Summary Report of the Identity Governance Subgroup meeting on 7 December 2010, 1000-1200 in Committee Room '2', Westminster Palace

Chair: Lord Erroll
Rapporteur: Dave Wright (EURIM)

NB: Section 2 of the report should be read in conjunction with the accompanying slide presentation.

SUMMARY OF MAIN POINTS

1. The purpose of the meeting was to receive a presentation on aspects of the Cross-Government Identity Management Strategy, and to progress drafting of the longer papers on 'Why world-class Identity Governance is central to UK economic performance' (formerly entitled 'How do they know it is really you?').

2. The Security workstream of the Public Sector Network has produced the cross-Government Identity Management Strategy pertaining to Employee Access; as soon as this is ratified by the CTO Council, it will be released to the EURIM Identity Governance Subgroup list, and sent to the House of Commons/Lords libraries. This is expected by the end of 2010.

3. PSN is planning as part of a cross public sector initiative to introduce an identity brokering system that will allow for employees to authenticate once against their "home" system and for the credentials to be brokered between different systems. The system will deliver a level of trust in each employee and person given access to Government information, in a cost-effective way which involves identifying an individual just once for them to be able to operate where appropriate across-Government.

4. This involves a federated identity framework with a trusted identity broker and multiple identity providers, so that an individual can be registered with any identity provider that operates through a common trust framework to verify the credentials, without replicating the original registration process. Future plans envisage the use of a PKI bridge that will allow shared authentication across other governments and the commercial sector.

5. UK and EU regulatory initiatives around identity risk global organisations based in London transferring their operations to more favourable locations, leading to massive losses of tax revenue to the UK Government. This is a key driver for the publication of the Subgroup's papers on "Why world-class Identity Governance is central to UK economic performance". The first of these, intended for MPs and senior officials, expected to be released shortly.

6. Another business driver for change is the level of identity fraud. Co-operation between the Government and industry on identity assurance will provide an opportunity to drive costs down dramatically. The most costly risk to Government is the potential for organised crime to defraud DWP through identity theft using electronic attack vectors and malicious code akin to that used against banking, unless effective identity governance structures and counter measures are at the heart of the new systems (security by design, not afterthought).

1 Introduction

1.1 Lord Erroll opened the meeting, and invited those present to introduce themselves.

1.2 The purpose of the meeting was to receive a presentation from Andy Smith on the Cross-Government Identity Management Strategy, and to progress drafting of the longer papers on 'Why world-class Identity Governance is central to UK economic performance' (formerly entitled 'How do they know it is really you?').

1.3 The draft 1-page 'Flyer' intended for MPs and senior officials, along with the draft 3-pager for parliamentary researchers and assistants, have been posted to the EURIM website and circulated to the Information Governance Group as working documents, with feedback invited. Feedback and comments from various members have been incorporated where possible into the latest versions.

2. Progress of the Cross-Government Identity Management Strategy - Andy Smith

2.1 AS explained that he was present at the meeting in a private capacity. He had spent 5 years as Chief Security Architect at the Identity and Passport Service, working on security and identity management aspects of the National Identity Scheme; he was now Security Architect for the Public Sector Network (PSN) in the Cabinet Office. [DW: the primary objective of the PSN Security workstream is to ensure that risk is properly managed in a cost-effective manner right across the PSN. The workstream is developing the security standards and policies that will enable easy migration to the PSN from various other networks, allowing stakeholders to make use of 'common good' information assurance services. The workstream consists of CESG IA experts, PSN technical and security experts and is supported in various subgroups by public sector stakeholders and industry. The subgroups are encryption, accreditation, protective monitoring and identity assurance].

2.2 Along with others, AS sits on the cross-Government Identity Management Strategy Group (IDMSG), reporting to the CTO Council. The Security workstream has just finished and published the cross-Government Identity Management Strategy pertaining to Employee Access; as soon as this is ratified by the CTO Council, it would be released to the EURIM Identity Governance Subgroup list, and sent to the House of Commons/Lords libraries. This is expected by the end of 2010.

2.3 A major reason for undertaking the work is to deal with the threat environment, and to define identity from the PSN perspective (Slide 2). This includes answering a series of questions, e.g. 'How can I be sure you are you? [DW: Sydney Bristow is a fictional CIA agent played by Jennifer Garner in the American action television series created by J. J. Abrams which was broadcast on ABC from September 30, 2001 to May 22, 2006. The main theme of the series explores Sydney's obligation to conceal her true career from her friends and family, as she assumes multiple aliases to carry out her missions].

2.4 Threats arise from multiple sources (Slides 3-5), and can derive from authentication, people and processes (where the biggest issues are apathy and complacency - Slide 4), and technology. A number of vulnerabilities are associated with computers and people (Slides 6-7).

2.5 There are 3 sets of data that can establish a fundamental identity – immutable, assigned and related attributes (Slide 8). Immutable attributes are few in number, fixed and unchangeable: biological parents, gender at birth, and date and place of birth (although these may be unknown or recorded incorrectly, by accident or by design). Biometrics can change over time, as can gender. Assigned attributes are acquired from others, while related attributes derive from social and cultural interactions etc. Together they constitute an identity (although individuals can create separate personas if they wish, that do not have to be linked to their real-world identity).

2.6 Establishing identity is a first step – are you really who you claim to be? – that has to be tested by corroboration of claims, while the existence of the identity can be demonstrated through social and historical footprints (Slide 9). The strength of corroborations should be evaluated, along with any anomalies. The next step is to ascertain whether the person claiming that identity is its real owner (Slide 10), including whether or not provenance can be established, and then whether or not the identity is unique (Slide 11). The individual is then locked into the established identity using biometrics and credentials.

2.7 Individuals working for or on behalf of Government will have access to certain information, often including personal information, which can be highly sensitive. Access therefore needs to be controlled through identity management – establishing an employee's (or contractor's) identity with background checks and vetting where necessary for e.g. security clearance (Slide 12). This involves issuing them with credentials, and ensuring that they will be used only by the accredited individual (e.g. by two factor authentication). The HMG IdM system will provide employees with a single identity per protectively marked domain, which can be used to access any Government building, system, service or resource at an appropriate level of security and clearance. The same identity can have different credentials, depending on the role.

2.8 In financial services, much of the security is built around rings of trusted individuals who work together, and different rings may not be permitted to interact with each other. Is access granted according to hierarchy (where seniority correlates with trust) or 'rings' of trust (where seniority is not the key determinant)?

In the IDMS, access is hierarchical, but based on clearances and vetting, not according to seniority.

2.9 Government is trying to achieve a level of trust in each employee and person given access to Government information, in a cost-effective way which involves identifying an individual just once for them to be able to operate where appropriate across-Government. This will replace the current practice of each department issuing its own credentials, through a strategy that allows access across organisational boundaries to multiple systems etc. through a single set of trusted credentials (Slide 13). It involves a federated identity framework with a trusted identity broker and multiple identity providers, so that an individual can be registered with any identity provider that operates through a common trust framework to verify the credentials, without replicating the original registration process.

2.10 Federated IdM principles are listed in Slide 14. An owner organisation does not have to remain so, e.g. if an employee moves to a different department, that will become the owner organisation. Where an employee is working across more than one department, only one will own the identity data, which others will use to verify identity.

2.11 Key processes (Slide 15) comprise a number of steps in registration, enrolment, authentication and authorisation (though the latter is out of scope for now, due to complexity). Once a primary identity is created, it is stored on a database, and the employee will be enrolled in their department's authentication systems. The identity is linked to secondary identifiers (e.g. usernames) and those attributes and credentials necessary for the department's systems (e.g. clearances, groups). Credentials are checked at log on for authentication for access to the system.

2.12 The strategy will deliver a federated identity system based on a common trust framework (Slide 16). This can comprise multiple registration authorities, whose credentials will permit an identity to work with any service provider and be trusted across government for a given security level. Thus where a contractor transfers working from one department to another, the second department will accept the identity established by the first department (and eventually even the credentials issued). Attempts by an individual to register more than once should be detected by the initial registration authority. This will significantly drive down back-office costs.

2.13 Where liability would lie in the event of an error?

HMG is liable - this was why the scope of the strategy is limited at the moment to central Government departments. Government is responsible not just for identifying the error, but also repair and redress. Most departments should be able to meet baseline standards for implementing the scheme, though some will outsource some functions to other departments.

2.14 Each department is implementing this trust system for their own needs but it must be transferable across Government without changing infrastructure and avoiding lots of different agreements between organisations. This involves having a root trust point (Slide 17), and implementing a central service through a root authentication broker (AB). Each department can have its own AB, with a bilateral agreement with the central service, and because each department is signing up to the same bilateral agreement (establishing trust between all departments signed up at that level), transitive trust can be established between any two ABs, because mutual trust exists

between an AB and the root AB. They can therefore contractually and technically trust each other at the same level. Thus any user authenticating to one AB should automatically be trusted by any other AB at that level.

2.15 The Root AB could be Government Gateway, which is a 'hub and spoke' model in which each of the spokes trusts the hub, and therefore also the other spokes. The root AB is divisible into a number of units (Slide 18), key of which is the protocol converter, which is designed to provide conversion between different identity credentials. For example, one department can authenticate using Active Directory to another department's web server that uses SAML, and the AB will authenticate the user through different identity protocols. Thus departments do not have to redesign their systems or invest in new technology.

2.16 Future plans envisage the use of a PKI bridge that will allow shared authentication across other governments and the commercial sector. The Policy Decision Point will enforce access control to protectively marked information etc., based on the clearances of the individual, and the Rules Engine can enforce legislative policy, preventing inappropriate access. AS concluded the presentation with a summary list (Slide 19).

Discussion

2.17 What is the delivery plan?

This is to push ahead with the Employee Access System, standardising as much as possible the registration processes. Delivery will be associated with other projects, such as the PSN and NHS initiatives. As other departments roll out individual IdM strategies, they will come together in the federated scheme. Departments will be under increasing pressure to re-use/adopt each others' identity systems as part of their cost-cutting exercises, which may therefore themselves help advance the strategy. Re-use of registration processes etc. will significantly reduce back-office costs.

2.18 While implementation of the strategy should make things simpler and cheaper, there was the risk of the 'single point of failure' if the system was compromised. However, background counter-crime and fraud checks etc. would be ongoing, which should improve security across the piece. Background audits should expose fraudulent registrations.

2.19 Lifestyle monitoring would be effective in detecting and sharing information of anomalous behaviour – an area in which the financial services sector is very strong and should become easier under the new structures. Currently hacking into the systems of a weak department or organisation can be used to provide a point of access to information. With all departments signed-up to the same stringent checks to the same level, security will be increased while costs will be reduced.

2.20 Anomalies should be picked up by the clearance authorities - this is the role of Policy Decision Point, because the vetting information will be updated and shared at an employee's annual or 5-year renewal.

2.21 Departments will operate different levels of security; how can someone at level 3 trust someone at level 2?

They would not; those at a higher level will be able to trust those at a lower level, but not at higher levels. Those who progress from level 1 to level 3 will be able to trust all others at that level.

3. Review of 3-page draft paper on 'Why world-class Identity Governance is central to UK economic performance' – Piotr Cofta, John Bullard, Philip Virgo

3.1 The 1-page 'flyer' intended for MPs and senior officials has been sent to the EURIM editorial board to check for clarity and political balance. Positive feedback has been received, but also criticisms about the format, which is too crammed, like a 2 pager pretending to be a one-page summary and this is not acceptable. Good layout is vital to communication.

A revised version in larger font and with a diagram has subsequently been re-submitted, in an attempt to accommodate the points above. The latest version of the 3-pager has been circulated to the Identity Governance Group list, in preparation for further discussion today. Work on the more detailed 'long paper' has not progressed beyond the outline 'List of Contents' drafted in August.

3.2 An author of the original 1- and 3-pagers felt that there were some key messages from the industry perspective that should be retained: how might we co-ordinate to achieve balance in the message?

Providing feedback on the revised version of the 3-pager is one route.

3.3 The Subgroup was reminded that the aim of the paper is to focus the reader's interest in the issues. Detailed points and recommendations should be put to one side so that the intended reader finds that the issues need attention, thus providing the political basis for the remit for a heavyweight exercise. The main aim of the flyer is to raise MPs' awareness of the issues; verbal briefings can then be used to get key messages across, e.g. at a PITCOM meeting on identity, to which MPs have been attracted by the flyer.

3.4 Much feedback has been received on the 3-pager, and attempts have been made to incorporate these in the revised version (V09), following detailed discussion in many cases to resolve both particular problems and alternate views without getting bogged down in philosophical discussions about terminology etc. Reference to the education sector has been added, but a question on whether we should propose a solution, e.g. to the problem of too many identities, in the paper has been omitted, other than to suggest that Government collaborate with industry where there are existing, operational, cross-boundary identity governance systems. We aimed not to be prescriptive.

3.5 Other questions arise – is the 3-pager the right vehicle for the 'vision', or should it be more content-rich, or focus more on identity assurance processes or architecture? Or should we stay within the original ToR, and focus on identity governance? Comments are welcome.

3.6 Is the reason why we are doing this sufficiently clear?

The key sentence in the original version was about economy of scale – co-operation between the Government, which is both a large customer and issuer, and industry in general, permits getting to the level or scale of identity assurance where costs decrease dramatically, even below those currently prescribed by the Coalition.

3.7 It was argued that one of the business drivers for change was the level of identity fraud, and adding figures would show that immediate cost savings would be possible through better identity governance – this might be included in the revised 3-pager. It was accepted that the addition of the latest figures would add value and could be re-introduced to the text. The numbers should be the latest figures from the National Fraud Authority, which can be attributed using a footnote.

3.8 Another key driver is the way in which UK and EU regulatory initiatives in this area are causing organisations to transfer their operations to more favourable global locations, leading to massive losses of tax revenue (hence the warning by Baroness Pauline Neville-Jones, who has direct experience of how capital markets work, on the importance of having governance regimes that make the UK a location of choice for internationally trusted operations).

3.9 There is a strong push within Government for all services to be online, including benefits payments from DWP and tax payments to HMRC – which carries significant risk. The most costly risk to Government is the potential for organised crime to defraud DWP through identity theft using electronic attack vectors and malicious code akin to that used against banking, unless effective identity governance structures and counter measures are at the heart of the new systems (security by design, not afterthought). It was accepted that the message on risk in the 3-pager should be strengthened by adding numbers.

3.10 We also need to include the reasons why multinational corporations are moving out of London – which are directly related to the regulatory initiatives and governance regimes within the UK: while the governance regimes of other countries allow global corporations to use world class identity management.

3.11 There are 3 sets of messages to convey: regarding public sector identities, regarding private sector (particularly financial services) identities and regarding the need for Government to exploit the

expertise of financial services based in the UK to produce the best governance regimes in the world (i.e. those which attract rather than repel organisations which take the security of their customers' data seriously). These messages should alert and advise MPs of the questions that need to be asked when the legislation is passing through Parliament.

3.12 Members cautioned against proposing a single solution; the value of the document lay in raising awareness of the problem. If we want a solid exercise that will describe and influence how HMG and the EC are looking at the issues, the next step should be to list the issues that need to be looked at, how and by whom – as opposed to a prescriptive solution.

3.13 In the education sector, there are various national and international routines for identifying students, and linked to these are the issues of immigration and student fraud. This could be seen as an opportunity for a rational way forward – or, if not addressed properly, could lead to big problems consequential to ill-thought out policy. We might consider a supporting paper, outlining what current routines are in operation, and how they might be adapted to help ensure that people from overseas coming to study in the UK are bona fide students, not brought in via 'bucket shop' colleges and imitation universities. This might also address how to ensure they do not bring in family and/or partners until they have earned the right to stay by making a serious contribution to the UK economy This was said to be an area where the devil was in the detail, not the headline objectives.

3.14 The outcome taken from the discussion was that we should replace dry content with examples of current practice, from both DWP and the education sector. On individual voter registration, the driver behind this was very different, and involved getting a complete and accurate register, at relatively low-level security. The EURIM paper on IVR could be cross-linked with this paper (which is focused on security and preventing fraud), since the target audience will include the Parliamentary Resources Unit (a pooled research facility briefing Conservative MPs and Peers), the Parliamentary Labour Party resources unit, and the House of Commons Library staff, all of which are used by MPs' researchers as authoritative sources of information on key topics.

3.15 We also need a paper on the current systems in education, because they are widely used, are very sophisticated for the applications they support, and provide a source of global experience in identity management. We should also bring in the pharmaceutical sector, which includes education and research networks as well as IPR etc., where Adrian Seccombe has volunteered to assist, though these topics are better suited to the longer papers.

5 Date of Next Meeting/AOB

5.1 No time was available for AOB, and no date was set for the next meeting.