On the web: uk.sun.com/identity

Positioning Federated Identity For The UK Government

Whitepaper

Date: February 21st. 2005

Author: Robin Wilton, Identity Management Solutions Manager

Sun Microsystems Ltd.
Guillemont Park
Minley Road
Blackwater
Surrey
GU17 9QG

Table of Contents

On the web: uk.sun.com/identity....1
Management Summary....3
Government expectations, themes and objectives....3
User inclusion, take-up and trust....3
1 The Liberty Alliance and the rationale for federation....4
Liberty's purpose....4
Network Identity and Federation....4
2 Sun's perspective on Identity in e-Government....5
Sun's vision and the role of identity....5
Identity 'drivers' in the Public Sector....5
Sun's strategic identity management aims....5
3 Application....6
3.1 Sun and Public Sector Identity solutions....6
3.1.1 The French Agency for e-Government Development....6
3.1.2 The North-East Regional Smart-card Consortium....6
3.1.3 US Department of Defense – Defense Manpower Data Center (DMDC)....7
Project characteristics....7
Functions provided by the DMDC Common Access Card....7
Customer comment....7
3.2 The legislation and its practical consequences....8
The broader e-government context....8
The importance of authentication and authorisation for policy control....8
Practical implications of legislation for identity management....8
4 Principles....10
4.1 Some informed views on identity and federation....10
Federated Identity Management – an introductory definition....10
Federated Identity and e-Government....10
Identity and Regulatory Compliance - “Crunch Time for Sarbanes-Oxley”....10
Why is Identity a key concept now?....10
Open, Federated Identity standards and the Public Sector....10
4.2 Core identity concepts and their implications for usage....11
A definition Identity....11
Credentials and the “Chain of Trust”....11
Stanrad assertions of identity and other attributes....11
5 - References and Citations....12

Management Summary

Government expectations, themes and objectives

Identity Management in the public sector is linked to a multitude of aims, principles and expected benefits. This paper sets out Sun Microsystems'™ Identity Management strategy, relating it to the Federated Identity architecture of the Liberty Alliance, and illustrating Sun's™ experience of public sector identity management projects. It addresses the following topics:

- Why federated identity management is the preferred option;
- What makes the Liberty Alliance a unique forum for standardisation;
- What qualifies Sun to advise on identity management strategy in the public sector.

Justifications for public sector identity management generally centre around four main themes:

- Law Enforcement: immigration and asylum control, prevention of terrorism, drug trafficking, money-laundering and other serious organised crime; identity as a key tool of regulatory systems.
- e-Government Service Delivery: more efficient and secure delivery of public services; better inter-agency and private-sector interaction; improved governance; reduction of benefit fraud.
- Business Process Improvement: improved interoperability between departments; measurable efficiency outputs; identity at the heart of information management and business processes.
- Delivery of Social Benefit: inclusivity of e-government; perceived benefits proportional to cost/effort; enhanced user experience (for both public servants and citizens); increased trust in e-government and privacy protection.

These in turn generate objectives of:

- extending and enhancing online collaboration and service delivery;
- improving efficiency and cost control;
- protecting sensitive information and critical resources.

User inclusion, take-up and trust

However, identity management also has the potential to bring about a fundamental change in the relationship between citizen and government[1] (The Identity Card Bill being a case in point). E-government will fail to achieve greater inclusion and participation if that change is not carefully managed, or the user experience it provides is worse than the status quo. It can deliver little or no benefit if citizens decline to use the service because it is too hard, or because they do not trust it.

Sun believes that there is now ample evidence in favour of federated identity as the best basis for overcoming these identity management issues and meeting the broader objectives. By contrast, there is also evidence that a centralised approach to large-scale identity management fails to provide a workable online analogue for real-world trust relationships. Indeed, centralised systems have been shown to undermine user trust – for example, when they are also used to aggregate 'behavioural' data about service requests and authorisation. This is particularly significant in the light of the UK Information Commissioner's expressed concerns about the current proposals for a National Identity Register[2].

- The Liberty model for federation means that the data custodian retains control of, and responsibility for, the data they manage on the user's behalf;
- It provides users with the means to control the sharing of their data, and therefore to manage their trust relationships with Service Providers and Identity Providers;
- It is, in Liberty's case, based on open specifications arrived at by consensus and with a publicly-affirmed commitment to interoperability and privacy protection.
- Federation provides better means of linking identity management with policy control, and therefore of exercising policy control over access to data and services. This, after all, is the goal: identity management is not an end in itself – it is useful only if it enhances service delivery.

1House of Commons Research Paper (Dec. 2004): The Identity Card Bill
2Information Commissioner's Office: Identity Cards - The Commissioner's View

1 The Liberty Alliance and the rationale for federation

Liberty's purpose

The Liberty Alliance was established to address the issues arising out of the global move towards online information-sharing on an unprecedented scale. The key identity management requirements it identified were:

- The need for an open, interoperable and decentralised standard for identity management;
- The need to provide privacy safeguards across all sectors.

The role of the Alliance is to produce open, standards-based specifications which meet these requirements and contribute to the following aims:

- An improved ability to form online alliances for the secure exchange of data (including between government agencies, as well as with non-governmental counterparts);
- Cost avoidance, cost reduction and increased operational efficiency;
- Interoperability without compromise to security or risk management;
- Decreased development cost through standards-based interoperability.

The Alliance has grown to over 150 members world-wide, spanning the commercial, government and non-profit sectors. Among the public sector member organisations are: Royal Mail, Hong Kong Post, Canada Post, the US Department of Defense, the US General Services Administration, the University of Hamburg, the University of Chicago, the Helsinki Institute of Technology and many others.

Network Identity and Federation

At the core of the Liberty Alliance's work is the concept that, online, an identity consists of multiple instances of credentials and attribute information. Those instances will be distributed amongst multiple organisations, often duplicated and sometimes inconsistent. One argument against centralisation is not so much that it puts all one's eggs in one basket: it is the wishfulness of expecting all one's hens to lay their eggs in a single basket in the first place.

Frequently the credentials, or some of the attributes, will establish the user as a member of a particular community of interest, and other members of that community will place trust in them accordingly. The communities of interest are often highly dynamic, and the trust relationships multi-party and asymmetric: the old ways of managing identity are seldom able to cope with this at all, let alone adapt if relationships or trust attributes change frequently.

The Alliance's specifications aim to help organisations meet the aims set out above, by:

- Simplifying access to services, whether inside or outside the organisation;
- Reducing the need to maintain and manage multiple sets of credentials;
- Reducing the cost and complexity of managing identity and attribute data;
- Catering for the dynamic creation and management of trust relationships;
- Preserving privacy and ensure data security.

The founders of the Alliance were motivated in part by a strong conviction that centralisation of credentials or attributes did not help meet these aims. Centralisation tends to result in trust relationships which are two-party, 'one size fits all', and therefore not a convincing equivalent for the way in which trust works in the real world.

As a result, the Alliance's specification work is based in the belief that federation of identity and attribute data is the most effective approach to the problems of using and managing network identities. The Alliance's white paper “Benefits of Federated Identity to Government” (see the Citations section at the end of this document) describes the approach in more detail, and sets out the ways in which federated identity can be applied in practice to government-to-government, government-to-citizen and government-to-business interactions.

2 Sun's perspective on Identity in e-Government

Sun's vision and the role of identity

Sun is known for its original corporate vision that "the network is the computer", a vision since supplemented with the idea of "everything of value connected to the network". There is a strong technological dimension to Sun's vision statements - but they are also important for what they imply about identity, authentication, authorisation, access control, trust and privacy. The more we assume that everything of value is connected to the network, the more vital it is that identity, appropriate access and online trust form the foundations of online service provision.

Identity 'drivers' in the Public Sector

Applying this vision to the government sector reveals a number of defining requirements:

- Use of the Internet and its technologies to meet e-government targets for improved collaboration and service delivery inevitably leads to increased data access and data sharing; this makes it critical to be able to secure information and resources, maintain integrity and auditability, and protect the privacy of those transacting online with government functions.
- Public sector funding is under constant pressure: the Gershon Review of Public Sector Efficiency (SR 2004) refers specifically to back-office, procurement and transaction services, and the need to ensure that cost is cut and budget efficiently allocated. In other words, services must be extended and improved, without compromising security and with year-on-year gains in the efficiency of public sector operations.
- The drive towards e-government and the knowledge-based economy extends the critical national infrastructure (CNI) in terms of scale and diversity, both inside government and in terms of its interrelation to the commercial sector. This is happening at a time of prominent concern over the vulnerability of the CNI to terrorist attack.

  "The office environment is evolving, with home-working, hot-desking and other kinds of flexible working becoming more common. Global competition has already increased the international mobility of many types of work, and the public sector will clearly not be immune from future changes. Following the events of September 11 2001, the need for resilience in the face of emergencies should have become a more prominent strand of business planning.[3]"
- Among others, the issues of counter-terrorism, crime prevention, management of immigration and asylum seekers, curbing benefit fraud and controlling healthcare costs have all been linked to measures which depend on establishing a person's identity (authentication) and entitlement (authorisation). There may still be debate as to whether a single physical national identity card is the most appropriate mechanism to deploy, but the requirement to enforce policy by means of one or more forms of credential is inescapable.

Sun's strategic identity management aims

In this context, Sun's strategy for identity management is based on the provision of:

- Secure control over information access by dynamic communities of employees, other agencies, vendors, suppliers, UK citizens and other individuals;
- Interoperable, federated authentication and identity management, so that users and transactions can pass seamlessly and securely from one IT environment to another without having to use multiple sets of credentials to do so;
- Automated provisioning and de-provisioning (the setting up and revoking of user accounts and access), to reduce the cost of managing users and accounts;
- Identity management tools which centre around users and identities, not computer accounts;
- Delegated administration, cost-effectively allowing users to manage their own details;
- Audit and reporting capabilities for internal governance and regulatory compliance.

3 Sir Michael Lyons – Independent review of public sector relocation

3 Application

3.1 Sun and Public Sector Identity solutions

This section briefly describes some of Sun's experience to date in the field of public-sector identity management. It is not intended to show that such projects are simple or problem-free, but it does indicate some of the relevant experience which supports Sun's conviction that a Liberty-compliant federated identity architecture is the most rational and productive approach. We would welcome further discussion of these, and other projects undertaken in such areas as secure distributed healthcare provision, e-voting and secure document exchange.

3.1.1 The French Agency for e-Government Development

Sun France recently produced an Architecture Reference document in collaboration with the French Agency for e-Government Development (Agence pour le Développement de l'Administration Électronique – ADAE); this sets out the functional and technical characteristics of a Liberty-based approach to federated identity, and since publication has been successfully used by the ADAE to explain and promote this approach across other government ministries.

Representatives of ADAE will be attending the Liberty Alliance's e-Government forum in Dublin on April 18th 2005, and would be willing to discuss their approach and the perceived benefits of federation in general and Liberty in particular. If there is interest beyond the data of the Dublin meeting, Sun is happy to conduct or to facilitate meetings and would welcome further discussion if this is the preferred approach.

3.1.2 The North-East Regional Smart-card Consortium

In the UK, work with the North-East Regional Smart-card Consortium (NERSC) has help Sun establish its credibility both as a trusted advisor and as a Liberty implementer. NERSC's project reveals some of the practical issues for which federation offers a significantly more practical solution than the alternatives. For instance, a requirement of the NERSC project is that multiple services should be accessible using a single smart card – but while some services (such as e-payments) are best accessed using chip-borne credentials, others (such as recording lecture attendance, or gaining physical access to buildings) may require the use of credentials in a different form (such as on a magnetic stripe). The project therefore exercises the ability of the architecture and technology to integrate multiple credentials into the card and allow them to be effectively managed after deployment.

It also exercises the fundamental Liberty principles of federated identity management between Identity Providers and Service Providers. In some respects, the non-technical aspects of the project present more durable problems than the technology: for instance, the commercial framework which would enable a library service (which cannot contemplate the expense of issuing its own smart cards) to share the resulting system with whichever organisation does issue the cards. These issues might be more clear-cut in a purely commercial operation – but in either instance it highlights the need to devote sufficient attention to non-technical factors. This is directly in line with Sun's previous experience in the Identrus inter-bank consortium for secure payment services: the consortium found that its time was spent roughly equally between developing technical specifications and agreeing the contractual framework within which the resulting systems would operate.

One final note is that the architects and leaders of the NERSC project are convinced that its successful adoption depends on the ability (which Liberty federation provides) for 'permissions' data (i.e. Attributes relating to entitlements) to be managed and exchanged in a secure and controlled way.

The key principle here is that of interoperability: the distinguishing value of the Liberty scheme is that it allows the integration of different service-provider technologies with minimal disruption of the heterogenous systems which are already in place.

3.1.3 US Department of Defense – Defense Manpower Data Center (DMDC)

Even in the early days of the Liberty Alliance, Sun was already helping to implement large-scale systems which embody the principles the Alliance would come to codify. The work currently under way on the NHS Spine directory is a case in point, which we are happy to discuss in detail on request.

Elsewhere, the completed project at the US Department of Defense (DoD) provides tangible proof of the benefits of this approach. A look at the original terms of reference set out by the DoD for the DMDC project indicates why:

> "-- Strengthen security -- Passwords are simply not good enough in today's Internet connected world, and PKI without a smart card is no better than a password.
>
> -- Guarantee privacy -- Digital identity is less about keeping people out and more about allowing only the appropriate people in. Identity is crucial to privacy and privacy is critical if personal, confidential data is used by digital services.
>
> -- Increase customer satisfaction -- The new ID badges bring the ATM user experience to network computing, giving users what they want, when they what it, from where ever they are in the world.
>
> -- Improve quality of life -- Reduced data entry, reduced processing time, reduced time in lines, reduced administration burden and more accurate information processing."

Project characteristics

The Defense Manpower Data Center implementation spans some 1,500 workstations at 900 sites in 13 countries; the target user population is some 4.3 million users, managing 23 million active records and generating over 1.7 million transactions a day. In this environment, identity federation is used to create interoperability between 75 disparate systems, from vendors and partners including Sun, Oracle, EDS, CSC, ActivCard and Schlumberger.

Furthermore, as the DMDC themselves put it: "The real kicker in the whole undertaking was that the [Common Access Card] system would be built upon an infrastructure that had been running at the DMDC for 17 years[4]". Exactly as for the UK NERSC project, an important principle of Sun's Identity Management systems is that they should add value based on what is already in place.

The implementation project for all this was successfully completed within a 15-month deadline, set by the US Department of Defense as the DMDC's 'customer'.

Functions provided by the DMDC Common Access Card

Functionally, the system combines several types of credential (encrypted passwords, PKI-based credentials) with other card-based access control mechanisms (such as magnetic stripe), e-cash and secure storage of personal details. The centralised control the system provides over identity management and access control allows the DoD to respond quickly and flexibly to changes in security status: for instance, should the over-all defence condition change, this can rapidly be reflected in access controls so that a system which previously only required password access might now demand a PKI-based authentication from the user.

Customer comment

"Almost everything in our system, from our Java cards to our issuance portals to the DEERS databases to our servers [is] either from Sun or built on Sun."

Bill Boggess, Authentication and Access Program, Development Chief Defense Manpower Data Center

4 Bill Boggess, Authentication and Access Program, Development Chief Defense Manpower Data Center

3.2 The legislation and its practical consequences

The broader e-government context

Public administrations of all scales, from the US and EU to member states such as the UK, France and Spain, and smaller states such as Dubai and Singapore, have recognised that information technology is key to the development of competitive, world-class knowledge economies and digital societies.

The Lisbon Agenda and the UK's e-Government targets embody this principle, and emphasise what Patricia Hewitt has described as "a sea change in European thinking away from heavy handed regulation and intervention towards knowledge, skills, enterprise and innovation[5]", with all that implies in terms of openness, flexibility and online access to government services. She also set out the following challenges:

> "... access for our individuals and our businesses, any time, any way, any where.
>
> Start with the citizen, not the service
> Get the process right, not just the technology
> Partner with the private sector [6]."

The importance of authentication and authorisation for policy control

If the service-delivery model is to be citizen-centric, then establishing the identity of the requester and the basis for their entitlements is indispensable. The same principles apply to internal 'government user' access as well as to interactions with businesses, NGOs and other administrations. In each case, a key first step is to establish which 'constituency' the requester belongs to, and therefore what entitlements, security and integrity measures are appropriate.

These requirements for authentication, data security and data integrity are evident throughout the legislative framework for e-government and the information society. Identity management is the keystone of these functions.

Practical implications of legislation for identity management

The following are some examples of just how inextricably identity processing is bound up with the practicalities of e-government:

1. The Data Protection Act 1998 (DPA)

   Among its other provisions, the DPA contains measures to prevent 'fishing' enquiries, where a request is deliberately vaguely framed so as to solicit large volumes of data from which the desirable items can then be selected.

   As an example of the practical issues raised: a police authority's request to a local authority under Section 29 of the act was rejected on the grounds that they were 'fishing'. The police authority re-issued a more detailed request including the subject's identity and the reason for the request – i.e. the alleged offence. This was done by email – unencrypted and without proof of origin, proof of integrity or proof of correct delivery.

   Refusing to reply by the same medium, the local authority would only provide the requested data in hard-copy to an identified officer in person. So the same piece of legislation was leading one agency to increase the amount of sensitive personal data it transmitted, while at the same time leading the other agency to revert to hand-carrying instead of online exchange.

   Clearly, federated identity management alone would not solve this problem - that would require a combination of improved user awareness, better processes and a more secure communications infrastructure. However, this illustrates that tools such as interoperable authentication and digital signing would be a key enabler of all these elements.

5 The Rt. Hon. Patricia Hewitt - The Lisbon Agenda - Delivering Jobs and Prosperity for all
6 The Rt. Hon. Patricia Hewitt - World Congress on Information Technology: "Better Government: The Vision and the Challenges"

2. The Freedom of Information Act 2000 (FoIA)

   The FoIA gives rise to cases where certain parts of the information requested should only be disclosed to individuals with a specific role: for example, in cases of assault or bullying in schools, the names of the children (or staff) involved might legitimately be accessed by a social worker or a school governor but perhaps not another parent.

   Context and role-based access control are effectively impossible without identity management, as well as the effective management of meta-data about entitlements and previous access. This still leaves the knotty problem of how one might deal correctly with multiple requests from a single person who can validly exercise different roles with conflicting access entitlements.

3. The European Privacy Directive (EPD)

   The EPD sets out requirements for control over the collection and processing of personal data, including the need to ensure that data is not subsequently used for other purposes (in common with the UK DPA). Again, this gives rise to requirements for contextual and role-based access control over the life of the information. The EPD has also led several stakeholders to conclude that information and e-government systems should be designed in a way which allows the possibility of anonymous authentication – in other words, the ability to assert the entitlement of the requester without necessarily also divulging their identity.

   The Article 29 Working Group examined the Liberty specifications and concluded that their federated approach had benefits for user privacy in line with the objectives of the EPD. Their review recommended that the Alliance produce guidelines for the application of privacy- and identity-related principles, which it has since done. There are links to these in the Citations section of this paper.

4. The Civil Contingencies Act 2004 (CCA)

   The CCA includes requirements for Category One responders, critical infrastructure providers and the wider business continuity community to create, maintain and communicate their continuity measures. Just as there are many aspects of Category One responders' plans which have to be kept strictly confidential if they are to be effective, so there will be aspects of other stakeholders' plans (including those in the private sector) to which appropriate access must be adequately controlled. Likewise, many of the powers of the CCA would be severely undermined if instructions issued under the act could not be shown to be genuine – whether issued physically or electronically.

These are only some of the legislative measures which give rise to identity management issues, and only samples of the kinds of practical problem which may arise. There are many other measures which generate similar requirements for secure online interaction between the regulators and the regulated, such as the US Sarbanes-Oxley laws on corporate governance and accountability, the corresponding UK Companies (Audit, Investigations and Community Enterprise) Act 2004 (CAICE), the Basel II regulations on banking capital adequacy and risk management and so on.

What is consistent across all of these, whether in the public or private sector, is the need to comply with the business regulations, achieve one's statutory or business goals, and do so online without compromising security. This is practically impossible without an effective and interoperable infrastructure for federated identity management.

Significantly, the Gartner "e-government hype cycle"[7] suggests that Security Issues are one of the factors which drive implementers from the Peak of Inflated Expectations down to the Trough of Disillusionment... and that Interoperability is one of the factors which marks the start of the gradual journey towards productive long-term application of the technology.

7 Andrea DiMaio, Gartner Research – 'Local e-government now – 2004': SocITM/I&DeA

4 Principles

4.1 Some informed views on identity and federation

Federated Identity Management – an introductory definition.

“Federated identity management makes it possible for an authenticated entity to be recognised and take part in personalised services across multiple domains. Federated identity avoids the pitfalls of centralised storage of personal information, while allowing users to link identity information between accounts. Since users can control when and how their accounts and attributes are linked and shared, they retain greater control over their personal information. In practice, this means that users can be authenticated by one organisation or website and be recognised, and delivered personalised content and services, in other domains without having to re-authenticate.”

Liberty Alliance White Paper - “Benefits of Federated Identity to Government”.

Federated Identity and e-Government.

“... we also recognize that rules and infrastructure for the federation of identity apply much more broadly than the Federal government and we are committed to work in collaboration with industry, states and local governments to best serve all of our citizens and customers.”

Karen Evans, Administrator of the Office of Electronic Government and Information Technology, US Government. (Liberty Alliance White Paper - “Benefits of Federated Identity to Government”.)

Identity and Regulatory Compliance - “Crunch Time for Sarbanes-Oxley”

"Some common problems are starting to emerge with internal controls at some companies. The first is multiple difficulties with information technology systems, including the basic need to ensure that only approved people have access to data."

Andrew Parker, Financial Times, 9th. February, 2005

While this was written in reference to the Sarbanes-Oxley regulatory requirements, parallels to the experiences of this massive community in trying to achieve accountability are already visible in the ongoing enterprise of e-government.

Why is Identity a key concept now?

“[In 2005] There will be almost no security problem left that isn't seen as really being an identity problem. This is a trend that has been going on for three years now. Think of the last product or method you saw at a security conference (that actually produced value) that wasn't identity based. By the end of 2005, it won't be just [Digital ID World] readers who understand the need for security to use identity as its organizing paradigm. Identity will finally be seen as critical to security success.”

Phil Becker, Editor-in-Chief, Digital ID World

Open, Federated Identity standards and the Public Sector

"Federated identity" technologies are at a natural advantage because of the extent to which they take account of integration constraints and personal privacy. They define protocols and data exchange formats for data management and access control, based on the principle that in a federated architecture 'each participating system retains responsibility for the processing and data which it holds'.

The Liberty Alliance solution is arrived at by consensus in an open consortium, and with a publicly-affirmed regard for cross-border (and in particular European) legislation concerning data privacy. It is absolutely suited to the issues of e-government in France."

Agence pour le Développement de l'Administration Électronique – ADAE

4.2 Core identity concepts and their implications for usage

Although this paper assumes that the term 'identity' is clearly understood and consistently applied, there is benefit in examining it in detail, and looking at the implications this reveals.

A definition of Identity

When we assert the identity of a person, we are usually asserting that the person presenting a given set of credentials (a passport, a user-ID and password) is identical with the person to whom those credentials were originally issued. Credentials such as Certificates of Birth or Marriage derive their validity from the various forms of proof available at the time of their creation. That validity is often used as the basis for the issuing of subsequent credentials (such as passports), which in turn are used to underpin other credentials (such as visas and airline tickets).

Credentials and the "Chain of Trust"

The issuing of the credentials and their subsequent validation are seldom performed by the same entity. (For instance, Driving Licenses are issued by the DVLA but usually checked by the police. Passports are issued by the Passport Service but usually checked by Customs & Immigration officials).

This makes explicit several factors which are otherwise usually ignored in practice:

1. There are discrete roles for issuing credentials ("Identity Provider") and using them to authenticate the holder ("Service Provider");
2. The use of credentials is a very 'transitive' process. Authentication depends on a 'chain of trust', which extends from the issuing of the credentials to the point where they are presented. If the original registration process, the credentials themselves, or the validation process can be subverted, then the chain of trust is broken and the authentication is undermined.
3. Identity is seldom asserted for its own sake; it is usually asserted in order to establish an entitlement to something (whether that is health treatment, or the less welcome 'entitlement' to have one's licence endorsed...).
4. It may be possible to establish that entitlement on the basis of the credentials alone, or it may require some additional piece/s of information. A good example is that a passport may provide good evidence of identity (i.e. that the holder identified themselves to the satisfaction of their passport issuer), but the entitlement to enter the country usually derives from a visa inside the passport which conveys additional information.

Standard assertions of identity and other attributes

It therefore makes sense to think of assertions of identity as the foundation for other layers of assertion: for instance, assertions of entitlement, or other attributes such as creditworthiness, subscriber status, location, or other data relating to this individual or this service request. As explained in the section on the Liberty Alliance, we can expect multiple instances of data to exist at all these layers, and to be distributed among identity providers and service providers.

In the model adopted by Sun, the Liberty Alliance and the Organization for the Advancement of Structured Information Standards [OASIS], those layers of assertion are embodied in a set of specifications known as SAML – Security Assertions Mark-up Language. This provides an open, standard way of defining and exchanging assertions about authentication (identity), authorisation (entitlement) and other service- or user-related data (attributes).

As discussed elsewhere in this paper, one possible requirement is for services to be granted on the basis of attribute-level data while preserving the individual's anonymity at the authentication level. This represents a major step towards the 'Privacy-Enhancing Technology' currently being proposed in support of legislation such as the European Privacy Directive.

5 - References and Citations

This document was drafted on 21st February 2005.

On the same date in 1952, identity cards were abolished in the UK.

The National Registration Act of 1939 established identity cards for the purpose of conscription, rationing and security enforcement.

By the date of their abolition, the identity records were being used by 39 government agencies.

Article 29 Working Party: Working document on online authentication services (Jan 2003)

Becker, Phil - "Predictions for Identity in 2005":
http://www.digitalidworld.com

Civil Contingencies Act 2004 (CCA)

Data Protection Act 1998 (DPA)

European Privacy Directive 95/46/EC (EPD)

Freedom of Information Act 2000 (FoIA)

Gershon, Sir Peter: Review of Public Sector Efficiency (SR 2004)

Hewitt, The Rt. Hon. Patricia – Archived speeches:
http://www.dti.gov.uk/ministers/ministers/hewitt.html

House of Commons Research Paper (Dec. 2004) - : The Identity Card Bill

Information Commissioner's Office - "Identity Cards – The Commissioner's View":
http://www.informationcommissioner.gov.uk

Liberty Alliance – Index of White Papers:
https://www.projectliberty.org/about/whitepapers.php

Liberty Alliance: White Paper – Benefits of Federated Identity to Government

Liberty Alliance: White Paper - Liberty Protocol and Identity Theft

Liberty Alliance: White Paper - Security Best Practices

Lyons, Sir Michael: Independent review of public sector relocation

SocITM/I&DeA subscriber report – "Local e-government now - 2004": http://www.socitm.gov,uk

SocITM insight report – "Knock knock: who's there?":
http://www.socitm.gov.uk/Public/insight/publications/Knock+Knock.htm

Sun Solution White Paper – Secure Identity at the US Department of Defense:
http://www.uk.sun.com/identity

All these documents can also be viewed on-line via Sun's Identity Home Page at:

http://www.uk.sun.com/identity