



**Minutes of the EURIM Personal Identity Group meeting, 2 June 2005,
1000 – 1200 at 1, The Abbey Garden, Westminster**

Chairman: Jim Lound (Experian); Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. Stephen Upton, as ex-CEO of tScheme, gave a personal view on the topic of secure personal identity. tScheme's original role was to provide digital certificate services. However, PKI-based business models require widespread public uptake of digital certificates in B2B and B2C e-commerce, including e-Government services. Unfortunately take-up of digital certificates was lower than predicted, and although a broader approach addressing the whole concept of electronic identity was postulated under the name of tScheme2, there was no support for change of focus.
2. Although digital certificates have not made the progress required, something akin to tScheme2 is still needed to satisfy the requirements for secure registration, data protection and regulation in a changed scenario where e-Government targets, and now entitlement or ID cards, are the priority. Trust and independent assurance are still vital, and the questions remain – what are the standards, who will assess the risks, and who will assure the information management processes?
3. A meeting on 12 May between EURIM Personal Identity Group officers and senior officials at eGU discussed future co-operation, particularly on issues of identity management, data sharing and trust, including contractual responsibilities and liabilities under the various models. A specific request was made for case studies and experiences of private sector models that could help inform debate in the public sector, and for input from financial services organizations.
4. While overall policy responsibility resides with DCA, the CIO network is responsible for the professional implementation of data sharing across departments. A major aim is to focus e-Government around the citizen through real time processing centres for developing national and local e-Government services. eGU wishes to promote more citizen-centric service models, like NHS Direct (including NHS Direct Online), by removing regulatory, institutional and cultural barriers to attract new providers and to enable existing organisations to join-up service delivery around the citizen.
5. An outline draft of the paper informing Parliamentarians about data sharing issues, remodelled from the paper sent to eGU, is being developed with more content on 'barriers to data sharing' and a focus on overall benefits sharing. **The aim is to have material ready for use in briefing the new intake of MPs before the end of June 2005.**
6. A more detailed paper for eGU on identity relationships will address management and people processes, not just the technology. **A straw man is being drafted for circulation to the group, with the aim of having material ready for the end of July, when the CIO Council is due to agree their core proposals.**
7. A 'straw man' on the ID Cards Bill has been drafted, and an expanded version of this will be circulated to the subgroup for comment. The main aim is to focus on the intentions of the Bill, since this will determine the Group's approach and response. **Major questions include whether or not Home Office will own the NIR, and how the NIR will relate to data sharing with departments.**

1. Introduction

1.1 The purpose of the meeting was to receive a presentation on tScheme from the ex-CEO, Stephen Upton, and to review progress of the data sharing and ID Cards Bill subgroups.

2. Stephen Upton presentation "t-Scheme: a personal view from the ex-Chief Executive"

2.1 *This section should be read in association with the [Powerpoint presentation document that was sent as an attachment to the email that carried this report](#). SU explained that after his departure as CEO, he could not talk about the current tScheme situation, and so he would give a personal view on the topic of secure personal identity.*

2.2 tScheme had originated from a number of commercial service providers who were promoting digital certificates. The business model of one of these, Consignia, required widespread public uptake of digital certificates to assert electronic identity in B2B and B2C e-commerce, and in other areas, possibly extrapolating into e-Government services. However, the business model proved to be flawed as there was a great deal of confusion about who required digital certificates for what purposes.

2.3 A fundamental question arose about the self-regulatory tScheme's role – should it continue to focus on PKI-based business models and provide digital certificate services, or should it address the whole concept of electronic identity, with a broader approach under the name of tScheme2? After a year long discussion, the service provider founder members decided that tScheme had achieved its original objectives, and they did not wish to fund the expansion of tScheme into other areas. tScheme2 thus did not go ahead, and it was at this stage that SU decided to leave tScheme.

2.4 tScheme's focus had remained at the Certificate Policy and Certificate Practice State (CP/CPS) – which defines how the PKI cryptology-based, digital signature service operates. However, tensions existed between the definition-based focus and the Government's stated security levels (0, 1, 2, 3). tScheme did not wish to specify how services should operate, because the market was too new for a legislative approach and wished to self-regulate. Also, Certificate Authority service co-regulation did not fit easily with e-Government service targets (online by 2005), and certificates became seen as part of the problem rather than a solution to service delivery. This dilemma led to the proposal of tScheme2, but internal pressures favoured the original focus.

2.5 Government minimum standards for the verification of identity of citizens wishing to use a Government online service are offered at different levels of security according to the perceived risk (0, minimal; 1, minor; 2, significant; 3, substantial). tScheme helped produce these security levels in 2001 for assessing how a digital certificate should be issued, but not all tScheme commercial services would need to meet the Government standards. The question now is how to issue a form of identity token, although both systems require registration of the individual or organisation. Mutually-supporting documentary, attributed or biographic evidence may be required in face to face or remote registration, dependent on the security level of the desired service.

2.6 A Home Office ID fraud report proposed definitions of identity (attributed, biographic and biometric), with authentication through a two-stage process of validation (does the identity exist?) and verification (does the individual present own the identity claimed?). Evidence for these three sources of real-world identity can be brought together for verification at the point of issue of a token, and once issued, it is difficult then to disprove it. Authenticate of the token depends on checking (e.g. against a central database) that the attributes of the individual correspond to the record on the card, but this in turn raises questions of accuracy and identity management.

2.7 Initially, Government was happy for tScheme to regulate the market, but with the introduction of Government Gateway to regulate online e-Government services, and with intermediaries able to readily create secure electronic identities in an efficient way with processes for access to those services, Government adopted an enabling role. tScheme required assurance that the intermediaries performed identity checks to the same standard, and so it developed a new approval process for electronic identities in which intermediaries were checked against a set of best practice criteria. However, few intermediaries cooperated.

2.8 The role of Government has become more proactive and controlling, with potential recipients of benefits being contacted to increase take-up and the ID cards proposals. Had tScheme2 happened, it would have shown many parallels to these developments in ongoing issues and trends, e.g. service intermediaries being the counterpart of data brokers, tScheme approval translating into a personal identity kite mark, RIPA as consent-enabled data sharing with security overrides etc. (see slides). One

of the major concerns is that all this information is becoming consolidated, with 'shared secrets' becoming joined-up Government (and therefore joined-up secrets).

2.9 There is also the danger that the concept of risk control, which started with security levels 0-3, will evolve into defensive intrusion. The challenges thus remain secure registration, data protection and regulation. The requirements of the original EC directive on e-commerce that regulation be objective, transparent, proportionate and non-discriminatory, which tScheme adopted, are still valid, together with a risk-assessment approach. Although digital certificates have not made the progress required, something akin to tScheme is still needed in a changed scenario where e-Government targets, and now entitlement or ID cards, are the priority. Trust and independent assurance are still vital, and the questions remain – what are the standards, who will assess the risks, and who will assure the information management processes?

Questions

2.10 In the presentation, it was predicted that tScheme was set to revert to its original role – could SU explain what this was in more detail?

SU replied that tScheme was seen by its founder members as bestowing a mark of approval for commercial B2B digital certificate services. A business could, for example, purchase a service to create a certificate so that it could sign transactions with other businesses online, or to authenticate a website. tScheme wishes to retain the ability to approve a service, independently assessed against best practice criteria, and to advertise the service as tScheme-approved even though the digital certificate market had not realised early expectations. Government did not invoke powers under the Electronic Communications Act 2000 to legislate for such services, because tScheme was expected to provide this. The 'sunset' clause in the Act expired in May 2005, without Government legislating, probably because the market in digital certificates had not grown, and tScheme operations were consequently scaled back.

2.11 Is anything being done to persuade intermediaries or service providers of the advantages of tScheme certification?

tScheme is not proactively trying to stimulate the market in digital certificates (though its members may do so individually).

2.12 Does departmental registration with Government Gateway conflict with the pre-issue model of tScheme?

Government had found that the complexity of the registration-certification process threatened the roll-out of secure (above level 1) e-Government services. Secure real-time online registration may help, but awaits an appropriate model. Individual experience had shown that it was relatively easy to sign up for Government Gateway by electronic verification of personal identifier numbers against their records.

2.13 The future of tScheme depended on whether or not there would be a renaissance in digital certificates. This is unlikely in the short term, and the likely outcome is gradual loss of support and eventual obscurity.

3. Report from meeting with eGU and subsequent developments

3.1 The purpose of the meeting on 12 May between EURIM and senior officials at eGU was to discuss broader co-operation, particularly on issues of identity management, data sharing and trust, including contractual responsibilities and liabilities under the various models.

3.2 Discussion included problems of inappropriate data sharing as well as failure to share data in the interests of the individual – how should we define the way forward? Among the actions agreed was that the political framework for the strategy on personal identity should be to find the least-risk route for delivery. **An approved report of the meeting has been circulated in confidence to EURIM Personal Identity group members.**

3.3 There was a specific request for case studies and experiences of private sector models that could help inform debate in the public sector, and for input from financial services organisations, e.g. APACS, LINK, Identrus. Departments and agencies generally do not trust each others' data, systems or even people, and lacked mechanisms for cooperation. EURIM would also provide educational material in the form of briefings for the new intake of MPs.

3.4 While overall policy responsibility resides with DCA, different departments lead on specific services and applications. The CIO network has responsibility for joining-up data sharing across departments, and for the professionalism of implementation.

3.5 Interest was expressed in EURIM-DCA collaboration over the process map, and it was hoped that EURIM will continue to develop this and the exceptions grid, keeping eGU informed of progress. Collaboration between EURIM and DCA is expected to resume in the summer, when it is hoped that eGU will join discussions.

3.6 A major aim is to focus e-Government around the citizen through real time processing centres for developing national and local e-Government services. eGU wished to promote more citizen-centric service models, like NHS Direct (including NHS Direct Online), by removing regulatory, institutional and cultural barriers to attract new providers and to enable existing organisations to join-up their delivery around the citizen.

3.7 DCA is in talks with eGU and is hoping to launch over the summer a cross-departmental project with senior officials to drive forward data sharing across Government departments. This might lead to a degree of ministerial involvement by the autumn of 2005, and it is hoped to organise a workshop on data sharing with key departments, including Cabinet Office, ODPM, DWP and Home Office.

3.8 It was confirmed that DCA has responsibility for data protection as a component part of data sharing, but that DCA has no control over other legislation which introduces barriers or gateways affecting data, and it is unlikely that this will change. Central co-ordination is unlikely to happen, or produce results – departments will continue to control their own legislation. The planned workshop will look at data sharing and the way data is used and controlled to better provide service delivery.

3.9 A potential problem is that many people will refuse to register for Government services because they have no wish to be told what to do by a 'nanny state'. Many people considered that Government interfered too much already in their private lives, and may resist data-sharing initiatives such as 'benefits push'. Data protection with effective oversight should therefore be an essential component of any initiative. **Appropriate and non-intrusive use of data is key to effective data sharing;** anything else is likely to be illegal anyway.

3.10 The approach to data sharing, either by giving explicit consent for each transaction, or by agreeing consent throughout a long-lasting relationship, may affect public acceptance of data sharing. The DCA project would be looking at such approaches, including whether global consent could actually be given, and the extent to which consent could allow data sharing. The extent to which interested private sector parties would be included in the DCA project is as yet undecided.

3.11 There is a distinct difference between having a system that supports enabling data sharing where it might be needed in the future, that doesn't diminish people's control of their own data, and data sharing itself. A system that is prevented technologically from sharing data has many implications, e.g. for the merger between HM Customs and Excise and Inland Revenue and for future data sharing as required by international law. Without legislation to enable data sharing, departmental mergers may be impossible. EURIM needs to express concerns that data control and enabling data sharing are necessary, including at the technical level, for systems to be able to support whatever regulatory decisions about infrastructure and choice are agreed.

3.12 There is also need to recognize that the current public sector position is that departments have no concept of whether the individual has given consent - data sharing is either instructed within known constraints, or it is forbidden. Problems arise when departmental mergers bring together various functions in one person, where data sharing between the former sections is not permitted. A problem for DCA will be to identify and resolve the powers and constraints enshrined in legacy legislation affecting different departments, and transform them into a rational framework.

3.13 A strategic overview of the controls on data sharing is needed to protect both the individual against the state, and the state against rogue individuals.

4. Report from Data Sharing Subgroup

4.1 The purpose of the last meeting of the PI Subgroup on 25 May was to progress the gathering of information for the educational brief on data sharing for Parliamentarians and to assess the format and content of a draft detailed paper on data sharing for eGU.

4.2 An outline draft of the paper intended for informing Parliamentarians on data sharing has been produced, remodelled from the paper sent to eGU. The paper would avoid ambiguous terms like 'financial services model' as used in consent-driven routines, and use new terminology. **The outline would be developed, with more content on 'barriers to data sharing' and a focus on overall benefits sharing. The aim is to have material ready for use in briefing the new intake of MPs before the end of June 2005.**

4.3 It was agreed that we should not proceed with the planned detailed appendices for House of Commons Library in support of the original paper to eGU, but to replace this with a glossary. The more detailed paper for eGU on identity relationships may be of use to those involved in developing an overarching personal identity strategy. Any paper we produce would have to address the management and people processes, not just the technology. **A straw man is being drafted for circulation to the group, with the aim of having material ready for the end of July, when the CIO Council is due to agree their core proposals.**

5. Report from Identity Cards Bill Subgroup

5.1 The reintroduced ID Cards Bill received its first reading in Parliament on 25 May. This had not appeared in the digital Hansard report, but had been announced by the BBC. A well-attended meeting of the subgroup took place on the same day, and considerable material and debate was generated.

5.2 The first task for the subgroup is to compile a list of references to help in drawing up a coherent paper that will provide a summary of the issues for MPs, so that they can take these into account during the drafting process. Members are encouraged to send in relevant references, including the positions of other lobby groups.

5.3 An outline 'straw man' has been drafted, and an expanded version of this in the form of a series of cogent and coherent series of questions of an analysis of the implications of the Bill will be circulated to the subgroup for comment when ready. The main aim is to focus on the intentions of the Bill, since this will determine the Group's approach and response. A key issue here is whether the Bill will be defined by Home Office or will it extend to the public sector? If the latter, questions which arise would include how to handle mixed economy models.

Questions

5.4 Is there a view that the primary legislation is insufficiently detailed to allow an understanding of how it would be implemented?

There is a need to understand the framework in which the Bill sits, because this will generate the questions. Debate will be determined by whether the Bill is designed around Home Office responsibilities, or if it is intended to have a broader scope for identity management. The 'straw man' would provide a useful framework for posing these questions. One of the stated aims of the Bill is to fight crime and terrorism, and as this would involve money-laundering regulations, there is probably a tacit assumption that banks will have access to data for verification purposes. **It was agreed that the paper should make clear that the legislation will assume a cross-over to the private sector.**

5.5 Banks may require the ID Card to be presented by an individual in person, but another question to be addressed is how the ID Card will enable online activity.

5.6 Recent ministerial statements suggested that the initial task would be the establishment of the National Identification Register (NIR) against which the card would be checked. **A major question is whether or not Home Office will own the NIR, and how the NIR will relate to data sharing with other departments. Industry therefore needs to look closely at the political implications of ownership and location of the NIR.**

5.7 Registration of biometric data and the audit record of access requests to the NIR are also a concern. The straw man should therefore address the following issues:

- who has the right of access to biometric data held on the NIR;
- what protection is there against unauthorised joining-up of data (e.g. where multiple identities are used legitimately);
- voluntary versus compulsory data sharing (e.g. enforcement agencies may argue for compulsory access);
- scope creep.

Once the purpose of the Bill is identified, for example through robust definitions, it should be possible to discuss implementation and place limitations on the scope of secondary legislation. This could be achieved by architecture design and choices in the linkages between the ID Card and the NIR.

5.8 Discussions between APACS and the ID Cards Bill team have indicated that cooperation might be possible if the ID card acknowledged banks' charging structures and was built around emv standards. High costs would deter banks from checking against the index. However, the use of emv cards and standards for Government identity should be approached with extreme caution, as they were designed for a different purpose. Although the two cards share certification processes, the emv card is issued by a bank to extend credit and protect against fraud, not to verify entitlement or identity.

5.9 The LSE report 'The Identity Project: an assessment of the UK Identity Cards Bill and its implications' is about to be published. The Report will conclude that the establishment of a secure national identity system has the potential to create significant, though limited, benefits for society, but that the proposals currently being considered by Parliament are neither safe nor appropriate. However, several members of the expert panel are uncomfortable with the way some of the input has appeared in the document, and have not put their name to the report.

5.10 The Interim Report often lacked scientific rigour, e.g. it states in the summary of conclusions that "the technology envisioned for this scheme is, to a large extent, untested and unreliable" – whereas it was difficult to understand how the technology could be deemed unreliable if it had not been tested! Also, many of the cited references were technical press or magazines rather than research sources containing actual details of experiments and results. In contrast, in the case of the EURIM-CESG biometrics workshop, references quoted were listed on the CESG website and pointed to the original research; **this should be included in educational material for new MPs:** <http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=40>

5.11 References in the LSE Interim Report to the policies of other EU members are sketchy. An article by Richard Sarson in a Government online journal covered the other European initiatives and experiences more comprehensively, though it may not yet have been published.

5.12 A distinction should be made between the ID card, and the NIR which can track events in an individual's personal history and can therefore be data-mined and present a threat to privacy. Issues of private access to public data, and the associated issues of ownership and liability have to be resolved. However, obligatory regulatory compliance, e.g. a private firm checking identity against a Government database, should be separated from liability: there would be no liability for reliance on the data, but there would be a duty of care to the individual.

6. Report on Residency Analysis Exercise

6.1 A report of 1 June on Residency Analysis in the Derby area was tabled. One area highlighted is people on the electoral register who have applied for a postal vote but are now deceased. The Registrar provides a list of deaths weekly to the relevant local authority, who can then suppress the poll card but apparently not the postal vote, though it is unknown whether this applies to authorities other than Derby.

6.2 A second issue involved moving to a new address and applying for inclusion in the updated electoral register. Unless the words used are identical with those in the previous entry, the previous entry may actually be duplicated not deleted! There appear to be a number of systematic flaws in current residency registration processes.

6.3 The ODPM consultation 'Towards the National Spatial Address Infrastructure', which aims to provide a national register of all properties, has a deadline of 30 June. The report authors will decide whether or not to contribute when they next meet.

7. Date of Next meeting

7.1 The next meeting of the PI Group will be held on 14 July in Conference Room 'E', 7 Millbank, 0930-1130, when John Bullard of Identrus will be giving a presentation along the lines of 'Identrus: where we are and how we got here'.

[Appendix 1 – Presentation given by Stephen Upton](#)

[Appendix 2 – Residency Analysis Report by Val Beech](#)