Draft Report of the Identity Governance Subgroup meeting held 1000-1200 on 7 May 2009 in Committee Room 8, Westminster Palace

Chair: Lord Erroll (EURIM)
Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

- A draft tripartite mission statement was presented for discussion:

    1. "To look at existing and proposed frameworks for the governance of identity, whether in the public or private sector, regulated under statutory powers or not, national or international.
    2. To summarise how they seek to meet the needs and rights of relying parties, the owners of the identities, and the organisations responsible for the protection, how they handle registration, management, use, revision, retirement and repair of identity information and how they handle inter-operability across organisational, regulatory and jurisdictional boundaries.
    3. To produce appropriate material to help inform those looking at policy formation and scrutiny or responding to consultations".

- The mission statement was agreed, subject to rephrasing to achieve clarity, and certain amendments. These were to add 'obligations and responsibilities' to 'needs and rights' in Part 2, and to refer to benefits and risks. Although there was no definition of 'identities', which could mean different things, there was a purpose and a benefit in preserving ambiguity at this stage: the "owners of the identities" could refer to both individuals and organisations as owners, and it may be useful to deal with each separately. The mission statement should also include reference to purpose and timeliness.

- Successful policy implementation requires an appropriate governance structure which has been shown to work in practice. By looking at the different governance frameworks, common attributes can be determined.

- The Subgroup should identify those circumstances in which the use of an unique identifier, for strongly authenticating identity, is justified, and the circumstances where alternatives may be more appropriate. Where there is a justification for using an unique identifier, it may be useful to define rules to cover it.

- There is potential for confusion between the identity card and National Identity Register Number (NIRNO), and whether the NIRNO as an identifier would be used to join up lead identities, or cross referenced across multiple transactions to track a person's everyday activities.

1 Introduction

1.1 The Chair opened the meeting and welcomed those present, inviting them to introduce themselves.

1.2 DW explained that Lord Erroll had very kindly stepped in at very short notice to chair this meeting, due to unexpected developments.

2 Mission Statement

2.1 The Chair invited discussion on the draft mission statement:

a) "To look at existing and proposed frameworks for the governance of identity, whether in the public or private sector, regulated under statutory powers or not, national or international.
b) To summarise how they seek to meet the needs and rights of relying parties, the owners of the identities, and the organisations responsible for the protection, how they handle registration, management, use, revision, retirement and repair of identity information and how they handle inter-operability across organisational, regulatory and jurisdictional boundaries.
c) To produce appropriate material to help inform those looking at policy formation and scrutiny or responding to consultations".

The need is for good material to pass to those working on policy drafts over the summer and for use in organising meetings to inform the political "class of 2010".

2.2 LE cautioned against focusing on technological aspects, and emphasised the need to concentrate on governance issues. While we need to be clear about what technology is capable of, it is information governance enabled by technology, and associated issues such as privacy, that we are concerned with. A subgroup looking at technological aspects could be established, for those who wished to do something on this.

2.3 The Report of the 2008 Working Group on User-Centric Identity (& Personal Information) Management, as sponsored by the Information Commissioner's Office, the Technology Strategy Board, and the Cyber-Security KTN, had been circulated to Subgroup members just prior to the meeting. One member said that he had found the Report useful, but felt that it skimmed over governance issues – which this Subgroup is all about. The issues raised by the report could be more appropriately discussed further into the agenda.

2.4 An action from the last meeting had been to produce a draft mission statement. This had been done, and it consists of 3 parts. Rather than be sidetracked into a debate on other issues, it might be useful to consider each part separately, and either accept or amend them in turn. After brief discussion, Part 1 of the mission statement was agreed.

2.5 Part 2 was considered to be too complex, and was unclear. For example, it was unclear what was meant by 'the protection'. Was this a typographic error? Should it be 'their protection', and if so, to whom or what did 'their' relate? It was probable that 'they' referred back to the frameworks (existing and proposed) in Part 1. This was agreed. What seemed to be clear however was that we should be considering how the existing and proposed frameworks would meet the needs and rights of all involved.

2.6 Another question concerned whether this referred to the protection of the individuals and relying parties, or of the protection of the identities? This might refer to the owners of the identities and the relying parties. Or was it the protection of the needs and rights? The precise meaning needs to be clarified. It was agreed that 'obligations' be added to 'needs and rights'; this was agreed.

2.7 It was suggested that the last part of the mission statement should be put at the start, because this was the Subgroup's objective. Others disagreed, stating that the logical sequence was to identify and evaluate the frameworks at the outset, and then determine the outcomes we wanted. It would not be feasible to produce appropriate material without relating to the existing frameworks. The mission statement was for us, to aid the production of an appropriate output for the target audience, which would assist them in the development of better policy outcomes.

2.8 EURIM's purpose is to inform the debate in parliament (including in the EU), and the material we produce should be designed to achieve this. The aim is to influence policy at the earliest stage, and this includes providing material to advisers, staff and officials, as well as parliamentarians. This would include the House of Commons Library, which produces authoritative and respected briefing packs for MPs.

2.9 It was suggested that for Part 3, we should consider adding something about benefits and risks. Although there was no definition of 'identities', which could mean different things, there was a purpose and a benefit in preserving ambiguity at this stage, which could help build consensus. Thus the "owners of the identities" could refer to both individuals and organisations as owners. We also need to clarify that the UK is required to introduce an identity card under EU legislation, and say why – rights change according to the purpose.

2.10 After some debate, it was decided to leave the order of the mission statement as it is, as this was the order in which we needed to work, but to amend it so that the statement included reference to obligations, purpose, timeliness, risks and benefits.

3 Assessment of other experiences of Identity governance

3.1 Those present were invited to report their experiences of identity governance, including case studies, use cases and examples of best practice. The term 'identity governance' is broader than identity management and identity assurance, and deals with policies on IM and IA. The frameworks and rules have to be managed and the different processes joined together in order to ensure that policies can be applied (which are enabled by technology). Identity governance involves the management of policies and the methods by which compliance with those policies is demonstrated.

3.2 An example of a framework in the education sector is where JANET operates the UK Access Management Federation for Education and Research. A Policy Board ensures that the federation's policies are implementable within JANET(UK)'s legal framework. Organisations may join as an Identity Provider (e.g. a university or local authority), or as a Service Provider (e.g. a publisher or content provider), or as both. A federation allows organisations and resources to work together within an agreed set of policies, governance and legal understandings. [DW: The federation uses the standards-based Shibboleth software, which defines a common framework for access management and governance that is being adopted by education and commercial sectors across the world. More details of the federation and framework are available at:
http://www.jisc.ac.uk/aboutus/committees/workinggroups/federationpolicy.aspx and at:
http://shibboleth.internet2.edu/

Shibboleth's policy framework will also allow inter-operation within the higher education community. An illustrated explanation of how Shibboleth works can be located at http://www.ukfederation.org.uk/content/Documents/HowItWorks. Although Shibboleth has been designed primarily for secure access to web resources, work is ongoing to extend the framework for institutional authentication and authorisation]. **Please send details of other frameworks to DW**.

3.3 Where disparate commercial organisations are seeking to collaborate, they may have established policy organisations to manage this, but the governance and policy rules are considered as IPR, which is unlikely to be shared publicly. However, there are increasingly occasions when it is not necessary to know someone's identity for transactions; in fact there ought to be good reasons for wanting to know identity. A strict policy might be in place where absolute assurance about an identity is required. On the other hand, loose registration but tight authentication may be appropriate, so that e.g. for a blood test, it is not necessary for the identity to be known, but it is essential that the right person receives the result of the test.

3.4 The identification of examples would satisfy Part 1 of the Mission Statement; tScheme is a method of demonstrating compliance with a policy. A framework could therefore use tScheme as the gatekeeper for access to a community. Where it is necessary to repeatedly assert one unique identity, enrolment and the verification of credentials are key to the entire process – whether we agree with this or not. The federated identity approach is an alternative for appropriate circumstances.

3.5 Governance of identity need no longer be seen as a necessary function solely of the state. Over the Internet, particularly concerning financial services, there has evolved a number of different

approaches for managing and governing the use of identity, nationally and internationally. This practice might be useful to look at; anyone with examples should pass these on to DW, for the Subgroup to look at in compliance with Part 1 of the mission statement.

3.6 It was noted that many social networking sites have identity governance policies which users have to agree to – e.g. it is not possible to de-enrol from Facebook. Different access controls using different combinations is an interesting way of looking at accessing services, including signatures and biometric controls. By looking at the different governance frameworks, common attributes can be drawn out e.g. policy characteristics and lifecycle management, gatekeeping functions for implementing and demonstrating policy appliance, so that can a governance structure can be invoked when enforcing policy. Successful policy implementation requires an appropriate governance structure which has been shown to work in practice.

3.7 The ability to partition the policy may depend on the ability to identify a number of governance frameworks to draw out key attributes for a particular purpose. Policy should be set in the governance environment, where it serves as a basis for developing processes and standards for the management of information, and the activities that need to be carried out. It is also concerned with matters such as who owns the information.

4. How to create a unique, trusted identity, and how this should be governed once established in a service environment

4.1 This proposition seems to assume that a unique trusted environment is what is wanted – and this is a key consideration. A secret is something that only you know, but once someone else knows, it is no longer a secret. Identity is much the same: the more that your activities can be tracked to a single identifier, the less privacy you have. The need is to balance individual privacy with society's right to protect people from harm by identifying wrong-doers. However, this should include the right to have a choice to take advantage of a cost-benefit if someone wants their identity to be shared for a given purpose.

4.2 The question is therefore, do we want to discuss how to create a unique, trusted identity, looking at enrolment, registration etc., or do we want to discuss whether or not we want to create a unique, trusted identity? The Post Office is building a national identity verification biometric enrolment infrastructure and service across the UK, although the Post Office has no interest in managing the identity acquired. This is related to where the boundary is located between the needs of central government and the rights of the individual, which is discussed in the User-Centric Report he had circulated. We need to draw out the two different standpoints.

4.3 It was suggested that we should spell out when the state, or an organisation, has the right to correlate identities, and when the individual has the right to prevent that correlation. An unique identifier doesn't necessarily carry detailed information about the person, but may be useful as an index to other data.

4.4 The possession of an unique identifier does not convey any information about whether someone is trustworthy or not, but gives a high degree of assurance that the identifier is linked to a particular individual. It was proposed that this is where the issue relates to risks and benefit; e.g. a bank has to be sure that you are who you say you are. Others disputed this, saying that this requirement was supposed to be related to tackling counter-terrorism. Financial transactions over the Internet do not require a unique identifier; sufficient information to assure a level of confidence in the ability to pay is generally all that is required.

4.5 Uniqueness is important in a number of circumstances, e.g. so that we can be paid correctly as employees. The example was given of a register set up for landlords that lists high-risk tenants, which is considered to contravene the individual rights and privacy of the individuals listed. Is this justified? It was suggested that if it was a fair and transparent list; it would be difficult to pursue a complaint.

4.6 An unique identifier used outside a closed system could generate serious problems. The unique identifier for the identity card should be used only in a closed national system, but uses are envisaged within subsets of that closed system, or across systems (e.g. an ID card is intended to be used for travel within Europe). However, credit reference agencies will collect information and create e.g.

registers for bankruptcies. Legislating against this will only drive the practice underground, so it is better for a governance system to acknowledge the existence of the lists than not.

4.7 There are circumstances when we do need a token, or an unique identifier, for strongly authenticating identity, or entitlement to a service, e.g. when dealing with certain Government departments, and others where it would not. It was agreed that we should demonstrate for our target audience of parliamentarians and policymakers examples of circumstances in which each or either might apply, or have a use. Perhaps a good way of capturing the debate would be to say that if there is a justification for using an unique identifier, then these are the rules that should cover it.

4.8 Policy is a mechanism for assuring that an outcome is achieved; if the outcome you want to achieve is a demonstration of an unique trusted identity, you should write a policy that can give some assurance that that outcome will be achieved. Similarly, if you have a business need that requires an outcome, a policy should be designed to achieve it. But to imply that such an outcome is the *only* one to consider would be too narrow. It is just an example of a policy that can be placed in a governance framework.

4.9 One problem is the confusion between the identity card (where the purpose is authentication) and National Identity Register Number (NIRNO); we should be concerned about how the NIRNO as an identifier can be used to join up the lead identities, or cross referenced across multiple transactions to track a person's everyday activities.

4.10 It was possible in the next 12 months that the ID card would be cancelled, but the NIR may continue - this is another area of debate. It was suggested that all members of the ID Governance Subgroup should be encouraged to read User Centric ID report preparatory to a 30-minute presentation on this at the next meeting. One aim would be to help identify those circumstances in which we might advocate the use of an unique identifier, and those in which we would not.

5. Outcomes planned, interoperability issues

5.1 A succinct, 1-page A4 document for parliamentarians and policymakers was envisaged as a main output. This might contain links to more detailed web-based resources (including the EURIM website), and/or be accompanied by more innovative media, e.g. video clips. The User Centric report could be posted to the website.

5.2 Use cases could be added to the website in the context of different circumstances, policies and governance structures, while keeping the main document to 1 page. The meeting was reminded that the target audience was parliamentarians and policymakers, and to increase the chances of our output being read, it had to appeal while being brief. A short, snappy, sentence on the core issue could direct attention to other sources.

5.3 One of the recipients of our 1-pager and linked resources would be the House of Commons Library, which regularly provides MPs with authoritative and respected briefing packs across a spectrum of issues. It would be most useful to articulate the benefits and the risks of an identity register, and what parts of the NIS might be kept in order to fulfil the needs of central government and business.

6. Structure of a technology reporting sub-group that looks at existing technologies and interoperability issues

6.1 The meeting considered that the present structure of the Subgroup was fit for purpose. JH and VG undertook to try to locate papers and other sources regarding interoperability issues, e.g. how different governance systems impact on interoperability.

7. Times, frequencies and format of future meetings

7.1 It was agreed that the frequency of meetings should be at 3-4 weeks intervals in the run-up to the parliamentary summer recess (commencing 20 July) and the development of party manifestos for the forthcoming conference season in September. We should aim to produce an output by mid-July.

8. AOB/Date of Next Meeting

8.1 The date of the next meeting will be decided by Doodle Poll and in the interval between late May and early June.