

Personal Identity Working Group

Drafted by: Dave Wright
Date prepared: 13/01/05
Date finalised: 24/01/05

Circulation: Group Members

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



Summary report of the EURIM Personal Identity Group meeting held on 12 January 2005, 1000-1200, Committee Room 19, Westminster Palace

Chair: Stephen Darvill (LogicaCMG)
Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The purpose of the meeting was to review the Group's progress on the circle of trust, process map, risk assessment and consideration of the need for primary legislation on data sharing.
2. A proposal for a pilot scheme on the validation and accreditation of lifelong updating and experience was agreed, to be operated jointly by IMIS and CHPC (see attached document). The EURIM proposal is an attempt to establish a self-funding, evidence-based, internationally accessible circle of trust model in the public sector, founded on lifelong learning, work experience and continuous professional development. The scheme would apply the same criteria to assessing employability as those that pertain when defining an individual's creditworthiness. Sponsors are now being sought; Experian is a possible candidate, and may be looking for partners to carry the exercise forward.
3. It was agreed that the risk assessment exercise should proceed as a straw man using public data, but applied to circle of trust model only alongside a specific Group proposal, likely to be in the area of education.
4. A meeting is planned with the Department of Constitutional Affairs in the near future to produce a timetable and to progress agreed collaborative actions on the data sharing process map. DCA is currently gathering information on statutory bars that prevent data sharing. The development of a successful Process Map for data sharing at the practitioner level might avoid the need to call for primary legislation; alternatively, it might identify areas where statutory solutions are required.

1. Introduction

1.1 The aim of the meeting was to review the Group's progress on the circle of trust, process map, risk assessment and consideration of the need for primary legislation on data sharing.

2. Circle of Trust Model (tabled paper)

2.1 The original aim was to test the Circle of Trust model in a particular field, and to assess its value and limitations. A proposal for a pilot scheme was presented on the validation and accreditation of lifelong updating and experience, to be operated jointly by IMIS and the Conference of Heads and Professors of Computing (CHPC), (see attached document).

2.2 While many different types of records of achievements exist, they mostly offer the same basic information, with little emphasis on validation. The proposed CV model would apply the same criteria as in defining an individual's creditworthiness when assessing employability, and which requires evidence gathering for international records. The intention now is to identify who is serious enough about wanting such evidence to pay for it; Experian is a possible candidate, and may be looking for partners to carry the exercise forward.

2.3 Could the model be seen as an analogue of the problem that applies to Government-related schemes? The circle of trust model is similar to those of the financial services and credit reference agencies, where people want their data to be shared because they want a service. If statutory duties to share are employed, there is no role for trust or consent. It can be argued that trust and consent models should be used wherever possible, but this would require major change in many public sector bodies. The EURIM proposal is an attempt to establish a self-funding, evidence-based, internationally accessible circle of trust model in the public sector, founded on lifelong learning, work experience and continuous professional development. Recent consultations on FE college funding indicate some movement in this direction, but this is based on social inclusion programs rather than workforce updating.

2.4 Information Sharing and Assessment is a key component of the Children Act 2004 which will ensure that every child at risk will be properly identified, referred to appropriate preventive services and that their progress will be monitored to ensure that they do not subsequently 'fall through the net'. DfES workshops are held to enable practitioners to contact others and develop a data-sharing index in a variety of agencies. The aim is to integrate information across services and develop an ISA system in every authority as part of a Local Preventative Strategy. Systems will be based on national standards to enable the exchange between local authorities and partner agencies of information on individual children. Systems will also be capable of interaction with other data sets. No permission or consent is needed to share data in the model, although it is considered good practice to inform parents in appropriate circumstances.

2.5 The EURIM circle of trust model did not require that consent would always be necessary, but that notification of data access requests could be made available to the individual whose data was accessed, to provide checks and an audit trail. Although the circle of trust model could be considered to be a hybrid between a pure consent model and an hierarchical model, there could never be a pure consent model because various bodies have powers to access data held under the consent model. The same situation would arise with the CV model, in relation to the probity, suitability and criminal history of people in high-risk situations such as financial services or child protection. Thus the underlying business case, based on a consent model, will be subject to statutory overrides and in the real world, the model will always be a hybrid.

3. Risk Assessment

3.1 It had been suggested that risk-assessment should be integral to the circle of trust model, and that EURIM should encourage risk assessment and benefit exercises to be undertaken across the public sector. Initially, it had been intended to quantify the probability of identity theft taking place, e.g. in the roll-out of ID cards across the national population of some 60 million people. However, difficulties had been encountered in advancing this proposal because it had proved impossible to obtain real data to be incorporated in a realistic model. A simplified approach is now proposed based on a 'straw man' using data in the public domain, and applying it to the circle of trust model. Future plans are outlined in the Progress Report attached to this email.

3.2 Another dimension was that although governance and information assurance models were associated with risk assessment checklists, none dealt with ranking and probabilities. The intention was to apply risk-modelling discipline to identify the probabilities and ranking of risk so that an effective response could be implemented. The reluctance of organisations, including EURIM members, to release data for a risk-assessment exercise, is directly related to their competitiveness, internal security and good name. The use of theoretical data however might afford the possibility of constructing realistic models.

3.3 A suggestion that contact be made with the DfES team working on a feasibility study on risk-modelling had not so far produced a response. Another suggestion was that EURIM might work with DfES looking at Recommendation 19 of the Bichard Inquiry (the proposal for a new national registration scheme for those who work with children or vulnerable adults). Informal approaches will be made to see if EURIM can help in this area. Another possible avenue might be in collaboration with the Financial Services Authority.

3.4 There was some scepticism that a single model would be applicable generally: different organisations require different models, what risks would be assessed? However, the key issues in Government systems are public sector data sharing and identity; massive investment was required, and we should surely assess risks beforehand. Although departments are in many cases using and adapting existing systems, this does not mean that we should ignore risk, and in any case, the central system for e.g. the NHS would be new and risk would have to be quantified and managed.

3.5 Concern about definitions was expressed – are we talking about a single public sector system or one with multiple identities? Or are we talking about different elements of a common infrastructure? Would the risk assessment apply to a single application, or to a value-for-money judgement of the infrastructure? There will be many public sector identities and different systems – e.g. the driving licence and passport are 2 different identities. It is important to keep separate absolute identity from an identity defined by a relationship with an organisation - the individual could then choose to share information with different organisations, and should be able to control by consent what personal information held by an organisation is shared with others. We should also differentiate between companies performing risk assessments on the delivery of services to Government, and Government departments that should be making risk assessments of the impact of service delivery on the citizen.

3.6 An original aim was to test the application of classical risk assessment methodologies by using a specific example within the circle of trust model. This had been mostly lacking in most public sector system proposals, and operational standards for risk assessment within e.g. the e-skills frameworks is one of the gaps that need to be filled. Although PRINCE 2 and the related area of Management of Risk was supposed to require risk assessment before a project was started, this often did not apply in reality. **It was agreed that the EURIM Personal Identity Group should apply risk assessment only alongside a specific Group proposal, likely to be in the area of education.**

4. Data Sharing Process Map

4.1 A copy of the current draft Process Map was distributed (attached with this report), together with a summary of the planned actions and outcomes of a meeting on 15 December between members of the EURIM PI Subgroup and officials from the Department of Constitutional Affairs. Collaborative work is continuing on this, in consultation with the Information Commissioner's Office, with shared responsibility for specific tasks between EURIM and DCA.

4.2 The development of a successful Process Map for data sharing at the practitioner level might avoid the need to call for primary legislation. Alternatively, it might identify areas where statutory solutions are required. DCA is currently gathering information on statutory bars that prevent data sharing. A meeting with the EURIM PI Subgroup is planned in the near future to produce a timetable and progress the agreed actions.

4.3 Once a practical model is developed, it will be tested in a working environment, perhaps with CIPFA. The draft process map will be posted on the website so that it can provide a resource as a working document, and also act as focus for comment, so that it can be continually updated and developed in response to comments from practitioners.

4.4 It was agreed that early draft of the Process Map, as it currently appears on the EURIM website (www.eurim.org.uk), could be cited as an example of the work EURIM is doing with DCA in providing practical guidance to data sharing practitioners, in an article for the IMIS journal. Interested parties will be invited to join EURIM.

5. Discussion

5.1 It would be useful to know if a comprehensive list of the plethora of data sharing and personal identity initiatives exists and if not, is there value in creating such a list? The EURIM e-crime study has generated a set of grids listing both players and initiatives in collaboration with Home Office and NHTCU. The grids are posted on a website so that they can be a source of information and a focus for comment, and are constantly being updated by sector input. The grids have thus become the most comprehensive source of information on current players, initiatives and schemes available in the UK; no-one else is doing this, and Home Office or NHTCU would not wish to. Should EURIM attempt something similar to add value for data sharing, perhaps in cooperation with DCA and other departments, but without declaring such? The list would always remain a 'draft for discussion only', and thus be subject to continual updating as a source of information.

5.2 A more pressing problem is data quality and verification, and which departments were responsible for the various exercises. It was agreed that the eGU be asked if it has been collating initiatives on personal identity, and whether this was still being undertaken; if not, maybe EURIM could do this. It is often the case that a grid of information can act as a powerful tool for change by stimulating new initiatives whilst identifying those that exist as concepts only; by doing this independently, suspicion would not fall on others as to their motives.

6. EURIM to help Ian Watmore --DW

6.1 An email was sent to Andrew Stott on 8 December to see if EURIM might be able to help Ian Watmore and the eGU to achieve its priorities of working across Government to create 'joined-up' IT strategies, and to promote relationships with the private sector. This work may also tie in with the eGU priority to secure reform of the governance of publicly held information, including identities. AS was informed that a major objective of the group is to put the issue of data sharing into the context of how to improve service delivery to the citizen, and to identify whether barriers to doing this are legal, cultural or organizational.

6.2 Ian Watmore would be attending a private dinner in February at which the topic for discussion is 'Identity in Cyberspace'. It was agreed that we use this opportunity **to approach IW on the issue of how EURIM could help eGU, particularly with issues of security, public sector information assurance, and efficiency (of service delivery).**

6.3. The e-Government Interoperability Framework (eGIF) was an initiative that had significant take-up by local authorities with regard to interconnectivity, data integration, e-services access and content management. A move to a common infrastructure is necessary across all sectors.

7. Agreed Actions

7.1 The agreed actions are:

- circle of trust – to continue with a proposal for a pilot scheme on the validation and accreditation of lifelong updating and experience to be operated jointly by IMIS and CHPC;
- risk assessment exercise – to pursue enquiries informally with DfES with regard to Recommendation 19 of the Bichard Inquiry;
- risk assessment exercise – to proceed with straw man applied to circle of trust model using public data;, and to explore a possible collaborative approach with FSA;
- data sharing process map – to set date for future meeting between EURIM and DCA;
- to speak to IW with respect to EURIM input to eGU;
- to ascertain if eGU is collating a grid of initiatives on personal identity.

8. Date of next meeting

8.1 The date of meeting will be 9 March to allow for input to policy in advance of the election process.