



Summary Report of the EURIM Personal Identity Group meeting held on 13 December 2007, 1030-1230 hours in Committee Room 12, Westminster Palace

Chair: Stephen Darvill (LogicaCMG)
Rapporteur: Dave Wright (EURIM)

Any details discussed in this meeting are 'off the record' and confidential. The account of the talk given by Richard Trevorah should be read in association with the accompanying Powerpoint file.

1. Introduction

1.1 Stephen Darvill opened the meeting and welcomed Richard Trevorah of tScheme, who had kindly agreed to give a talk to the Group entitled 'tScheme, from PKI to Information Assurance'.

2. tScheme, from PKI to Information Assurance – Richard Trevorah

2.1 RT explained that tScheme is a not-for-profit membership organisation chartered by the Electronic Communications Act 2000. It was established after its founder members were successful in persuading HM Government that tScheme was an appropriate voluntary accreditation scheme able to deliver to the standards required, and there was therefore no need to invoke direct regulation under an EC Directive on the electronic trust services market (Slide 2). After 5 years of successful operation by tScheme, Government powers were deemed unnecessary and its powers under the legislation were allowed to lapse.

2.2 tScheme operates via 4 interested parties (Slide 3): members, assessors (who make an assessment against tScheme criteria), trusted service providers (seeking approval under the scheme) and accreditation bodies (authoritative bodies that conduct and administer an Accreditation system and grants Accreditation to Certification Bodies i.e. the assessors. In the UK, this is UKAS).

2.3 Funding is through an annual membership fee; assessors pay a licence fee per assessment; service providers pay an approval fee and an ongoing licence fee. Members and assessors contribute to the committees that determine the best-practice guidelines, and may involve external experts.

2.4 The original work was done under the guidance of the (then) DTI, who suggested utilisation of existing certification schemes, and tScheme was established as a BS 7799 sector scheme (now ISO 27000); assessors are accredited by UKAS as being competent to certify Information Security Management Systems plus tScheme-specific capabilities. The tScheme, best-practice guidelines are organised into Approval profiles, which assure that the service provider is properly established and resourced and that the user receives the service expected (Slide 4).

2.5 The approval profiles do not, however, test that the service is fit for any particular purpose, or for interoperability (Slide 5). The description has to define what the service is in auditable terms, and this is what tScheme measures. Thus users and relying parties themselves can then make informed decisions as to whether the service is fit-for-purpose.

2.6 The approvals process is schematically summarised in Slide 6. tScheme has an agreement with the accreditation body to include the tScheme-specific capabilities when accrediting the assessors who want to be allowed to carry out an approval against the tScheme Profiles. tScheme then has a contract with recognised assessors who have been accredited as being familiar with tScheme processes and have demonstrated that they are competent.

2.7 The assessors, in turn, enter into a contract with the Trust Service Providers to carry out the audit; the information revealed to the assessors being confidential - a report is issued to the TSP stating simply whether or not tScheme requirements have been met, which they then submit to tScheme. If the report is acceptable, tScheme grants an approval.

2.8 Current tScheme status is shown Slide 7; there are 4 service providers (RBS, Trustis, BT and Equifax), approved in 2002-3. After a period of little activity, 3 new services have become 'registered applicants' and are now working toward approval namely Registers of Scotland, BT Global Services and the NHS Root. Also, there are currently 9 different approval profiles, with > 300 individually-tagged criteria (see http://www.tscheme.org/profiles/index_digest3.html).

2.9 The growth of PKI is continuing, particularly since the concept of a PKI bridge has been developed (Slide 8). In the US, the federal bridge provided a shared trust infrastructure between various state departments; similarly aerospace & defence and higher education bodies etc. have established their own bridges, thus making it easier for them to do business securely and electronically with each other as well as the US Government. However, the sole reason for the development of these bridges is to provide authentication credentials: a single identity credential that can be trusted by partners, suppliers and customers alike - confirming that identity assurance is here driving the take-up of PKI.

2.10 Identity assurance has many facets; it can be developed as a technologist's view (Slides 9 and 10), but a more common view (Slides 11-13) shows various aspects of identity that need to be managed. Management is a process, comprising a number of steps, and ISO 27000 is designed to ensure that such a process is based on a risk analysis and is properly carried out so that an appropriate service is provided. This then provides a basis for the trust in the system.

2.11 However, there are a number of issues around ensuring that the process is enforced, and that credentials will be revoked when necessary. Credentials must also relate to different security levels of access, and a 'trust life-cycle' (Slide 14) can be established, allowing the identity and access rights of an individual to be known dynamically.

2.12 The only way to have trust is via an underlying audit regime conferring an appropriate level of assurance that the process is being followed, and will continue to be followed, as tScheme assures. Authentication itself is not the same as trust: the credential will only enable you to know who the person is, but "knowing the name of the crook does not make him honest" (Slides 15, 16).

2.13 Trust can thus be established via a trusted identity scheme (Slides 17-18) such as tScheme, which is an existing mechanism for providing trust and confidence to Her Majesty's Government as well as UK citizens and businesses. Re-use of appropriate existing national and international standards helps ensure a focussed solution and provides implicit updating to current versions. It is also a flexible solution - after developing the original 8 PKI-related profiles, tScheme developed an identity profile with the Cabinet Office in 2003, in association with the roll-out of Government Gateway (GG).

2.14 Some of the online banks were approached about their assured users - why not allow them to use their credentials to access the GG? The banks were prepared to agree - for a fee, but Cabinet Office demurred, saying that as they provided the service, payments should be made to them! The result was stalemate, but at least it resulted in the development of a technology-neutral version of a PKI registration profile, which can be viewed as the first step from PKI to Identity Assurance, we just didn't think in those terms back then!

2.15 Examples of the kind of information flows in a credential validation service, showing how an identity service provider relates to a user and the relying party, appear in slides 19-21.

2.16 GG is already requiring that, for access via any outsourced scheme, the Identity Provider has to be tScheme accredited (Slide 22).

2.17 The role of the assessors is critical to tScheme, and, by using Certification Bodies that are accredited by UKAS, an international yardstick applies so that tScheme can be assured of the quality of their assessment (Slides 23-24). Although tScheme is a national scheme, because UKAS is a signatory to a multilateral agreement under the international accreditation forum, assured accreditation

can be carried out in any part of the world if it is performed by an assessor who is suitably accredited, as embodied in the ISO 27000 suite of standards. For more information, go to <http://www.tscheme.org/index.html>

3. Discussion

3.1 Can you say something about tScheme audits, and the resemblance of some profiles to architectures – where are they from?

tScheme operates as an audit regime: it enters into agreements with the auditors and tells them what to audit against. The profiles are developed by the tScheme expert committee; in the case of PKI, this included those involved at that time – IBM, Inland Revenue, Microsoft, Royal Mail, HM Customs & Excise etc. – who determined the criteria that should be audited against in order to assure to the appropriate level of confidence.

3.2 When tScheme received a request from GG for a credential validation service, GG was one of the expert bodies invited to determine the criteria to be audited against. The actual technologies and architectures employed in providing the service are determined by the provider. tScheme is also in discussions about a model for Liberty Alliance via its identity assurance expert group, and is working with the federal PKI credential committee on how to extend their audit regime into Europe. It is the principles that tScheme is supporting, not the protocols or architectures as such.

3.3 How many of those using tScheme are very high response services, e.g. where financial transactions must be rapidly done and secure?

The tScheme-approved Trustis service is relevant here as they provide outsourced PKI services; as well as the new BT Service providing a PKI for secure communications links between customers and the CREST Settlement system operated by CrestCo.

3.4 When looking at the processes in an organisation, how deeply does tScheme check that staff are thoroughly vetted and trained?

This falls mostly into the ISO 27000 area of audit, where suitability of personnel is a crucial factor; the assessors would thus check against compliance with ISO 27000 in great detail. tScheme itself looks only at the service delivery elements.

3.5 It was pointed out that this means looking at the assessor's report. Such detailed investigation would involve looking at the scope of the tScheme ISO certifications, rather than any service tScheme provided. Cabinet Office some while ago had required all government departments to be ISO 27001 compliant (with an independent assessment of compliance). tScheme had encountered no problems so far. It was agreed that this was a major point of weakness, since compliance and even 'adequate' practice was an issue.

In the work tScheme was doing with the DCSF, Contact Point were looking thoroughly at employee authentication including for agency and contract staff, because they do recognise this as a major potential weakness.

3.6 Is anyone responsible for guaranteeing the effectiveness of the schemes?

With regard to the strength of credentials, Cabinet Office has produced a number of framework and architectural documents prescribing all levels of assurance. Equifax are audited not only against tScheme profiles, but also against HMG minimum verification requirements for the individual. So if they say they are producing a Level 2 credential, there is confidence in what that means in terms of the Government document; it is up to the relying party to decide whether they need Level 2 or 3; tScheme provides a yardstick giving confidence in the level requested or used.

3.7 Does this not infer that tScheme is providing the rule book, but no-one is ensuring that the service is regulated according to the right rules?

tScheme polices the contract, and ensures that the service does what it purports to do, but it does not set the market.

3.8 At a workshop yesterday in Brussels on interoperability, despite defining a number of standards, guidelines, agreements and recommendations, there was a general feeling that the Directive left key questions unanswered, including an understanding of what combination will achieve the desired results. Certain Articles require member states to fulfil the requirements of the Directive, but do not specify or advise how this should be done. Therefore the EC should say, 'in order to fulfil the requirements of the Directive, you should demonstrate compliance with CWA14167 etc'. Clarity is needed in establishing how to move from the Directive into the market place.

Article 3.7 allowed member states to define their own security requirements for a public service, but some were effectively adding requirements that had nothing to do with public safety and security but appeared to be designed to protect their national markets, and none of the e-government services had providers from outside the member state providing certificates for credentials or support services. It was felt that the Commission should look more carefully at member states' responses.

3.9 How does the UK compare with EU good practice.

There is no EU-wide good practice! However, the UK approach was seen not to be restrictive, and of good quality, although the number of services involved was relatively small. However, unlike the UK, many EU citizens enjoyed the benefits of smart-card access to services.

4. Report from 'brainstorming' workshop on data sharing

4.1 A small team of EURIM members held a workshop on 9 November, with the objective of identifying 'gaps' in current activities across the public and private sectors in Personal Identity and Data Sharing and to highlight those activities where EURIM is uniquely positioned to play a leading role. A list of those 'gap' items, identified in a separate document, is open for discussion here; members are invited to comment and say whether they are prepared to supply resource to follow up. The items will then be circulated to the wider EURIM membership for input.

The notes below should be read in conjunction with the 'Brainstorming meeting' document attached to the email carrying the minutes of this meeting.

4.2 Points 1 & 2 can be taken together, the summary suggestions for action are:

(i) EURIM should facilitate debates with influential parliamentarians to help them develop a clear vision.

(ii) Government must begin to reverse the downward spiral of mutual distrust; EURIM should campaign for a change in government approach.

There was some discussion as to whether these tasks might better be undertaken by BCS or EURIM, and speculation as to whether this might have been picked up by the Crosby review. In the meantime, it was felt that neither issue at present should be taken up by EURIM.

4.3 Point 3.

(iii) EURIM should provide ideas to help Government make it easy for citizens to comply with regulations and to access entitlements; Government must also be able easily to identify non-compliance by citizens.

It was noted that MPs seem to be picking this up, and professional bodies might be best advised to get together to influence the regulatory agenda.

4.4 Point 4

(iv) EURIM should educate parliamentarians on the need for them to focus on how citizens/citizen groups should be serviced and to ensure that any enabling legislation provides access to the right data to perform the service. EURIM should also help government by identifying costs of NOT managing personal identity and sharing essential data to provide citizen services.

Data sharing was a very live issue given recent losses by Government departments and agencies. At an Intellect-IS meeting yesterday, there was confusion as to who should be taking the lead. It was noted that further business is unlikely until the issues are resolved; if politicians want to look at this, EURIM should help.

4.5 Point 5

(v) For years in the private sector the rule has been ‘Simplify first, then automate’. EURIM should campaign to persuade government to follow that rule for success.

It was suggested that Government has to discover this for itself; the private sector cannot do it for them, and EURIM would be better placed helping others. Others suggested that we should be endorsing best practice, and that the private sector had learned how to do this, and so could offer examples of good practice to government. The problem was not best practice, but why it was not followed: it was a matter not of changing policy, but of implementing and enforcing existing policy.

4.6 Point 6

(vi) EURIM should campaign for government to use only professionally developed, implemented and operated processes and systems.

SMEs have difficulty communicating with government, and as they could not join ‘the club’, they were inhibited from bidding for work. Effective processes were also needed to ensure compliance: perhaps an annual prize should be offered from the Industry for the public sector body that most closely met the requirements. There are a number of good small schemes; there are also secure systems in place for transmitting data between government bodies – but in many cases they have not been used!

It was agreed to establish a working group to look more closely into the issues (including how to involve SMEs) and decide if EURIM should proceed.

4.7 Point 7

(vii) EURIM should campaign for the Information Commissioner to have powers of enforcement.

It was argued that the HSE legislation works because directors fear jail terms and therefore take the issues seriously: if the Information Commissioner is to be taken seriously, similar powers are necessary, and the ICT industry should be campaigning accordingly.

This issue tied in with the independent review to be conducted by Richard Thomas (Information Commissioner) and Dr Mark Walport (Director of the Wellcome Trust), on the use and sharing of personal information in the public and private sectors. EURIM had received a specific invitation to respond to this, and will be organising a meeting in the New Year to discuss how we can help collectively with this consultation.

It was agreed to establish a working group to respond to the ICO consultation. In the meantime, members are invited to send comments to Dave Wright (davywright2@ntlworld.com).

4.8 Points 8 & 9

(viii) EURIM (in conjunction with Intellect) should continue to support the IMSPG through five working groups on Identity Management Standards.

(ix) The Identity Assurance Advisory Council is initiating a workshop to assemble a map of Information Assurance Initiatives. EURIM should support that initiative and develop a road map for data sharing.

It was agreed that EURIM should support both initiatives.

5. Information Sharing Protocols Report

5.1 Over the past 12 months, the EURIM Data Sharing Subgroup had been looking closely at barriers to data sharing from a local authority perspective, and how decision makers and frontline staff can be confident about what information can be shared in compliance with data protection legislation. A clear message from at least one local authority was the confusion associated with data protection and data sharing legislation, hence the call for clarification and tracing enabling legislation to citizen's needs.

5.2 The report has made a number of clearly focused recommendations in collaboration with the Ministry of Justice and the Information Commissioner's Office. These will tie into the ICO Draft Code,

and the revised report has been circulated for review by EURIM members and observers in the Personal Identity, Data Sharing and Transformational Government groups, with a deadline of 20th December for comments. After any revisions, the document will be published as a Status Report, and dispatched to the target audience hopefully by mid-January.

5.3 Further complications are introduced with multi-agency working; for example, different legislation applied to the NHS, which held a different view to others.

This point had been noted in the DSSG's report; simplification would depend on a common understanding of identification, in which the primary principle is to protect privacy.

5.4 A number of points in the DSSG report are relevant to both the ICO consultation and the IAAC. The ICO had provided feedback to the DSSG's Information Sharing Protocols Report, and the comments had been circulated to subgroup members and attendees of this meeting.

6. AOB

6.1 An event hosted jointly by EURIM, CSC and the All Party Group on Identity Fraud held on 10 December in the Macmillan Room, Portcullis House had attracted a good turn-out of parliamentarians, with a number of senior officials, including from the IPS. Nick Palmer MP had talked about the need for field separation in data. The representative from the Belgian Government said that this was used in its national identity scheme. There was sharp intake of breath from the MPs present when it was said that the Belgian Government accepted responsibility and liability for errors.

7. Date of next meeting

7.1 TBA, third or fourth week in January 2008.