



**Summary Report of the EURIM Personal Identity Group meeting, 14 July 2005,
0930 – 1130 at 2 Millbank, Westminster**

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

SUMMARY OF MAIN POINTS

1. John Bullard, Global Ambassador for Identrus, gave an overview of the company in his presentation 'Identrus – where we are and how we got here'. The highly-regulated Identrus community issues and manages identity credentials, runs and maintains a scaleable and secure, real-time identity validation network, and uses common open standards and best practice to enable global e-commerce.
2. ODPM will withdraw from e-Government policy and be replaced by a new 'e-Government Regional Partnership Group' due to take over the ODPM's responsibilities in this area from March 2006. See <http://www.egovmonitor.com/node/1455> for more information. It is likely that the CIO Council announcements of its Information Strategy in November will refer not to IT issues, but rather to organisational and decision-making structures, hopefully including a cross-departmental strategy for identity management.
3. The potential impact on data sharing of the Government Connect (GC) program was discussed. Although the GC program enables rather than requires data sharing, over 100 LAs are already reported as working together on the business account, indicating active collaboration with eGU and the CIO Council. There are concerns that the uniqueID/ authentication structure that is tied to the GC program might also be intrinsically tied to the National ID Card project; the key issue is where the project is likely to fit in the overall IS strategy that the CIO Council will announce in November.
4. A EURIM response to the ODPM consultation on the proposed National Spatial Address Infrastructure had received no acknowledgement (though an article appears at <http://www.egovmonitor.com/node/1822>). An invitation had also been extended for a speaker from ODPM. Points raised included questioning the need for the proposed single database and yet another unique identifier. A copy of the EURIM response is at http://www.eurim.org.uk/activities/pi/NSAI_response.pdf.
5. The current draft of the EURIM paper on data sharing for Parliamentarians incorporates new input from subgroup members, including the section on 'barriers to data sharing'. However, there is a need for compelling, practical examples of successful data sharing in the public sector, including the protocols used in data sharing channels. Members are therefore invited to send details of data sharing schemes to paul_mckeown@uk.ibm.com for inclusion in the draft.
6. Following the imposition of nominal sentences for the unlawful sale of personal information exposed by Operation Glade, the Information Commissioner is planning to use his powers to report to Parliament about the need for meaningful, deterrent penalties.
7. The EURIM ID Cards Bill Subgroup plans to pass to appropriate EURIM observers a list of questions for potential use in the OGC Gateway 1 review of the ID Cards Bill programme.

1. Introduction

1.1 The purpose of the meeting was to receive a presentation by John Bullard (Global Ambassador for Identrus), to consider recent developments and to review material being prepared for MPs.

2. Identrus – ‘where we are and how we got here’ – John Bullard

2.1 This report of the talk should be read in association with the presentation attached to the email that carried this report. JB began by giving an overview of what Identrus is, what it is not, the business drivers around identity management, and what differentiates it from similar organisations.

2.2 As a banker, JB had been involved when Identrus was founded by 8 banks (ABN AMRO Bank, Bank of America, Bankers Trust (since merged with Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank and HypoVereinsbank) in 1999. Identrus was incorporated in the USA and is regulated by the Federal Reserve and the OCC (Office of the Comptroller of the Currency). It built and developed a system based on interoperable, open technology standards with application functionality to allow the use of a wide range of identity credentials.

2.3 Many financial institutions have since joined Identrus' operational, closely regulated, global trust system, helping to define policies for technology, risk management, contracts and business practices to bring certainty and security to business-to-business e-commerce. Participating financial institutions in the Identrus system serve as Identrus Certificate Authorities (CA's) or Registration Authorities (RA's), establishing the identities of their corporate customers and certifying them as trusted trading partners on the Internet. Identrus Certificate Authorities issue unique digital ID's to their customers. These trusted Identrus credentials are backed by a global PKI, making them virtually impossible to falsify. The aim is to manage identity-related issues of the Internet, moving away from VPN to an Internet-based transaction environment.

2.4 Identrus is all about identity, authentication and authorization. The Identrus community issues and manages identity credentials, runs and maintains a scalable and secure, real-time identity validation network, and uses common standards to enable global e-commerce. An alliance with Adobe in 2004 allowed an ability to embed a trusted Identrus credential into an Adobe pdf form – giving users access to an ubiquitous, secure document exchange solution that provides for authentication, non-repudiation etc. (known as ‘SimpleSign’) using the free Adobe Reader). Further developments are anticipated.

2.5 Identrus contractually binds the banks, but has no relationship with the end-customer: business is conducted entirely through member financial institutions, the delivery channels for the credentials. Nevertheless, Identrus runs trusted and protected Internet-based applications, and operates throughout the transactional cycle. In addition to the need for strong authentication, secure e-commerce and regulatory compliance, business drivers include the emerging online trust roles of banks - transactional banks are increasingly providing customer services further up the value chain in the management of operational (not credit or capital) risk in electronic transactional exchange. The complexity of PKI is mitigated by scalability using third party certificate issuance, and frequency of use; the aim is to provide an all-round business solution, not just a banking service.

2.6 Identrus is not just a technological solution; it is a rule set, covering 4 crucial aspects of identity management: policy, legal, operational and technical. A comparison with other operations such as Verisign (which is also used with the Identrus frameworks) shows that Identrus provides a complete, end-to-end IP-based identity management solution, and excels in the registration (KYC - Know Your Customer-based), storage, validation and reliability of identity. Three major operational areas providing opportunities are FI's (Financial Institutions), Government and corporates. Identrus focuses on an identity solution and validation service, but depending on how identity credentials are used, it can be extended into other areas. Recent deals with RosettaNet (the IT e-business standards consortium) and SAFE (the pharmaceutical industry's identity consortium) further extend Identrus' functionality.

2.7 The core messages are:

- The framework and all participating financial institutions are highly regulated by the national regulatory bodies (Identrus itself is regulated by the Federal Reserve and the OCC).
- Strong issuance processes are built upon extensive mandatory KYC procedures used for today's AML (Anti-Money Laundering) regulations.
- Strong and real time validations at the time of use.
- Multiple usages/applications atop the same identity/validation layer.

- International applicability and enforceability of the contractual legal framework; non-repudiation, exactly aligning with the distributed architecture/characteristics of the Internet.
- Identrus is not proprietary (other than the 3,000 page mandatory, contractual rule set), but based on Open Standards and best practice.

Questions and answers

2.8 Identrus' system seems to be based on a single identity, whereas in a networked world an individual may have multiple IDs. How does Identrus authenticate different IDs of the same person?

This would depend on how the individual wished to use the credential. Liability would not be important when borrowing a book from a library, but it would be an issue for transactions requiring strong authentication, and would therefore affect how identity was managed.

2.9 Could Identrus interoperate with other organisations, such as Local Authorities?

An Identrus-based credential could be used in any environment outside the Identrus framework. However, the relying party will not have the benefits or attributes unless it was part of the contractual framework. They can choose to trust the identity, but would lose the liability cover.

3. ODPM withdrawal from e-Government policy

3.1 According to recent press cover, ODPM would be withdrawing from e-Government policy, to be replaced by a new 'e-Government Regional Partnership Group' due to take over the ODPM's responsibilities in this area from March 2006, when funding for the national programmes ceases and the local e-Government programme is to conclude. See <http://www.egovmonitor.com/node/1455> for more information.

3.2 It appeared to be intended to migrate the outputs from the programme to ownership largely within the LA community (of which regional partnerships are part). It is not clear how the programme will develop, but it is expected that there will be 2 representatives from each region and 1 from each e-Government Regional Partnership in the new Group, which will have a rotating chairmanship, initially to be London Connects. Senior representatives from Government may be invited to join the Group (e.g. ODPM, eGU, Government Connect, IDeA). There may be links with the Council of the Chief Information Officer (CIO), but the lack of information for a business case or a formal bid for start-up financial support may suggest that the programme will end with nothing more than a positive spin.

3.3 Experience of the national smart card project has shown that late delivery of funding is unlikely to prevent ODPM from terminating an incomplete project suddenly: rapid results are expected in which LAs use the outputs to their own advantage. The national smart card project was intended to lead to a legal framework with a set of standards etc. available to all LAs. Although some progress was made, it will not yet lead to change, and independent finance is now necessary to continue.

3.4 Any forward plans may form part of the 2006 spending review, which would also include any inputs from the CIO Council's IS strategy. However there appears to be a lack of continuity with current developments; contact with London Connects may be helpful.

3.5 The public statements of Ian Watmore provide the only information we have about CIO Council's IS strategy, what role it will serve and how it will be accountable, although future leaks may indicate areas for which the CIO Council is seeking support. The strategy is likely to include how to incentivise joined-up government between independent departments. This involves organisational, process and cultural issues, and we have no vision of what form this may take (if any). However, the terminology has changed – it is now an Information Systems (not 'Technology') strategy. Significantly, BCS is promoting IT professionalism, in recognition that its members do not have the skills necessary to handle the IS strategy. It is therefore likely that the CIO announcements in November will refer not to IT issues, but rather to organisational and decision-making structures, hopefully including a cross-departmental strategy for identity management.

4. Government Connects

4.1 The following note from a member of the EURIM Personal Identity Group on the potential impact on data sharing of the Government Connect (GC) program was presented to the meeting:

The GC program consists of several elements including:

*Identity Management: GC Registration (using the Government Gateway)
Interoperability: GC Exchange
Email: GC email*

*The basic model is that a Government Gateway (GG) account will be mapped to a CRM (Customer Relationship Management) identifier held locally within the Local Authority. This identifier will then be used to provide the index/link to all records associated with that citizen. So for example GG account AAAA will be mapped to a CRM ID ZZZZ in an LA. That CRM ID, ZZZZ, will be used to link together all associated dealings with that Local Authority. So in a sense the GG will do the *authentication* and the LA will do the *authorisation*. This common CRM ID can hence be used to link together associated records across systems and lead to appropriate data sharing between those records, applications and processes.*

Looking at the bigger model, when one LA wants to communicate with another agency, (for sharing of data), the GG identity (e.g. AAAA) will provide the common identifier that then cross-links into each LA's own systems. LAs do not need to know how other LAs are indexing and holding that same citizen's records: by using a common identifier between LAs (e.g. GG ID AAAA) and their own CRM identifier within each LA (eg. ZZZZ in one LA and 9999 in another), privacy is also assured whilst still allowing appropriate data sharing. This is effectively an extension of the same data sharing model that has been in place around the GG in central government for the last 4+ years.

4.2 This meant that GG and the LA will effectively hold a universal identifier. It is possible to envisage a system (as the GG worked originally) in which the UI is never disclosed to the LA, so that the LA cannot link records to a particular individual. However, where an individual has multiple accounts with the GG, data sharing is frustrated.

4.3 The note expressed what might happen with the national ID Card, where the unique national ID number over a period of time appears on different Government databases and possibly in the private sector. Thus there are concerns that the unique ID/authentication structure that is tied to the Government Connects programme might also be intrinsically tied to the National ID Card project.

4.4 Four relevant documents concern property, business, employee and citizen accounts. Over 100 LAs are already reported as working together on the business account, indicating active collaboration with eGU and the CIO Council, although this is not true for the others. While there appeared to be much enthusiasm, some detected little in the way of clarity for implementation and roll-out, and the expense of the process, together with other operational factors, suggested an uncertain outcome.

4.5 The note describes a method of pointing to the right record associated with the individual; questions remained about how the GG identity was first entered into the LA record, and whether this involved the individual's permission or input. Most of the public sector organisations involved have no concept that permission (or consent) is relevant to personal data management – data entry is either obligatory or forbidden depending on the wording of the relevant statute covering that application. There is no current provision for a citizen to give permission to an LA to check records via another LA.

4.6 The GC program is a common index for Government records that enables, but does not require, data sharing. It appears to change the role of the GG purely into an issuer of ID numbers, and can also be used to connect LAs to Whitehall. A report on the status of the GC project, and an idea of where the project is likely to fit in the overall IS strategy that the CIO Council will announce in November, would be most useful.

4.7 While it did not allow the exchange of ID numbers, the GC project is not a great privacy-enhancing technique, and issues of appropriate data sharing need to be addressed. It would be useful to see a map (that must exist somewhere?) showing where bodies are and are not permitted to share data, and whether restrictions are enforced when used with a single identity in GG: it was possible for an individual to use different identities for transactions with different government departments. **It was agreed to invite a EURIM member to undertake and report further research into the GC project and to convene a Subgroup meeting for this. If not, we should try to find a speaker.**

4.8 Some considered that it may be preferable for the LA identifier to be held in the GG account, rather than vice versa. This would require the LA to request information from the GG whenever they wished to access or share data, and may be the reason why this is not the chosen routine.

5. National Spatial Address Infrastructure (NSAI) Consultation

5.1 A quickly-written EURIM response was sent to the ODPM consultation; no acknowledgement had been received, despite sending a second time. An invitation had also been extended for a speaker from ODPM to address a EURIM meeting. **A copy of the response is attached to the email that carries the summary report of this meeting.** Points raised included questioning the need for the proposed single database and yet another reference number.

5.2 An item of interest was the proposal to identify second and holiday homes – apart from tax purposes, what reason could there be to include this? It was suggested that the NIR would store address information, and assuming integration with the NSAI, there would be a need to identify ownership of second homes etc. This is likely to raise issues of data accuracy and multiple occupancy due to rapid changes of personal circumstances. EURIM also recommended broader private sector input and ownership of the database.

5.3 A list of URLs of current and proposed geographic initiatives would be added to the EURIM personal identity initiatives grid, stating who uses them, and for what purposes. It was pointed out that data accuracy was a serious problem due to residential churn, unreliable updating routines etc., as researched and reported in the EURIM Residency Analysis exercise. We need to know the purpose of the NSAI for the context of any discussion, and for accountability.

6. Report of Data Sharing Subgroup

6.1 The draft briefing on data sharing for Parliamentarians incorporates new input from subgroup members, including the section on 'barriers to data sharing' and now reads reasonably well. However, there are some gaps to fill, and there is a need for practical examples of successful data sharing in the public sector, including the protocols used in data sharing channels. Members are invited to send details of public sector data sharing schemes to paul_mckeown@uk.ibm.com for inclusion in the draft.

6.2 A slight shift in public sector attitudes could be detected; a tentative acceptance that data sharing was possible or even desirable in certain circumstances, was replacing the former perception that it was undesirable, impractical or impossible. Instead, there is now a focus on protocols.

6.3 Most MPs were well aware from their constituency casework of the need for organisations to securely share data, but were also alert to the problems and abuse associated with inappropriate sharing of data. The paper should therefore also inform MPs of ways of overcoming such problems – **Philip Virgo offered to contribute a political perspective to the draft.**

6.4 A more detailed draft paper for eGU was in progress, and had been circulated for comment within the PI subgroup on data sharing. Circulation of the drafts would be widened to the full PI Group once agreed versions had been finalised by the subgroup.

7. AOB

7.1 The launch of the Information Commissioner's report on 13 July is likely to include a reference to Operation Glade and the handing out of nominal sentences to offenders for the misuse and sale of personal information. The IC is planning to use his powers to report to Parliament about the need for meaningful, deterrent penalties. EURIM should comment on this in any briefing for MPs.

7.2 Interest had been expressed in the circumstances of the deletion of information held on Ian Huntley in police records in Humberside, and the policy that led to their deletion. Press cover has suggested that the failure to share data may have had more to do with the motives and actions of certain people responsible for the governance of records, rather than problems with the Data Protection Act. Dave Wright agreed to forward details to DCA.

7.3 The ID Cards Scheme (and in particular the security of the proposed national identity register) is due for assessment in the Gateway 1 stage of the Office of Government Commerce classification of major programmes (the stage at which a formal security evaluation is required). It was agreed that the list of questions being compiled in the draft paper on the ID Cards Bill for MPs be modified and passed to EURIM observers for potential use in the Gateway 1 review, if time allows.

8. Date of next meeting

8.1 The date of the next meeting is to be decided in the light of developments.