

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



**Draft report of the EURIM Personal Identity Group meeting, 27 January 2006,
1000 – 1200 in the Macmillan Room, Portcullis House, Westminster**

Chairman: Stephen Darvill (LogicaCMG); Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The Government Connect Programme supports the Transformational Government strategy; its' vision is to provide and promote a secure and sustainable framework that will deliver public sector service improvement with personalised, joined-up services for citizens. It is hoped that the GC product set will be available for take-up in April 2006.
2. The GCP can be seen as a toolkit and set of infrastructure products that can be merged into shared services and a common infrastructure, building on GG and GSI (Government Secure Intranet). A key target is to bring all English local authorities into membership by the end of 2008 and accelerate their provision of online services to citizens, business and intermediaries.
3. Government Gateway has a track record of 99.5% uptime over the last 72 months of operation, with ~ 9 million active enrolments and 102 Government enabled services. A 'White label' interface will facilitate access to GG, via GC Register, which enables a consistent approach to online registration and enrolment and is based on the development of T0 and T1 levels of secure authentication. There will be a single sign on across websites.
4. A balance has to be found between usability and security: vigilance, awareness and training by all stakeholders must form part of the solution, which must also be tested and improved in the light of real-life experience. Feedback and comment from EURIM members on any and all aspects of the GC programme is most welcome, including registration, authentication, infrastructure and standards-setting, by email (steve.lawrence@cabinet-office.x.gsi.gov.uk).
5. It is not clear how EURIM could contribute to the ID cards debate without the engagement of Government. Plans are ongoing to meet with DTI and Home Office on the costings of major elements of the ID Cards scheme, and on interdepartmental cooperation, but specific dates have yet to be proposed.
6. The circulated draft EURIM response to the Transformational Government consultation produced feedback for inclusion in the final response. This includes comment on the holistic approach to identity converging towards the ubiquitous use of biometrics in ID cards, and the practical and legal issues of making wider use of the NINO to index citizen records. Members with experience of possible alternative models (e.g. APACS, LINK, Experian and Identrus) are therefore encouraged to provide examples that we can forward to Cabinet Office for consideration.
7. Members are asked to continue to send any further examples they have of successful data sharing, and good practice in security (especially authentication), standards and governance of sharing routines, to Dave Wright (davywright2@ntlworld.com) for addition to the EURIM data sharing grid. The grid is an important resource for those engaged in implementation of the Transformational Government strategy.

1. Welcome and Introduction

1.1 Members and observers were welcomed to the meeting, with introductions around the table.

2. Government Connect Overview – Steve Lawrence

2.1 SL gave an overview of the content of his talk on the Government Connect Programme (GCP), including updates on progress, governance, business context, the pricing model, sustainability and benefits. The main aims were to:

- provide an update on how Government Gateway (GG) will help to power the GCP;
- describe what Government Connect (GC) is hoping to achieve for local authorities (LAs).

The [presentation](#) should be read in conjunction with the notes below.

2.2 GC is geared to supporting the Transformational Government strategy; its' vision is to provide and promote a secure and sustainable framework that will deliver public sector service improvement with personalised, joined-up services for citizens.

2.3 The GCP can be seen as a toolkit and set of infrastructure products that can be merged into shared services and a common infrastructure, building on GG and GSI (Government Secure Intranet). GG was 5 years old on 26 January, and has attracted ~ £90 m funding until 31st March 2011 from Government Organisations (GGSS Strategic Investors), which should provide reassurance to the GCP's customer base (initially the English LA's).

2.4 A key target of GCP is to bring all English LA's into membership by the end of 2008 and accelerate their provision of online services to citizens, business and intermediaries. It is hoped that the GC product set will be available for take-up in April 2006. GC is holding Phase 2 of its implementation on 9-10 February (in Bolton and London) to discuss readiness, support and training; DWP will describe how they expect to add value to the LA investment by potentially using the infrastructure for LA to DWP information flows. SL is accountable for take-up and cost recovery, with a target of 200 enrolled LAs by the end of the next financial year.

2.5 GC is a local government-owned programme, chaired by Steve Gallagher (ex-CEO of Knowsley Council) with stakeholder representation from across the public sector. Funding, currently largely from ODPM, will become subscription-based as GCP is rolled out. Roy Marshall (ODPM) has now taken over from Julian Bowrey as SRO.

2.6 There is ongoing work on registration, authentication, infrastructure and standards-setting. GC has strategic objectives that include engagement with central Government, including DWP and DfES, based on the need for secure transfer of data between LAs, their partner agencies and the rest of Government connected to this infrastructure.

2.7 The impact of the Gershon agenda and the Comprehensive Performance Assessment (CPA), which gives a measure of LA effectiveness of service delivery, provide challenging targets, with a requirement for 24/7 availability and multiple channels of access. In particular, there is an aspiration that a customer should have to provide personal details to Government just once in order to register for a number of services and use multiple points of access. Warwickshire, for example, record 70% of their daily website accesses out of business hours, and have estimated that they save ~£700,000/a by providing 24/7 online access to their website. There is clearly scope for much greater savings through secure, trusted customer-centred, online services across the public sector.

2.8 The two components of the GCP are GC Core and GC Plus (see Slide 21 of presentation). GC will re-use the registration and enrolment sign-up product that has been provided via the Businesslink.gov.uk website from the DTI's Small Business Service. Within GC Core, the GC Register enables a consistent approach to online registration and enrolment, based on GG. GC is working on developing smart authentication online using one user ID and password; thus GC Exchange provides a stable platform for the secure transfer of structured data between LAs (effectively an XML relay), while GC Mail enables secure email between LAs and others.

2.9 GC Plus is designed to make available a wide range of additional components to the developing 'community of trust', exploiting the same or similar products, infrastructure and standards. Two components available now are:

GC Pay - providing an e-payments solution

GC Alert - extending the options for customer contact.

2.10 GG has a track record of 99.5% uptime over the last 72 months of operation, with ~ 9 million active enrolments and 102 Government enabled services. A 'White label' interface will facilitate access to GG, building on the DTI's SBS approach, via GC Register together with a single sign on across websites without the need to log-on again. GC Register is based on the development of T0 and T1 levels of secure authentication (from t-Scheme and HMG standards) backed up perhaps by an LA identity number.

2.11 Anyone interested in testing standard tokens from the GC interoperability lab should inform him of their findings (<http://starhall.pwp.blueyonder.co.uk/SSOinterop>). Success with security and standards will ensure the benefit of commonality and a consistent user experience. The GCSx (Mail, Exchange & Connectivity) interfaces with GSI and will use best practice principles to provide a secure, managed intranet for local government, built over a private network, allowing data to be exchanged without using the Internet. GSI, NHS and CJIT users will be able to identify trusted users within Councils so they can exchange emails. GCSx will also provide a messaging hub for structured XML content routing (e.g. of secure documents and forms) both between LAs and with the rest of Government.

2.12 It is estimated that the running costs for LAs will range from ~ £5000/a to ~ £120,000/a, depending on their size, degree of readiness (e.g. of products and development, back office with front office), and appetite for risk. As an example, Rotherham Council is running at £65,000/a. There are many benefits and efficiency gains, as listed in the slide set.

2.13 GC has been built to provide and promote a secure and sustainable framework, underpinned by a concordat between Government Connect, ODPM and Cabinet Office. This enables local government and its partners across the public sector to deliver service improvement and personalised, joined-up services to customers. Through CO, GG has secured ~ £90 million over the next 5 years from DWP, HMRC and ODPM.

2.14 Over 335 councils in England have registered their interest in GC so far; attempts will be made to recruit the remaining ~50. February 9-10 will be a 'litmus test' for when GC goes 'live' with GC-Register (for T1 authentication) and GC-Mail for 'early adopters' in April 2006. SL concluded by inviting questions, and by expressing his wish for future feedback and comment from EURIM members on any and all aspects of the GC programme, including registration, authentication, infrastructure and standards-setting, by email (steve.lawrence@cabinet-office.x.gsi.gov.uk).

Questions and Answers

2.15 In a low-security environment (T0, T1), would there be any way of sharing information on false identities?

Security levels at present were citizen-facing aspects of the GC Register; back-office aspects would be restricted level. Where work is shared with CO, a special interest group has been set up with t-Scheme, CSIA, CESA and others, which will discuss the conditions under which identity information can be shared. Feedback from EURIM members would be helpful here. Although there is no plan for information sharing now in place, the work programmes may provide appropriate opportunities.

2.16 How does GC respond to fears of identity theft?

Moral and ethical imperatives demand that Government provide a heightened profile of the problem, and this should include security and awareness training. Online applications should be made only with appropriate computer security and vigilance, including anti-virus and firewalls. Identity theft and security aspects would be looked at by the special interest group, together with data protection and sharing.

2.17 How would higher-level authentication for sensitive transactions (requiring e.g. token, smart card etc.) be paid for?

LAs had the opportunity for checking applicants' personal documents in face-to-face interviews during the registration process. If t-Scheme approved an LA registration process, there is a possibility that the LA could absorb the cost of digital certificates (which previously had proven too expensive for general

roll-out) or tokens, at fraction of the current cost. The validity of this approach is being investigated as part of the GCP.

2.18 In view of the answer to 2.17 above, why should one LA bear the registration costs for others?

There are policy aspects to a solution, perhaps involving making the 'invest to save' case to Treasury for funding, with LAs picking up the marginal cost of issuing a digital certificate when pooled with the costs of ID cards, smart cards, tokens, PKI etc. Nothing formal has been agreed, but these ideas may provide the starting point for an agreement.

2.19 Individual LAs might start up their own individual schemes, entailing high set up, registration and enrolment costs but not providing interoperability: can GC persuade LAs to join or await the results of pilot schemes to avoid expense and duplication?

GC might perform an 'intelligent customer' role, and encourage LAs to recognise the power of the GC infrastructure, and use it. All LAs are connected to the GCSx, and by working with standards, individual initiatives (e.g. local smart cards etc.) could be replicated across the network. Although LAs make their own decisions, a relevant question they should ask themselves in this context is why they should not use the national programme.

LAs might be encouraged to sell their own tested products to others, perhaps through a partnership approach (carrying a financial discount), with financial modelling to support it.

2.20 How would GC manage the fine balance between promoting awareness of identity theft and its impact on usage.

A balance has to be found between usability and security, and will be largely dependent on who uses the services and how often. There are no magic solutions; vigilance, awareness and training by all stakeholders must form part of the solution, which must also be tested and improved in the light of real-life experience.

2.21 With regard to identity theft, a useful service provided by CRAs is notification to the account holder of any enquiry to their record: this may be a first indication of an attempt at identity fraud or theft. Is this an area in which industry might help GC with solutions?

The representation of organisations like APACS as members of the GC special interest group will help. Feedback had already been received in the form of advice and information from banks with experience of using PKI and tokens etc.

2.22 Are not LAs increasingly unable to determine their own policies and directions, being subject to a number of centrally-imposed controls?

Gaining the support of LAs can be achieved through demonstrating value to the citizen, and the potential savings to the LA in the form of case studies (e.g. Warwickshire made savings of £700,000 last year, with improved service delivery).

2.23 The use of a unique LA number, and also service activation in identity management have been mentioned, but these do not sit well together. Where would the unique LA number be held, and who would hold it?

Local identity management solutions exist, as offered by e.g. Oracle and IBM. The unique LA number would be held by the LA. Reference Numbers will effectively relate to all other services in the LA. This LARN would then in turn be linked to the GG UserID and Password which enables access to [102] other Government Services. The most important information is the credential identifier between GG and the LA reference number, and this would entail some sort of storage system to host it such as a CRM system or Local Identity Management System (IMS). A customer would enter an LA website on Council Tax. If the LA adds leisure bookings online and relates this to the same locally-held IMS/CRM the customer accesses the new service once the LA has enabled the access via the IMS/CRM.

Once you are a registered user there will be no need to remember different user IDs and passwords for each of the government services you use, which are enabled by GG. One Single User ID, One

Password and you will have access to all the government services that you have enrolled to use, via GG.

2.24 According to one report, only 46% of UK Internet users would use online government services – what reasons were proffered by the remaining 54% for not wanting to use online services, and how might this reflect on social exclusion? Research suggests that the ‘digital divide’ would persist for some time, with ~ 30% of the population not directly accessing online services by 2025.

Lack of take-up could be attributed to a range of issues, including lack of trust in online services (exemplified by the recent identity theft of individuals in DWP etc.), apathy (how does it relate to me), lack of interest or motivation, and a low level of confidence in using the Internet. There are still many people who prefer face to face transactions.

However, quick wins possible through online transactions should not be jeopardized, and people wanting to use GC should be encouraged to do so. Case studies might be helpful in persuading people of the benefits, while further work with intermediaries e.g. Citizens’ Advice will be necessary to spread the net more widely. GC is in similar discussions with other potential intermediaries like Barnardo’s, trying to find ways of extending access, including by consent routines.

2.25 Increases in take-up should be benchmarked against levels of activity at different times to give a better idea of progress, rather than using overall take-up in the general population. Does GC have any statistics on current customer interactions so as to provide information on channel migration take-up?

Warwickshire LA had tried to predict what would happen if their website went down. When asked, 2% - 5% of customers interviewed said they would contact the LA in person, 15% would telephone in, and 1% - 2% said they would write in. The LA estimated that over 1 year, the additional cost of dealing with customers in other ways would be > £700,000. Examples of innovative uses of technology in bridging the digital divide include information sharing, community support websites, alerts and advice sent by mobile phone – GC was already in active discussions with the NHS about the latter, using the mobile phone as a token.

2.26 SL was thanked for his presentation and frank responses to questions. EURIM looked forward to working with SL and offering any help it could it helping to ensure the success of the GCP. SL stated that any feedback from the accompanying slide set would be most welcome.

3. Identity Cards Bill Subgroup report

3.1 Although events have been moving quickly, it is not clear how EURIM could contribute without the engagement of Government. Plans are ongoing to meet with DTI, but so far they have not proposed specific dates, while Home Office have yet to go public on their next round of meetings, and there is a need to consider how to proceed.

3.2 More information was needed from Home Office, e.g. on what they propose as the business model, liability etc. Debate was also needed on the costings of major elements of the ID Cards scheme.

3.3 At the EURIM-ID-entity joint meeting of 12 January, the ID-entity group of suppliers were questioned by Parliamentarians and their researchers on a number of the technical issues involved with ID cards systems. The general feedback suggested that the meeting had been worthwhile. It was accepted by many that the enabling technology was not an issue – what was unusual for the UK ID cards scheme was bringing all the technologies together, with the additional difficulty of getting the different government departments to cooperate with each other in an integrative scheme.

3.4 Another issue raised by researchers was how to get realistic costings when companies are unable to give detailed answers, due to confidentiality, lack of available information on the requirement and other issues. A potentially bigger problem is how to get departments to say what they are willing to pay from their budgets for particular services: this may require ministerial cover for civil servants to engage in more detailed, private discussions. EURIM is planning a meeting with Home Office with these objectives in mind.

4. Response to Transformational Government consultation

4.1 The draft EURIM response to the Transformational Government (TG) consultation had been circulated, the deadline for feedback being today (some comments had been passed directly to eGU).

Concerns raised for inclusion in the final EURIM response included the holistic approach to identity converging towards the ubiquitous use of biometrics in ID cards, and the practical and legal issues of making wider use of the NINO to index citizen records.

4.2 Given that technology is only a minor part of the problem, we need to explore what are the organisational, responsibility and other 'people' issues around alternatives that might be used (e.g. federation). **It would be useful therefore if PI Group members (e.g. APACS, LINK, Experian and Identrus) could provide material on experience with possible alternatives, so that this could be forwarded to Cabinet Office for consideration.**

4.3 One observer had noted that many new Government IT systems failed because staff training was inadequate or non-existent. Most proposals did not include realistic estimates for staff training for new systems, which might well cost more than the hardware and software added together, There was a recommendation therefore that this should be a mandatory part of every Gateway review.

4.4 Another issue is to resolve security issues, including penalties for abuse, (e.g. in departments or suppliers' organisations), including by people with 'authorised access'. The Police and Justice Bill now before Parliament will increase the penalty for CMA section 1 (hacking) offences from six months to five years and will increase the penalty for CMA section 3 offences from 5 years to 10 years. The Bill will also add a new offence relating to supplying articles (e.g. hacking tools) for committing CMA offences. We shall undertake enquiries to see if this offers a way forward in this area. However, there was no sign yet of legislation to increase the penalties under the DPA in the light of the non-custodial sentences for those convicted of selling data from criminal and medical records after Operation Glade.

4.5 Regarding social inclusion and citizen feedback, it would be helpful for CAB to look at the specific points of social inclusion and intermediaries in the EURIM response to the TG consultation and to comment on how expertise in the voluntary sector might be better used.

4.6 PV noted that only 3 attendees were from organisations planning to submit their own response to TG (BCS, Nortel Networks and Notaries), although CAB may also respond directly. PV therefore invited comments for consideration for inclusion in the EURIM response, to be submitted before the 3 February deadline.

4.7 The EURIM TG response will also now include cross-links to the Royal Academy of Engineering on complex systems. US data indicates that $\leq 34\%$ of large IT systems succeed (c.f. 16% in UK), and success is strongly linked to the 'structured evolution' approach (phased implementation), as opposed to 'big bang'.

4.8 The EURIM response seems to focus on barriers to shared services rather than to public take-up, which the planned Notaries response will do – would EURIM like to comment?

PV replied that the EURIM TG response only used material that could be referenced to work previously undertaken by EURIM, although it alludes to management and information assurance issues of individual registration and the vulnerabilities associated with checking subsequent changes. There are also issues with a holistic approach, where identity can be hijacked by attacking a single location: this has been covered in the IMIS submission. Many IMIS members operate in countries that run ID cards, where they are useful as a one-stop-shop access to low value public services, but afford little or no protection against ID theft and fraud.

4.9 With security levels T0 and T1, good routines for detecting fraudulent approaches to the individual's account can be effective, but where an identity is stolen and used to defraud the owner in a system that is highly integrated (e.g. as in Sweden), it is extremely difficult for the true owner to recover their identity. The role of the notaries is in underwriting identity and accepting liability (currently, the Notaries accept liability of $> \text{£}1$ million), whereas most organisations look to avoid liability. PV looked forward to reading the Notaries' response to the TG consultation.

4.10 A new project is planned by the Notaries which recognizes the importance of management and people issues, and for which assistance from EURIM and its members would be helpful. It would enhance the chances of success if the proposals in any new project were compatible with e.g. TWIST and Identrus systems, which currently are setting new standards. Discussions would continue 'off-line'.

5. Grid of data sharing exercises

5.1 The data sharing grid now has >30 entries, with many additional links within the documents referenced, and hopefully now forms a useful database for use in the drive to raise the political pressure to help ensure implementation of the TG agenda.

5.2 An exercise to dig deeper into LA sources has so far not produced additional examples for the grid.

5.3 It is important to have pointers to as many projects as possible in order to alert those responsible for delivering the TG programme to what is already happening, and to join up and build on the best. Members are asked to continue to send any further examples they encounter of the benefits of sharing and of good practice in security (especially authentication), standards and governance to Dave Wright (davywright2@ntlworld.com) for addition to the grid.

6. AOB

6.1 A replacement chair of the Data Sharing Subgroup was still needed, following the resignation of Paul McKeown. There is a role for the Subgroup in advertising widely examples of the benefits of data sharing, and finding innovative ways of exerting sustained political pressure for joining-up, addressing the issues of management and governance (rather than technology). It was agreed to progress this at the EURIM Council meeting on 31 January.

6.2 The issue of convergence between the national ID card and a single identifier such as NINO would be addressed in a note planned by certain group members and observers.

7. Date of next meeting

7.1 Future meetings of the PI Group are themed, and set for:

- 3 February – David Myers on the subject of shared services
- 23 February – Iain Bell on data sharing and the DWP Longitudinal Study