and ID card will make it infinitely more useful to the public
- Need to remember that passport cards were dismissed because you cannot stamp them
- Every other citizen in the EU travels on their ID/resident's permit except for the UK
- Need a public-public debate on ID schemes, not just a public-private debate
- Not just data standards but also trust standards

User-friendly solutions

- This is one of the key areas that interests consumers
- Need to divorce government and commerce but ensure any solution is scalable
- You want to assert an identity that has value and the ID card should be that medium
- Take up for this is up to the individual: public and private are moving towards more people-centric services

- It picks up on this point on you're interfering with the market because it's a 10-year transition
- If you create a market where the cost of enrolment and renewal are not expensive, then the opportunities for a marketplace for public-private sector partnership is vastly improved
- What consumers perceive the cards will be able to do e.g. work across multi-platforms is far removed from the technical practicality of what the cards actually can do e.g. Oyster
- Free wireless network issue is potentially a disruptive technology. Essentially it will be a free utility whose ease of use will be disruptive to existing incumbent businesses. It is about to be offered in California.

Pie-in-the-Sky Technologies

- Quantum based technologies can erode the basis of trust we have in the world today
- The idea that we have paper documents to back up virtual signatures will no longer hold
- If quantum computing reaches it's full potential it is very disruptive
- Emerging commercial application is laser identification

Two themes which were mentioned with were not linked to any specific technology were:

- Need to make technology neutral rather than politicised
- Need to educate public of what government IDM plans are; how can the public oppose if they don't properly understand

Section 3: Technologies analysis against context

After plenary discussion of points raised in Dr Huth's presentation, participants divided into breakout groups to analyse the technologies against context. The following are the topics considered by each of the four groups and the participants in the group.

These topics follow approximately the same sequence as in Dr Huth's paper, with the "pie in the sky" technologies distributed across the groups. The full template for discussion is provided where appropriate: where technologies were not discussed at length the relevant part of the template is provided.

Group 1 Biometrics Two-Factor Authentication Role-based Access Control Quantum-based Digital Identities	**Participants** Colin Robbins Jeremy Monroe Fred Preston Rob Laurence Colin Whittaker Sir James Crosby John Elliot Richard O'Brien
Group 2 Biometrics Digital Rights Management Systems (DRM) Directories & their Meta and Virtual Versions Adaptive Behaviour	**Participants** Michael Huth Neil Munroe Andy Robinson Rupert Lewis Job Parke Julian Thompson
Group 3 Identity Management Systems and Architectures Federated Identity, Risk/Trust Management Anonymity, E-Cash and E-Voting Computer Forensics	**Participants** Robert Temple Simon Mitchell Ian Bourne Tim France-Massey Geoff Linton Simon Davies Michael Keegan Alasdair Keith

Group 4	**Participants**
Interoperability Standards	Bill Guy
User-Friendly Solutions	Jerry Fishenden
Regionally/Globally Unique Identifiers	Toby Stevens
Nanotechnology	Richard Trevorah
	Maria Burroughs
	Neil Fisher
	David Rennie
	Barbara Muston

Group 1: Results and discussion

Biometrics				**Comments on Definition** 1 to MANY for enrolment; **1 to 1 for verification**
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	**x**	x		**X** depends on risk being taken
2. Government	**x**x			
3. Business	x	**x**		
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities	**x**x			4: enrolment link; more effort on the exceptions – it is necessary 5: perceived as an issue ▪ civil liberty – what access does Government give to Biometrics? ▪ no compelling need. ▪ A "Channel Tunnel" problem i.e. an infrastructure to last
5. Privacy				
6. Ownership, Control, Extracting value				
7. Trust and Culture				
8. Attitudes to Risk				
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment				
10. Demographics: Mobility and ageing				
11. Criminality	x			
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards	x			▪ Standardisation an open issue – bio vs bio ▪ Important for verification, not enrolment matters ▪ Money matters
B. Consumer				
C. Legislative				
D. International				
What role and opportunities does this technology offer for public-private cooperation?				
▪ Jury out on the need for Biometrics for verification, civil liberty issue critical (see above)				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ 3rd factor for verification is fundamental for enrolment ▪ Authentication versus Government Biometrics database all using two-factor verification				

Discussion

- Distinguish between 1 to 1 and 1 to MANY and analyse them differently
- Individual and Government view each of these differently. Corporate sector view the 1 to MANY as more important
- A key issue is moving through the authentication problem: the jury is out on how to do this. Two factors can be used for verification, but the 3rd factor of biometrics is not necessary. It's merely an option, not one that will get much take up

Two-Factor Authentication				**Comments on Definition** The comments under Biometrics apply to this aspect too (hence this has not been ranked in discussion aside from the comment on individuals)
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	x			▪ Important to confidence system
2. Government				
3. Business				
B. Consumer				
C. Legislative				
D. International				
What role and opportunities does this technology offer for public-private cooperation?				
▪ Ubiquity of use: if used across public & private sector, there needs to be standardisation ▪ Physical accessibility/practicality – biometrics can help ▪ Opportunity for Government to be a market brand leader ▪ Will two factors get more necessary for more functions? ▪ Look for the killer application				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Bar keeps rising – how high and when does it reach a limit? ▪ Biometrics won't happen if not mandated, business will wait ▪ Authenticating off a biometric database ▪ Ability of Government to interface is wasting asset ▪ Build database fast – how does Government build business case for building quickly?				

Discussion

- What's the demand for two-factor authentication? How much do we all care about this service? It will most likely be Government that raises the bar on this, especially if it is cheap and easy to do and Government also has the power to do this. Timing of this might be problematic: 10 years is too long. By what means can you advance the means of implementation?
- Big issue about the public/private issue to exploit private sector demand to drive this in 5 years
- Private sector may have to invest in an alternative solution because Government scheme is too far ahead
- It will not be the best technology that wins, rather the first on the scene
- Perhaps the private sector can strengthen its two-factor authentication while the Government builds its database
- Is the Government's database really an asset? It is speed and market penetration that will make this a good business case i.e. 90% market penetration good for Government

Role-Access Control	Comments on Definition Not discussed in sub group: see plenary discussions from the morning
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability	
▪ Potential as a bolt on application/way of delivering this service	

Quantum Computing				Comments on Definition Quantum may solve the unsolvable maths e.g. rock modern cryptology
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment				▪ Levels of attack below quantum can upset confidence
10. Demographics: Mobility and ageing				
11. Criminality				
12. Internet				
What role and opportunities does this technology offer for public-private cooperation?				
▪ What counter measures? ▪ Government will need solutions more than others				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Could generate fear and threat in consumer mind ▪ Put measures in place to track it				

Group 2: Results and discussion

Biometrics				**Comments on Definition** ▪ Behavioural biometrics e.g. gait, habits & behavioural o Monitoring behaviour o Anticipating behaviour
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	?	?	?	1. Behavioural biometrics as evidence to prove you had no malicious intent, but manipulatable e.g. lie detector. Could be 3rd/4th factor – stress analysis on telephone re: lying on insurance 2. Government monitors civil disobedience 3. Business could target individuals based on behaviour
2. Government	x			
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities	x			4. Maximise exclusion: different cultures and individuals behave in very different ways and could be left out
5. Privacy				
6. Ownership, Control, Extracting value				
7. Trust and Culture				
8. Attitudes to Risk				
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment				11. Criminal profiling and anticipation e.g. Minority Report ▪ Could monitoring dynamic systems e.g. crowd control, but very difficult to understand e.g. neural networking ▪ Internal criminality – how people behave internally e.g. pattern of typing keyboard signatures ▪ Security/terrorism could flip the decision and push Government to go ahead
10. Demographics: Mobility and ageing				
11. Criminality				
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards				C. Snooping e.g. voice recognition by Government on telephone or keyboard recognition – restrict freedom of individuals to behave as they want
B. Consumer				
C. Legislative	x			
D. International				

What role and opportunities does this technology offer for public-private cooperation?

- Suggest applying in combination with other IDM technologies
- Use this as a backup/multistage confirmation
- As a tool to reinforce other metrics to anticipate and gauge behaviour of terrorists and security threats

Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability

- Profiling would preclude main application – very costly and intensive
- IPS (International Passport Services) application by interview – deliberately set up to capture BB – gauge whether applicants are fraudulent – very controversial and newly established

Digital Rights Management Systems				**Comments on Definition** Consumer centric DRM an appealing concept
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	x			1. Reverse DRM: ▪ Consumer controlling rights of companies to use their data ▪ Critical to get the public engagement right – explain it to consumer as there's no current perceived consumer benefit ▪ Get away from the control model & communication – selling if needed ▪ Explain balance of costs and benefits – could be a great enabler in the long term to winning people over for business 3. Business protecting IP and data
2. Government				
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities	x			4. Digital divide and excluding proportion of population 5. Depends on whether people can control access to their ID details 7. People annoyed by haphazard introduction of digital rights – could force people back to traditional forms e.g. CDs ▪ Private sector trait – use public ▪ Whose rights are they?
5. Privacy	x			
6. Ownership, Control, Extracting value				
7. Trust and Culture	x			
8. Attitudes to Risk				
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment				11. Denial of service attached could prevent victim assessing their resources and managing their identity ▪ Criminal behaviour disrupts consumer-centric DRM, disintegrating consumer confidence in the whole system ▪ Opportunity for attacking organised crime by criminals' DRM 12. Opportunity to use web as primary interface with DRM as the principle mechanism, also with mobile phones and MP3s
10. Demographics: Mobility and ageing				
11. Criminality	x			
12. Internet	x			
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards				A. Easier way to deliver common standards? Because at higher level of abstraction BUT no consensus and market very fragmented ▪ Lots of different models exist ▪ Opportunity to draw it all together – Government led standards ▪ Constrain the market and freedom for companies to adopt market approach DRM ▪ Need to develop standards that establish common principles of what they need to deliver to consumer with their approval B. Consumer control: Need to have feasibility to cope with realities of people's lives e.g. selling your computer
B. Consumer	x			
C. Legislative				
D. International	x			
What role and opportunities does this technology offer for public-private cooperation?				
▪ Agree on standards first – otherwise risk of Betamax vs VHS, to underpin consumer confidence ▪ Consumer-centric DRM very compelling BUT what incentive if this system doesn't force people to buy services from companies; major market opportunities and international ▪ New domains of products and services as individual manages rights				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Delaying introduction until we know what works ▪ More 10 years than 2 (today's 10-year-olds!) – impact on Department of Education ▪ Who else will benefit? On for consumer but how broad are benefits (e.g. digital divide)?				

Discussion

- Least consumer aware technology
- More like a result of other technologies
- DRM being a control mechanism rather than a consumer mechanism – reverse DRM

Directories				
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals				2. Coping with all the legacy Government systems; managing inconsistency; can't build systems from scratch. Need to have common indexing system otherwise impossible to manage 3. Intra-organisational sharing especially as companies become more globalised; federated IMS more applicable? International legal issues
2. Government	x			
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities				5. How long data will be stored and de-provisioning very hard e.g. Tesco loyalty cards, function/mission creep > relates back to DRM & user-centric DRM ▪ Nazi Germany and trust issues ▪ Political, cultural and ideological dimension – role of the individual and the State ▪ Difference in societies and willingness to cede control and data to the State 7. Consumer trust issues about "database culture" – out of control and impossible for users to control and manage data
5. Privacy	x			
6. Ownership, Control, Extracting value				
7. Trust and Culture	x			
8. Attitudes to Risk				
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment				10. Frustration of having to shift percentage to different payment cards and credit transactions: international directory to manage and facilitate global transactions 11. Human corruption in databases > getting hold of private information & airbrushing it ▪ Role based rights vs easy to compromise and abuse e.g. benefits office and NI number
10. Demographics: Mobility and ageing	x			
11. Criminality	?			
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards	x			A. Huge difficulties – standards being agreed; interoperability standards B. Consumer acceptability and political message – too many negatives, not enough incentives
B. Consumer	x			
C. Legislative				
D. International				

What role and opportunities does this technology offer for public-private cooperation?

- Interoperability e.g. SOCA and passports agency
- Government needs to agree and identify common standards or is there a market creating standards which Government can sign up to? Need more evidence on this.

Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability

- Technically we're there but common standards have not been properly finalised and reviewed, they are emerging organically
- If speed of change moves faster than public perception it could cause a public backlash

Discussion

- Databases and data need indexing standards
- Consumer trust issues: "privacy secondary" even if databases can't speak to each other
- Pulling together all technologies
- Combined tech approach to support any disaster

Adaptive Behaviour				
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals				2. If specific behaviour, Government can tailor services around this – get some consistency – long-term adaptation. Military action > flexible entitlements that respond immediately e.g. Iraq War 3. Targeting and content-based communication – e.g. viral marketing – just enough for a superficial profile e.g. consumer variable pricing; Olympics (short timeframe for selling/marketing)
2. Government		?		
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities				6. System needs to be highly adaptive to locations of control
5. Privacy				
6. Ownership, Control, Extracting value				
7. Trust and Culture				
8. Attitudes to Risk				
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment	x			9. Cross cutting issue – how can IDMs cope/which would fail if we were hit with massive environmental shock e.g bird flu. Over-reliance on some IDMs – vulnerability if whole system compromised – critical failure 11. How can you cope with people assuming identities and adapting to commit fraud? Need for contingency planning
10. Demographics: Mobility and ageing				
11. Criminality	x			
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards				A How do you get common standards for shifting, ephemeral behaviour without a massive depth of data?
B. Consumer				
C. Legislative				
D. International				
What role and opportunities does this technology offer for public-private cooperation?				
▪ Opportunities for targeting public and private goods and services > context and behaviourally specific				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Already viral targeting happening now				

Discussion

- Identifying people by profiling to get some identity there. Might be some early drivers here that Government can use to target services better
- How does it adapt to a major disaster like avian flu…what would you fall back on when it breaks down? Also, what remains in such a disaster?

Group 3: Results and discussion

Identity Management Systems and Architecture				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards		x		A.&B. What are the requirements? Not myriad ways of doing things, front end important ▪ Different infrastructures need to co-exist, need for at least some common architecture C. Government defining architecture but got what we need: constraint D. ITL operability standards, good case studies of architecture
B. Consumer	x			
C. Legislative		x		
D. International		x		
What role and opportunities does this technology offer for public-private cooperation?				
▪ Has low coupling to end user capabilities				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Interoperability the important question				

Discussion

- Can be broken down into adjacent systems rather than have one big piece of work
- Components into adjacent systems

Federated Identity: Risk/Trust				**Comments on Definition** Number of other ways to achieve the same effect
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards	x			A. Need to ensure case to share data; also business-readiness to share their risk B. Is it useful to the consumer? C. To use across departments there has to be legislation; electronic signatures would be stored on IDM (relevant leg) D. Trend is increasing (driven by security). Travel increase (as driver); EU standards; other commerce doing this internationally
B. Consumer		x		
C. Legislative	x			
D. International		x		
What role and opportunities does this technology offer for public-private cooperation?				
▪ Joined up view of customer/citizens e.g. anti money laundering (also public-public: do not have to keep on reasserting ID) BUT dependent on who in private sector				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Need mechanism to approve access ▪ Technically we are there but how to get systems talking to each other is the big challenge ▪ Commercial, culture, Trust questions o Point interaction rather than ambition for wholly federated > do we need truly federated? ▪ Need accreditation criteria.				

Discussion

- Could be related to re-used id credentials
- If federal ID gave different parties access to shared data then there has to be a clearly defined case for that to be acceptable and transparent
- Reuse across departments/private sector
- Strong case for access, defined mechanisms

Anonymity (E-Cash and E-Voting)				**Comments on Definition** Technological accountability important. Anonymity an enabler for other. Anonymous from whom?
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	x			1-3: It is an important question whether I am anonymous. Linked to trust ▪ Can be of high/medium/low importance (especially for business) ▪ Imposters, even in business ▪ E-Cash important for money supply
2. Government	x			
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities		x		8. Anonymous: far more risky
5. Privacy	x			
6. Ownership, Control, Extracting value				
7. Trust and Culture	x			
8. Attitudes to Risk	x			
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment	x			9. Enable to abdicate responsibility
10. Demographics: Mobility and ageing				
11. Criminality				
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards		x		B. Selling benefit C. All kinds of responsibilities on Government D. Cross border trade
B. Consumer	x			
C. Legislative	x			
D. International		x		

What role and opportunities does this technology offer for public-private cooperation?

- Not much existing > great opportunity to shape
- Facilitating other use of IDM, along as have consumer consent, it economically makes sense
- "Do what you want with IDM": a good thing? Consumer utility (Pay on marginal benefit, State provides infrastructure)

Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability

- Design of IDM important for scalability
- Strata of anonymity against business IS
- Needs to be easy
- Going mobile
- No framework for anonymity (debate will pit Government against private sector)
  - Needs to be defined in a publicly acceptable fashion
- Getting people to exercise ID: are they ready?
- Not just question of choice but also policy

Discussion

- If ID cards enabled anonymous transactions to take place what other types of usage can result?
- Important to give individuals/private sector ability to choose which transactions are anonymous
- Concluded that by providing these options it would give ID card greater reason to be adopted
- No standards for anonymity, but this is being worked on

Computer Forensics				**Comments on Definition** Expand beyond criminal
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards			x	B. Stuff others do, not important but does impact on buy-in C. Right level of supervision – not currently regulated D. International borders, blurred but no supervision
B. Consumer		x		
C. Legislative	x			
D. International		x		
What role and opportunities does this technology offer for public-private cooperation?				
▪ Mine data for interesting activity (trend to democratise forensics)				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Will fail if 100% anonymous. Computer forensics could undermine anonymity if abused (not necessarily Government, could be a third party) ▪ Lack of end-to-end system, more access points, more options for fraud ▪ Why make haystacks better? But way of engendering trust ▪ Audit trail will become an ever increasing feature but how much do we need?				

Discussion

- Data mining undermines anonymity and trust in scheme
- Individual verification or trawling

Group 4: Results and discussion

Interoperability standards				**Comments on Definition** Need to separate secondary identity providers, providing support to external 1-op-standards e.g. IKO. NIR has clear 1-op-standard with secondary identity providers
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	x			1. Politicians, Government/commercial uses/needs 2. Needs open, interoperable standard 3. Necessary for market to work
2. Government	x			
3. Business	x			
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards				A. Liability issues have to be exterminated B. Underpins user-friendliness C. Need to create getaways/remove existing barriers
B. Consumer				
C. Legislative			x	
D. International				
What role and opportunities does this technology offer for public-private cooperation?				
▪ Multifunction schemes lead to interoperability problems ▪ Architectural weaknesses				
Timescale in Use/Impact; Doability; Applicability; Technical possibility, Commercial viability; Social, Political viability/Acceptability				
▪ Architecture is key				

Discussion

- Not just international: must also achieve public-public consensus
- Need to separate what is public and what is private
- IKO: does this thing want to be multifunctional and act as a travel document
- It must work between businesses and Government, systems etc
- Government needs to set up open access and standards for how we interoperate
- Have the NIR at the top; additional data feeding in & government a tree with many branches feeding into NIR. Other main branches to feed into NIR are supermarkets, pharmacists, mobile phone providers who will have to interface with NIR. How much info will be available to Government?
- If businesses are going to operate using NIR they have to have a framework
- From a consumer perspective it will have to be user friendly
- More multi-option schemes complicates & adds to interoperability obstacles
- Interoperability of standards must include European standards
- Legal implications must be considered

User-Friendly Solutions				**Comments on Definition** Must give benefit to individuals; people-centric. Two aspects: ease of use and delivering benefit
Players	**H**	**M**	**L**	**How does this technology influence actors, govern their actions, be used by actors?**
1. Individuals	x			1. Increase and broaden take up 2. Set minimum standard for private sector for development of systems to minimise exclusion 3. Critical mass is very important. Systems must aim for ubiquity – support multiple channels
2. Government	x			
3. Business	x			
Key Issues	**H**	**M**	**L**	**How will this technology impact on these key issues?**
4. Exclusion and Inequalities	x			4. Can reduce technological exclusion 5. Must recognise rights of individual 6. Individual must feel it retains ownership. Data subject should be in control of extraction of value 7. Critical – derives from success of 4-6 8. Users must see risk attitudes reflected in system
5. Privacy	x			
6. Ownership, Control, Extracting value	x			
7. Trust and Culture	x			
8. Attitudes to Risk	x			
Challenges & Dimensions	**H**	**M**	**L**	**How will this technology shape the response to these challenges and new dimensions?**
9. Environment			x	10. Must be user-friendly across age range and must be mobile 11. Yes 12. Should be useful in remote usage as well as face to face
10. Demographics: Mobility and ageing	x			
11. Criminality	x			
12. Internet				
Key PPFI Dimensions	**H**	**M**	**L**	**What link between the technology and these PPFI dimensions?**
A. Convergence and Common standards				A. Must be common standards for system to be useful B. Must improve quality of life, every aspect C. Protection of individual data. Legislation can obstruct user friendliness e.g. money laundering D. User friendliness must be international
B. Consumer				
C. Legislative				
D. International				
What role and opportunities does this technology offer for public-private cooperation?				
▪ Who will lead? Private sector or Government? ▪ Government could impose user friendliness by setting standards ▪ User friendly is key issue for consumers ▪ Value-based identity vs basic core identity ▪ Government must expect that private sector will want to have easy access to/ free use of info on NIR (with individual consent) ▪ Could massively increase the resolution for traceable products within the public and private sector				

Discussion

- A high priority throughout for Government, individual, business
- Critical mass important
- Exclusion inequalities; policy must recognise
- Individual must feed own data
- Trust and culture derives from others

Regionally/Globally Unique Identifiers	
What role and opportunities does this technology offer for public-private cooperation?	
▪ An essential component of interoperability	

Nanotechnology	**Comments on Definition** Off the radar Not significant

Appendices

Appendix One: Participants

Iain Bourne	Information Commissioner's Office	
Maria Burroughs	Department of Trade and Industry	
Spencer Chapman	Identity and Passport Services	*
Sir James Crosby	Chair, PPFI	
Simon Davies	London School of Economics	
John Elliott	Consult Hyperion	
Jerry Fishenden	Microsoft	
Robert Temple	BT	
Duncan Hine	Qinetiq	
Colin Robbins	Siemens Enterprise Communications Limited	
Michael Keegan	Fujitsu Services	
Neil Fisher	Unisys	
Tim France-Massey	Multos	
Bill Guy	HMTreasury	
Michael Huth	Imperial College London	
Rob Laurence	Interactive Media in Retail Group	
Rupert Lewis	Horizon Scanning Centre, OSI	
Geoff Linton	Oracle	
Alasdair Keith	Outsights-Ipsos MORI	**
Simon Mitchell	Accenture	
Jeremy Monroe	IBM UK	
Neil Munroe	Equifax	
Barbara Muston	Outsights-Ipsos MORI	**
Richard O'Brien	Outsights-Ipsos MORI	**
Jon Parke	Horizon Scanning Centre, OSI	
Fred Preston	Motorola	
David Rennie	Identity and Passport Services	*
Andy Robinson	Serious Organised Crime Agency	
Toby Stevens	Enterprise Privacy Group	
Julian Thompson	Outsights-Ipsos MORI	**
Richard Trevorah	tScheme Limited	
Colin Whittaker	APACS	

* PPFI Working group project manager

** Facilitation team

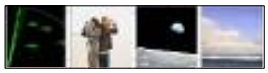
Appendix Two: Workshop Presentations

Introduction Presentation

Foresight: Horizon Scanning Centre
Office of Science & Innovation

Identity Management Workshop

Prospero House
24 January 2007



1

Foresight: Horizon Scanning Centre
Office of Science & Innovation

Overview

Purpose of the workshop:

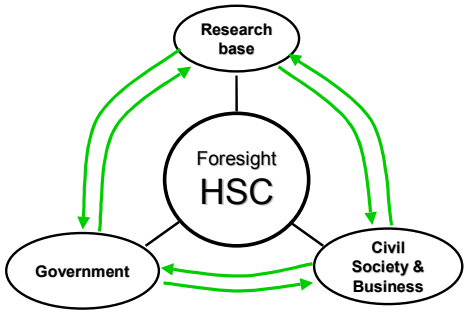
- To explore the scope and opportunities for technology to deliver viable and sustainable solutions to the future (2 to10 year) challenges of ID management.

NB - Chatham House rules

2

Foresight: Horizon Scanning Centre
Office of Science & Innovation

Position and role of the HSC



3

Foresight: Horizon Scanning Centre
Office of Science & Innovation

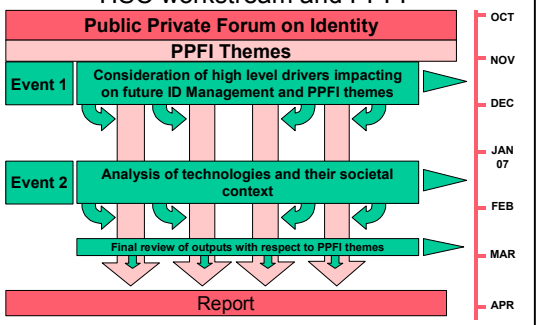
Workshop objectives

- Conclusions of the first workshop
- Review current and emerging technologies
- Consider the potential impacts on the themes of particular interest to PPFI

4

Foresight: Horizon Scanning Centre
Office of Science & Innovation

HSC workstream and PPFI



5

Key Context Dimensions Presentation

Identity Management Workshop: scope and opportunities for technologies

Hosted by OSI HSC

Ipsos MORI outsights

Identity Management

Our Framework and Questions

12 contextual themes
- Players
- Key issues
- Challenges and new dimensions

Four PPFI dimensions
- Consumers
- Convergence and common standards
- Legislation
- International

Key assessment dimensions
- Role and opportunities for public-private cooperation
- Timescale, Viability, Acceptability

Ipsos MORI outsights

Identity Management

The Players

1. **Individuals**
   - Importance of perception: "it works for me" and "hassle reduction"
   - Labour markets, immigration, and impact of EU legislation
2. **Government**
   - Gaining citizen trust in delivering public services
   - Managing devolved and supranational dimensions
3. **Business**
   - "Business buy-in critical for consumer buy-in"
   - Shapers of IDM
   - Issues will change as the nature of transactions change

Ipsos MORI outsights

Identity Management

Key Issues

4. **Exclusion and Inequalities**
   - Creating better access and individual choice in public services provision
5. **Privacy**
   - Grey area between governance and privacy: how is the consumer empowered to change things? People need to be more aware
6. **Ownership, Control, Extracting value**
   - Control of what companies ask you to provide
   - For consumer, extraction of value from information is a threat
7. **Trust and Culture**
   - Culture of trust emerges as people understand what they have to do (e.g. eBay) through use and experience. Trust requires standards
8. **Attitudes to Risk**
   - Individual and collective differences. Needs standards

Ipsos MORI outsights

Identity Management

Challenges and New Dimensions

9. **Environment**
   - IDM important response; saleable consumer benefits
10. **Demographics: Mobility and ageing**
    - International movement of people requires international framework
    - Diversity makes it harder to create an identity framework
    - Will biometrics be reliable with ageing and diversity?
11. **Criminality**
    - Impact overstated? Opportunity to close loopholes on low-level criminals. International dimensions
12. **Internet**
    - New domain, requires adaptation; open vs closed aspects; difficult to control internet over any planning time-period

Ipsos MORI outsights

Key Context Dimensions Presentation

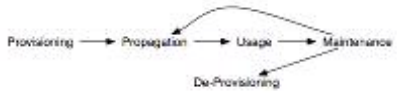
Imperial College London

Identity Management:
Key Technologies

Michael Huth
imperial.ac.uk/quads

Identity Management System (IMS) lifecycle

- ***Provisioning:*** creates/initializes identity records
- ***Propagation:*** stores/sends identity records to required locations/devices
- ***Usage:*** e.g. *authentication of finger print*
- ***Maintenance:*** *change management* of identity attributes and required resources
- ***De-provisioning:*** remove identities from IMS



Biometrics

- Uses biological or behavioral traits to *uniquely identify* person or animal
- E.g. *signatures, voice, palm or finger prints*
- Its strength (uniqueness) also its weakness: e.g. *copies of finger prints "as good" as the real thing*
- Useful for *negative identification*, e.g. *detection of benefit fraud*

Authentication & Authorization Technologies

- ***Authentication:*** process of checking validity of credentials, e.g. *passport*
- ***Authorization:*** process of mapping identities onto entitlements for access to resources
- Authorization Technologies have Authentication Technologies as vital components
- E.g. *check authenticity of passport before granting access to baggage claim area*

Key Concepts

- ***Subjects:*** agents that can request access to resources, e.g. *you or Microsoft Word*
- Subjects get access by claiming identities
- ***Identities:*** collate attributes or traits of subject
- ***Traits:*** *inherent* characteristics, e.g. *eye color*
- ***Attributes:*** *acquired and transient*, e.g. *visa status*
- ***Credentials:*** means of *laying claim to* an *identity*, e.g. *biometric*

Two-Factor Authentication

- Authentication based on two credentials, *both must be approved*
- E.g. *ATM card & PIN. Username/password. One-time passwords for sensitive transactions.*
- Great scope in nature and interaction of two factors
- Two- and multi-factor authentication have *many future applications*, e.g. *fraud resistant train tickets, electronic voting, and exams*

Directories & their Meta and Virtual Versions

- ***Directories:*** centrally managed repositories for retrieving structured information to be supplied to distributed applications
- E.g. *Domain Name Server (DNS), X.509 Public-Key Infrastructure Standard, Lightweight Directory Access Protocol (LDAP)*
- ***Meta Directory:*** centrally managed, *needs to synchronize* with other directories of organization
- ***Virtual Directory:*** *no synchronization, presents single/integrated view* of data that reside in different directories

Identity Management Systems and Architectures

- ***IMS Architecture:*** result of systematic analysis of how to conceive and carry out identity management in an IMS
- Comprises *process* architectures, *data* architectures, *policies*, and *interoperability frameworks*
- Architectural Patterns, Best Practices, *Capability & Maturity Models* will emerge

Role-Based Access Control

- Systems that control access to resources *based on subject's role*, not their identity
- E.g. *company access policies*
- E.g. *role-based email: seniortutor@imperial.ac.uk*
- Offers *better change management*: only role attributes need to be updated; existing credentials then bind to new role
- Different roles as different personas

Digital Rights Management Systems (DRM)

- Framework for *controlling circumstances* under which digital resource can be used
- Possibly dependent on usage history but independent of usage location
- E.g. *Fairplay (iTunes), Zone Codes for DVDs*
- Of considerable interest for military and media companies
- Consumers need to see *cost/benefit value* in being under such contextual usage control

Federated Identity, Risk/Trust Management

- ***Federated Identity:*** Software architecture with *low coupling between heterogeneous IMSs*
- Coupling provides well defined & contained sharing of information
- E.g. *PingID & SXIP offer products*
- Increasingly important for *opportunistic federations in business and government*
- ***Risk/Trust Management Systems:*** automated risk assessment, risk revision; e.g. *in setup or negotiation of federations*

Anonymity, E-Cash, and E-Voting

- ***E-Cash:*** (real or virtual) money exchanged in electronic form
- ***E-Voting:*** provision, conduction or audit of election by electronic means
- *Anonymity or Pseudonymity* desired in E-Voting
- E-Cash versus Credit/Debit Cards
- Anonymity versus Traceable & Analyzable Customer Behavior
- Great potential of E-Cash and E-Voting in future

Interoperability Standards

- Specifications of *how data & processes should be implemented so that other systems can understand them*
- E.g. *Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML), eXtensible Access Control Markup Language (XACML)*
- *Clear need for this*, e.g. in federated IMSs
- *XML key technology driver*

User-Friendly Solutions

- Solutions to Identity Management that are *easy to learn*, *easy to recover*, etc.
- E.g. *Single-Sign-On, Identity-Based Encryption, Self-Service Password Reset Service*
- *Free* Wide Area Wireless Network Access?
- *User empowerment great economic & societal enabler*

Regionally/Globally Unique Identifiers

- Means of *identifying subjects* or resources *uniquely within a region*, or globally
- E.g. *Oyster Card, Radio Frequency Identification Device (RFID), Universally Unique Identifier (UUID), The Digital Object Identifier System (DOI)*
- *Public perception and trust issues*
- Open standards and solutions (e.g. UUIDs) can be used within IMSs
- DRMs to control use of Unique Identifiers, e.g. *National Insurance Card*?

Pie-in-the-Sky Technologies

- ***Quantum-based Digital Identities:*** require scalable and stable quantum computers, which will make *past digital signatures insecure*
- ***Adaptive Behavior:*** *Ad hoc networks*, e.g. *Car Platooning*, and the emergent & evolving roles/identities of agents therein
- ***Computer Forensics:*** *increased logging of identity-related information* for possible forensic activities; privacy issues
- ***Nanotechnology:*** creation of *unobtrusive and unique credentials*, e.g. *"synthetic" biometrics*

Recommended Reading

Philip J. Windley
Digital Identity
O'Reilly Media, Inc.
2005