Identity Management

The Technologies
Their Business Value
Their Problems
Their Prospects

Roger Clarke

March 2004
Executive Summary

The concept of 'identity management' has burst into prominence during the last few years. Identity management schemes are intended to provide organisations with assurance about the identities that they deal with over the Internet, particularly the identities of individuals.

This report commences with an introduction to the problem that identity management schemes are designed to solve, and an outline of the general shape of the solutions that are being promoted. A case study is provided of the first scheme that was deployed on a large scale, including lessons learnt from it.

Many variants of the general solution have been proposed. The second part of the report examines those that are being offered to corporations and government agencies, in particular extended forms of single-sign-on, and federated services.

But tools already exist, and more are emerging, which place identity management closer to the client end of the network. Moreover, the scope exists for subversion of corporate identity management schemes and for counter-measures against them. This alternative world of identity management mechanisms is examined, and the tensions identified between them and mainstream, server-side schemes. A 'super-architecture' is outlined, which provides an overview of the complex inter-relationships that are emerging.

For a product to succeed in the marketplace, it needs to display a number of characteristics. Strategic partnerships and client lists are important, but they are unlikely to overcome the disadvantage of poor product features. The next section digs down beneath the surface of the mainstream schemes in order to evaluate whether they are conceptually sound.

The current crop of products and proposals are shown to be seriously inadequate. One problem is a deficiency in the appreciation by designers of what the assertions are that organisations need to authenticate in order to manage their business risks. Most schemes also fail to distinguish between identities and the entities that underlie them, and overlook the existence, and likely continued existence, of anonymity and pseudonymity.

Consideration is also given to the extent to which scheme sponsors are addressing trust and privacy issues, and whether and how they are involving in the development of their schemes the people whose identities they propose to manage.

The schemes that are attracting the most press are conceptually inadequate, and have not achieved a balance among their many objectives. The report identifies ways in which identity management schemes could reconcile the conflicting interests. It draws attention to research projects that may enable the next round of schemes to be more likely to succeed than the current proposals.
# Contents

1. INTRODUCTION ........................................ 1
2. THE CONTEXT ........................................ 2
   2.1 The Perceived Problem .......................... 2
   2.2 The Basic Solution Envisaged .............. 4
   2.3 Possible Extensions ......................... 5
   2.4 The First Widespread Implementation .... 6
3. SUPPLY-SIDE ARCHITECTURES AND PRODUCTS ...... 9
   3.1 A Working Definition .......................... 9
   3.2 Single-Organisation Single-Signon (1-to-1-to-n-in-1) ................. 10
   3.3 Single-Signon to Multiple Organisations (1-to-1-to-n-in-n) ...... 11
   3.4 A Comprehensive Inhabitant Registration Scheme ............. 12
   3.5 Closed-Community Schemes .................. 12
   3.6 'Federated' Single-Signon Services (1-to-n-to-n-in-n) ....... 13
4. DEMAND-SIDE ARCHITECTURES AND PRODUCTS .... 18
   4.1 Consumer/Citizen Interests ................. 18
   4.2 An Extended Set of Architectural Alternatives .................. 19
   4.3 User-Selected Intermediaries ............... 20
   4.4 Own-Device as Identity Manager ........... 21
   4.5 Nymity Services ............................... 24
   4.6 Identity Management Subversion Tools ...... 24
5. THE MULTI-MEDIATED SUPER-ARCHITECTURE ...... 26
6. CONCEPTUAL INADEQUACIES .......................... 28
   6.1 Authentication .................................. 28
   6.2 Entity and Identity ............................ 30
   6.3 Data Representing Entities and Identities .............. 31
   6.4 Nymity .......................................... 33
   6.5 (Id)entification and (Id)entity Authentication ............ 35
   6.6 Natural Persons, Organisations and Agents ........... 36
7. SOCIAL IMPACTS ..................................... 38
   7.1 Understanding and Valuation of the Privacy Concept ......... 38
   7.2 The Value of Multiple Identities ............. 41
   7.3 Anonymity and Pseudonymity ................ 41
   7.4 Representation of Consumer Interests ........ 43
8. THE SCOPE FOR BALANCED SOLUTIONS ............ 47

REFERENCES ............................................ 49
APPENDIX: INDUSTRY PARTICIPANTS .................. 54
GLOSSARY ............................................. 57
1. Introduction

The term 'identity management' has been much-used since about 2000, as a generic descriptor for services designed to authenticate remote users of network-accessible services. Typical of the popular descriptions was this: "eliminate the need to remember multiple names and passwords while browsing the Web" (Mook & Newell 2001). Another catch-cry has been 'authenticate once, transact many'.

The genre came to public attention in 1999 with the deployment of Microsoft's Passport, initially when it was imposed on users of the Hotmail service, and again when it was announced that Passport would become a generalised login scheme to support centrally-stored 'wallets' and to enable people to store all of their passwords for many different services in Redmond WA. This competitive manoeuvre stimulated the formation of a broadly-based business coalition, Liberty Alliance.

Several other services have been announced and some have been implemented. The maturation process of new technologies is more rapid than it once was, and standards processes have been launched, and some specifications have been published. The identity management movement has developed in a close relationship with 'web services'. Web services are intended to enable applications that involve collaboration among the web-sites of multiple providers. Identity management is regarded both as a good example of a web service, and as a foundation for other web services.

As is common with rapidly developing ideas, the identity management arena is subject to a great deal of marketing hype, power-plays, frequent and rapid changes in focus, and many conceptual misunderstandings. This survey of the field draws attention to key commonalities and differences among the approaches being taken, and to tensions among different interests.

This report commences by examining the context within which products, collaborative initiatives and protocols are emerging. It then describes the various architectures that have been developed by business for business, and several others that are emerging that are more strongly oriented towards consumers' interests. Later sections identify a range of conceptual inadequacies inherent in much of the conventional thinking about the topic, and consider negative social impacts of current approaches. The report closes by suggesting how the conflicting interests can be reconciled.
2. The Context

This section considers the context within which existing and proposed schemes have been developed. It commences with an examination of the problems that the schemes were conceived to address, then describes the framework underlying the basic and the more advanced solutions that have been devised. Finally, a description is provided of the first product that was launched, Microsoft’s Passport.

2.1 The Perceived Problem

Since 1993, Internet infrastructure and Web facilities have greatly increased the ability of users to connect from remote locations in order to access data and services.

Much of the data and many of those services are freely and openly available on the Web. If the Web continues to function as it was originally envisaged, that will always be the case, because a great deal of the motivation driving publishing and services provision is social in nature. Even where the motivation is economic, it may involve deferred or indirect reciprocity rather than the direct and immediate reciprocity inherent in conventional markets, and hence may still be open to all comers. For treatments of cyberspace economics, see Shapiro & Varian (1999) and Clarke (2003b).

Access to some data and to some services is not free and open, however, but contingent upon various conditions being satisfied. On eCommerce sites, access may be restricted to people who pay a fee, or have already paid a fee in the form of a subscription. In the case of eProcurement, detailed requirements documents may only be intended for pre-qualified tenderers. And accounts associated with individuals, for example in Internet banking and some eGovernment applications, are only intended to be used by the relevant person and their agents.

In these circumstances, web-servers need to permit access to data and services in a way that is appropriate, depending on who the user is, or on some attribute of the user. In most of the discussions to date, the focus has been on the user’s identity rather than on their characteristics, although this is starting to change.

There are many challenges involved in determining who the user is and what they should be permitted to access. Conventionally, the processes that need to be performed are divided into three phases, outlined in Exhibit 2.1.

Each of these segments of activity is difficult to perform well, and expensive. In addition, the procedures involved may be inconvenient and intrusive. Problems arise both from false positives (accepting a user who should have been rejected) and from false negatives (rejecting a user who should have been accepted).

When organisations decide how they should perform each of the phases, they trade off the costs and the many other disbenefits against the benefits that they can gain, and the risks that they can neutralise. There are many alternatives, and
many different cost and risk profiles; and hence there is enormous diversity in the processes that are employed.

**Exhibit 2.1: Phases in User Access Security**

- **Pre-Authentication.** This is undertaken as part of a registration or enrolment process before a user-account is created. It involves activities intended to provide some level of assurance that the person is who they claim to be. Common techniques involve requests for documents or information that represent evidence of the use of an identity. The question to be answered is: ‘who is the person who I am going to associate with this identifier?’

- **Authentication.** This is undertaken each time a person initiates activity that involves access to controlled data or services. It comprises activities whose aims are to provide confidence that the user is the person who was intended to use that particular identifier. This typically involves the keying by the person of a password that was issued to them. The question to be answered is: ‘is the person presenting the identifier the person who it is intended to be?’

- **Authorisation.** This is undertaken each time an already-authenticated user seeks access to particular controlled data or services. It comprises activities which aim to establish what privileges or permissions the user should enjoy. A common technique is to look up that user’s entry on an Access Control List (ACL). This addresses the question ‘what access should I permit this user?’

In the pre-Internet era, organisations mostly performed these identity management functions themselves. Although some rationalisation of effort occurred, it was seldom pursued with commitment. In the new context of eBusiness, attempts are being made to achieve a greater degree of rationalisation. One approach is through commonality of procedures and infrastructure. Another is the performance of appropriate functions by third-party services.

The movement towards third-party services has arisen because several players have perceived a need, and an opportunity, for users to be automatically transferred between web-sites, with their identity made available to the next site in the chain. Those players have seen this as important because continual requests to users to re-authenticate themselves to the next site in the chain are perceived as being an impediment to adoption.

The primary drivers to date have been information technology companies that see such service-provision as an attractive line of business. Consumer marketing companies are also alive to the potential advantages in their dealings with their customers, and with the customers of their strategic partners and of other companies.

Governments are also players in this sphere. Motivations for eGovernment include enhanced service, cost reduction, and cost transfer from agencies to
business enterprises and to citizens. In addition, there are many contexts in which inter-relationships arise among eGovernment services, and the notion of ‘joined-up government’ has been much-discussed in recent years. Individuals could find it convenient to permit data about them to be transferred from the first agency that they interact with onwards to the next in the chain. Agencies could achieve savings in the areas of pre-authentication and authentication, but also in data-capture, and could thereby provide their services both more effectively and more efficiently.

A further factor is sometimes raised (although it figures remarkably little in documents produced by scheme sponsors). Organisations that hold personal data generally have an obligation to make the data accessible by the person that the data relates to. But they also have an obligation to take precautions to prevent other people masquerading as the data subject and thereby gaining access to the data. Identity management services may be able to contribute to the effective and efficient performance of that responsibility.

### 2.2 The Basic Solution Envisaged

The problem is in sharper focus than it was one and two decades ago, but it is not new. There is a variety of predecessor schemes, which have been to some extent reflected in recent proposals for identity management mechanisms. During the hey-day of mainframe computing in the 1970s and 1980s, access control products such as IBM’s RACF provided protections against inappropriate behaviour by internal users, and to a lesser extent by external users as well. The Access Control List (ACL) approach used by such products has been augmented in recent years by the concept of Role-Based Access Control (RBAC). RBAC associates permissions with organisational roles (such as operator, manager, guest, system administrator), rather than with individual usernames.

Other tools that pre-date identity management include Kerberos and the X.500 directory standard. X.500 failed its original purpose, but the approach has been implemented in more limited form as multiple, independent X.500 and LDAP directories. Conventional public key infrastructure (PKI) for digital signatures, based on X.509v3 digital certificates, would have performed the function of identity management had it not proven ineffectual when applied to large user-populations (e.g. Clarke 2001a).

Up-to-date solutions are envisaged, that reflect the particular context of the open public Internet, and the facilities available over the World Wide Web. Exhibit 2.2 provides a simplified description of how the authentication phase is meant to work.

Many variations to this basic idea are possible, and many have been deployed, prototyped or proposed. Some of those variants adopt particular approaches to the nature of the token. Others adopt different patterns of communication between the server that performs the authentication and the server that relies on the authentication and permits the user to access data or services. This may involve traffic between the servers and the browser, or between the various
servers without reference to the browser. In some schemes, those flows involve a substantial digital signature PKI.

Exhibit 2.2: The Conventional Process

1. A user performs authentication procedures by means of their browser. (Typically, this involves the keying of a username and password into a web-form, but many variants are possible using passwords, tokens or digital signature keys)

2. The browser transmits the authentication data to a web-server. (To protect sensitive data such as passwords against interceptors, this would be commonly by means of an encrypted channel, typically using the well-established Web add-on feature SSL/TLS)

3. The web-server performs the appropriate authentication process. (That most commonly consists of checking that the password is correct)

4. The web-server creates some form of secure digital token. (This might be a Kerberos ticket, or a signed digital certificate that identifies the user in some manner, and declares that the user has been authenticated)

5. When the user clicks on a link to another site, that token is made available to the second site

6. That site may choose to accept the token as sufficient authentication of the assertion that the request came from the user identified in the token

2.3 Possible Extensions

The basic solution envisages a service that authenticates the assertion that the user is the (or an) appropriate person to use a particular identifier. The opportunity exists for enhanced services. In particular, the identity management service might provide the relying organisation with such information as the following:

- further identifiers of the identity, such as the user's full name;
- attributes of the identity, such as the person's age-range or qualifications;
- additional authenticators that can be used to increase the authentication strength (e.g. call-back arrangements, shared secrets, public digital signature keys);
- authorisations that the identity has to access specified data and software on specified servers;
- information about the capacities that the identity has to act as an agent for a specified principal.

Some visions for identity management extend the notion further, to include notarisation of the identities of parties to a message. The intention in these cases is to achieve 'non-repudiability', or at least the more attainable aim of providing...
evidence that places the onus of proof on the party that wishes to repudiate their responsibility for a message.

At this stage in the evolution of the schemes, their capabilities are in most cases restricted to basic identity authentication, and the provision of some additional data. The extensibility of the services, and the declared ambitions of many service providers does, however, need to be borne in mind during the remainder of this analysis.

2.4 The First Widespread Implementation

Insight can be gained by reviewing a mainstream example. This particular case is important because it was an early deployment, it was an initiative by a major player, it has influenced the path of development of the idea, and it has been adapted somewhat since its first introduction.

(1) Single-Signon for Multiple Microsoft Sites

Microsoft's Passport was imposed on well over 100 million Hotmail users in 1999. It can be used as a single-signon mechanism for many Microsoft applications and sites, including Microsoft corporate, Hotmail, the various Microsoft Network (MSN) services, and the MSNBC news service.

A Passport comprises a username /password pair, supported by a shared secret to deal with lost-password problems. The username is an email-address (not necessarily at Hotmail).

User-supplied attributes are associated with the username. During the period 1999-2003, the data has comprised:

- e-mail user name (as primary identifier);
- first and last name and birth date (presumably combined, as second identifier);
- country/region;
- state/territory;
- postal code;
- time zone (which is theoretically redundant given the country and postal code, but could be used as a cross-check for data-accuracy);
- gender;
- language;
- occupation.

During registration/enrolment, authentication procedures continue to be limited to call-back, i.e. when establishing the username, the person has to respond to an email sent from Passport to the email-address that the person nominated. The process gives rise to lightly authenticated pseudonymity. That is to say that, in its raw form, Passport does not provide any basis for strong authentication of
identity, and hence is applicable to applications for which minimal security concerns exist, and for which nyms are permissible.

The basic service is capable of being significantly extended, however. Any nym can be used to build up a profile based on the transactions that it conducts with sites, including for example which pages are visited, when, how often, from which IP-address, and using which browser-type and operating system. Users also disclose data while conducting transactions. This may include important additional data-items, such as addresses (e.g. for delivery of goods or prizes), telephone-numbers (e.g. for notification of delivery or awards), and credit-card details (to pay for purchases). Subject to any regulatory and contractual constraints that may apply, data from other sources such as credit bureaux and marketing database services can be merged with the profiles.

(2) Single-Signon for Multiple Sites in Multiple Organisations

A Passport can be used on additional sites, under a scheme currently branded as .Net Passport. Over 40 .Net Passport sites were declared as at December 2003). Under this arrangement, a person can sign into sites such as eBay, Starbucks and 'USA Today' using their Passport identity rather than having to establish an account directly with the site, and remember that username and password as well. The mechanism underlying the service is that the site seeks a token from the Passport site that declares the user to be authenticated, and sets a cookie in the user’s browser.

Use of a Passport beyond the Microsoft realm is based on consent, and the user can currently choose whether to disclose only their e-mail address, only that plus their first and last names, or all of their registration information. However, the site warns that the complete set is required for registration at many web-sites, and that some .Net Passport-participating sites may require each user to undertake further authentication measures.

Each organisation can develop a user profile, as described in the previous subsection. Subject to any regulatory or contractual constraints that may apply, multiple organisations may share the data in the user profiles that they accumulate.

(3) Extensions

Microsoft’s Wallet is an extension to the Passport scheme, although it appears to have made slow progress during 2002-03. It stores additional personal data relating to the person’s payment methods, in order to make that data available to Microsoft and to third-party sites. At various times, the data has comprised Payment Information (Card type, Card number, Name on card, Expiration and Description); and Billing Address and default Shipping Address (First name, Last name, Address line 1, Address line 2, City, State/province, Postal code, Country/region, Phone, E-mail, and Description). Data can be stored about multiple credit cards, and about debit cards if they do not require a personal identification number (PIN).
There appear to be plans to either augment the wallet content or to create additional wallets, in order to store further data such as shopping preferences (e.g. clothing-sizes), and health information.

A further offering is Kid's Wallet, which claims to enable parents to manage data about their children, once again under Microsoft’s control in Redmond. Its primary purpose is to assist merchants to comply with the U.S. Children’s Online Privacy Protection Act (COPPA).

For some time, Microsoft referred to Passport as the basis for an initiative at first code-named Hailstorm, and later My Services, which was to be a centrepiece of the .Net family of web-services capabilities. There have been reports that this has been shelved (e.g. Markoff 2002), due to channel conflict issues and resultant unpopularity with key Microsoft customers, although privacy concerns were also mentioned.

(4) Regulatory Hurdles

The conditions imposed on users when they sign up to Passport have attracted attention from regulators. Following an action by a coalition of consumer and privacy organisations commenced in July 2001, the Federal Trade Commission found that Microsoft had made false representations concerning Passport and associated services. It imposed requirements for a comprehensive information security program, for action to avoid further misrepresentation, and for independent audits every two years for the next 20 years to ensure compliance (FTC 2003).

The European Union has also investigated Passport, and the relevant EU Group issued a Report that found that the system violated several EU data protection rules. It required Microsoft to "better inform users of their privacy rights under European laws, more fairly collect and process their personal data, make it easier for Passport users to know what personal information Microsoft and its Passport affiliates collect about them, and allow users to restrict the use and sharing of that information for commercial and marketing purposes" (EPIC 2003, summarising EU 2003).
3. Supply-Side Architectures and Products

This section provides an overview of schemes that have been devised by information technology providers and their various industry associations. These designs have been oriented strongly towards the perceived needs of business and government, with the needs of individuals operating as constraints on the achievement of the organisations' objectives. Later sections of this report draw attention to a number of problems with these schemes. For the moment, however, these problems are left to one side.

This section commences by providing a working definition. The following subsections deal with single-organisation single-signon; extensions of that idea beyond the boundaries of a single organisation; the extreme case of a comprehensive inhabitant registration scheme; more limited community-specific schemes; and finally the currently mainstream notion of federated single-signon schemes.

3.1 A Working Definition

It is useful to formulate a definition of the key term that reflects the information presented so far:

Identity Management is a set of processes that enable the authentication of assertions relating to identity. The term is often used in a more restrictive sense, however, to apply to the specific context of online access over open public networks.

A number of processes is involved. Some of the important elements are:

- registration or enrolment, in order to establish the basis for subsequent processes. This includes:
  - pre-authentication of assertions about the person; and
  - the establishment of means whereby authentication can later be performed conveniently but reliably;
- authentication of assertions that the user presenting is that person;
- assurance to relying organisations and services;
- maintenance;
- revocation.

The definition focusses on identity, but is intentionally worded openly ("assertions relating to identity", rather than "assertions of identity"). This is because the scope encompasses single-signon to multiple applications and sites, but extends further, to support the sharing of data about users.

Proposals for identity management schemes have focussed very heavily on authentication services, with extensions to data-sharing. But they have generally
paid only limited attention to pre-authentication, and have left authorisation matters to the relying parties. This report accordingly omits discussion of access controls, whether username-specific, role-based or otherwise.

### 3.2 Single-Organisation Single-Signon (1-to-1-to-n-in-1)

The basic context is access by users over open, public networks to multiple websites within one particular organisation. Separate schemes for each web-site are expensive, and require users to remember multiple username/password pairs.

The general notion of 'simplified signon' reduces the number of username/password pairs that users need to remember in order to gain access to multiple systems. The concept of 'single-signon' enables a user to access multiple sets of system resources after being authenticated just once, most commonly by keying a single username/password pair.

**Exhibit 3.2:**

**Single-Organisation Single-SignOn**

(or Silo'd) Identity Management

Most commonly 'single-signon' is used for employees within a company or government agency. A typical use is to enable access to several operational systems plus the human resources management (HRM) system. In each case the person may have multiple roles, e.g. in the HRM system, they may have supervisory responsibilities for a number of staff-members, and of course are themselves a staff-member. In some cases, people external to an organisation may be users of multiple applications, servers or web-sites, e.g. as taxpayers dealing with multiple branches within the national taxation authority, or as customers of a provider of a range of financial and/or travel services such as American Express.

Examples of such schemes include applications of such products as Passlogix v-GO Single Sign-On® (SSO), IBM's Tivoli Identity Manager, MS Passport when
used for Hotmail and MSN, and AOL’s ScreenName used within the AOL family of services.

This approach has been retrospectively dubbed the *silo* approach to identity management, because it is specifically targeted at internal use within a particular application or organisation. A user seeks to access multiple applications, servers or sites within a single organisation, hence the relationship is 1 user to 1 identity management system enabling access to a number (n) of applications, servers or sites, within 1 organisation. This pattern, represented in the sub-section heading as 1-to-1-to-n-in-1, will be used again in subsequent sub-sections in order to differentiate among the various contexts.

### 3.3 Single-Signon to Multiple Organisations (1-to-1-to-n-in-n)

The 'single-sign-on' concept originated within organisations, but is capable of being applied across multiple organisations as well. A user seeks to access multiple applications, servers or sites within multiple organisations, hence the relationship is 1 user to 1 identity management system enabling access to a number (n) of applications, servers or sites in a number (n) of organisations. Exhibit 3.3 provides a graphical representation of such a scheme.

*Exhibit 3.3: Multi-Organisation Single-SignOn Identity Management*

Examples include .Net Passport, which is available for use by (currently) 40 organisations other than Microsoft, and AOL’s ScreenName, to the extent that it is used on sites other than those operated by AOL.

There are thought to be advantages in the performance of identity authentication by one organisation on behalf of many services and organisations. The argument is based on the same reasoning as outsourcing more generally: that economies of scale can be achieved, that a single service that supports many organisations will be less expensive to establish and/or less expensive to operate than would multiple services each supporting a single organisation; and that therefore
organisations can save money by sharing among collaborating organisations, or by using a service provided by a third party.

The 'economies of scale' justification is intuitively appealing, and is sometimes justifiable. However, it is not clear that much investigation has been performed into the validity of the assertion that economies of scale are available generally or only under particular circumstances. Hence the movement is at risk of making the same misjudgements as the outsourcing movement before it.

### 3.4 A Comprehensive Inhabitant Registration Scheme

Another business driver for identity management schemes has been social control. National security has become a mantra since 12 September 2001. The focus on authentication and authorisation in such locations as airports has given fresh impetus to the recurrent question as to whether a general-purpose identifier should be imposed on the whole population. Logically, a 'comprehensive' scheme would apply to individuals worldwide, and could be used by all applications in all organisations (i.e. in principle, it is merely the extreme case of single-signon across multiple organisations). In the absence of world government, the scope of discussions to date has been mostly confined to nation-states, or to regional groupings such as the European Union.

Inhabitant registration schemes exist in some countries, and could be extended to support network access. Those countries that do not have such schemes could create them, as the United Kingdom government is currently considering, and Ireland, Canada and New Zealand are toying with. New schemes would be likely to be devised to encompass network access. Background to such schemes is in Clarke (1987, 1994 and 1997b).

The challenges involved in such an initiative are enormous. Some of the challenges are technical, and go to the questions of physical practicality and economic feasibility. Some are psychological, social and political, because the concepts of freedoms and democracy are seriously harmed by the imposition of a comprehensive, general-purpose scheme. See Clarke (1988). Although schemes of this nature arise in discussions, they are impracticable for the time being at least, and the focus needs to be on schemes that are capable of being implemented.

### 3.5 Closed-Community Schemes

An alternative is to be less ambitious in terms of the coverage, of the extent of applicability, and/or of the assertion that is being authenticated. More limited schemes have enjoyed some success in restricted contexts such as Extranets, electronic meetings conducted by associations, electronic voting in association elections, and professional communities such as medical specialists within a limited geographical region.

There is scope for these islands to be bridged. But this raises all of the familiar problems that are summed up by the term 'inter-operability issues'. The nature of the token varies, and so do the processes whereby it reaches the relying site.
The approach taken to pre-authentication also varies enormously among schemes, and even within each scheme the approach may not be applied consistently, and may not be subject to adequate controls. Most critically, the nature of the business that is being conducted may vary enormously. As a result, there are likely to be widely varying risks, and the risk/cost trade-off appropriate for one participant is unlikely to be appropriate for others.

3.6 'Federated' Single-Signon Services (1-to-n-to-n-in-n)

One particular approach has generated most of the publicity, and has consequently sometimes been (incorrectly) assumed to be the sole category of identity management schemes. This is the provision of services by multiple organisations, such that a relying site may accept a user that has been authenticated by any of a range of participating identity management service providers. Hence the relationship is 1 user to a number (n) of identity management systems, enabling access to a number (n) of applications, servers or sites in a number (n) of organisations.

(1) The Basic Proposition

The identity management services may be offered by organisations such as Microsoft and AOL that use the services themselves as well as making them available to other relying parties. They may also be offered by specialist third-party service providers. Exhibit 3.6-1 provides a graphical representation of such a scheme.

Exhibit 3.6-1: Federated Identity Management

Generally it is envisaged that each relying organisation would manage the authorisations that are associated with the authenticated identity. On the other hand, some of the proposals go beyond mere authentication, envisaging that 'user attributes' and 'user preferences' would be passed as well.
In order that relying parties can use multiple identity management services, a considerable degree of commonality must be established among them. Because commonality requires compliance with agreed technical standards and commercial conditions, the term 'federated' is applied to such schemes. A popular definition of 'federated identity management schemes', attributed to the Burton Group, is "the agreements, standards and technologies that make identity and entitlements portable across autonomous domains".

The benefits are seen as including not only the usual:

- convenience to users of being able to use a single username/password pair on multiple sites;
- support for sites to customise and personalise their services based on the profile associated with the username; and
- cost-savings arising from a shared scheme;

but also:

- additional cost-savings arising from the sharing of costs across multiple schemes (whether achieved through 'knock-for-knock' agreements or cross-charging among participating sites);
- greater focus by most organisations on their distinctive competencies, by outsourcing the identity management and authentication processes to a range of other organisations for which it is a specialty; and
- user choice as to which service they use to provide them with their widely-applicable username/password pair.

(2) The Business Architecture

The notion has a strong commercial driver. The organisations that already have significant communities of authenticated users can leverage off their user-bases, by referring those people onwards to other sites. This is to some extent a revival of the flagging 'portal' concept. Microsoft can on-sell its Hotmail and MSN users, and gain referral and commission fees. AOL and Yahoo can do the same with their users. So can airlines, car-hire companies, Amazon, eBay, and every other web-site that has 'captive eyeballs' and that can perform e-introductions by intermediating a connection between their users and other web-sites.

Considerable negotiation is necessary in order to launch such services. The range of topics on which agreement is necessary include:

- standards and protocols in order to achieve technical inter-operability;
- procedures for pre-authentication and authentication;
- commercial matters such as fees and audits;
- regulatory matters such as trade practices / anti-trust, consumer protection and privacy laws; and
- contingent matters such as risk-allocation, warranties and indemnities.
The approach assumes that the design decisions made by the identity management service providers are satisfactory for the organisations that are intended to rely on them, and for the subjects who are required to use the services to authenticate themselves. The diversity of contexts, requirements and expectations suggests the need for a range of levels of service, supported by a range of pre-authentication procedures and a range of authentication mechanisms.

For example, risk assessment for some applications is likely to conclude that authentication can be performed by means of a simple password scheme. For many, however, passwords need to be of sufficient length, and not easily discoverable using dictionary attacks, and need to be passed across encrypted channels. For a small number of applications, the risks involved may justify the trouble and expense of one-time passwords transmitted securely; of digital signatures generated using private keys subject to (inherently insecure) software protections; or of private keys subject to hardware protections.

The number of points on which agreement must be reached is substantial, for even the simplest federated scheme. The scale is much greater if multiple levels of service are offered. A federated scheme accordingly needs a policy information clearing-house or registry.

Multiple bilateral negotiations among the parties would result in Babel. It is therefore essential that multilateral approaches be adopted. In some cases existing industry associations have been used (e.g. OASIS, Internet2 and the Open Group). In addition, new associations have been formed to provide fora for such multilateral negotiations (e.g. Liberty Alliance, SourceID, PingId and the Web Services Federation).

(3) The Technical Architecture

Virtually all of federated schemes are based on the presumption that the Internet and Web provide the infrastructure over which the scheme is to be built. But there is a variety of ways in which the message-flows and message-content could be implemented. New communications protocols and message-format standards need to be agreed, so that software can be constructed and its behaviour tested for conformance with those protocols and standards.

Emergent federated architectures can be depicted as hierarchies of application layers built over the top of the Web and Internet. As in so many other aspects of information technology, the old adage holds: 'standards are nice because there are so many to choose from'. The examples in Exhibit 3.6-2 refer to multiple standards activities that are at best loosely affiliated, and at worst directly competitive and incompatible.

Almost all proposals rely on lower-layer protocols that are well-established (HTTP, HTML, XML), and many rely on mid-level protocols that are some distance down the path towards stable specifications (SAML, SOAP).
Exhibit 3.6-2:
The Protocol Hierarchy for Federated Identity Management

- **High-Level Identity Management Protocols** (in particular Liberty Alliance and WS-Federation, generally expressed in XML):
  - using **Standardised Message Formats** between remote devices. For example, Liberty Alliance and Shibboleth use Security Assertion Markup Language (SAML), which is in turn expressed in XML; whereas WS-Federation proposes its own specification
  - using an **Identity Exchange Protocol** for web-services actors (such as XNS)
  - using a **Data Release Protocol** based on a language for expressing policies and guiding the computation of permissions and denials (such as APPEL and EPAL, discussed below)
- **Process Invocation on Remote Devices** – in many cases using Simple Object Access Protocol (SOAP), which is also expressed in XML
- **World Wide Web Message Transfer** – in all cases using HyperText Transfer Protocol (HTTP) and the Domain Name Service (DNS)
- **Internet Transmission Protocols** – in all cases using either Transmission Control Protocol / Internet Protocol (TCP/IP) or User Datagram Protocol / Internet Protocol (UDP/IP)

Most of the action is at the most abstract level of data and process definitions. The Liberty Alliance and WS-Federation are essentially parallel initiatives. Liberty Alliance was formed to provide a counterweight against the perceived competitive threat of Microsoft’s Passport, and comprises scores of large, medium and small companies. Microsoft later retaliated with a separate alliance that features a small number of very large players. During 2003, the two alliances have been fighting for dominance and for endorsement by various other industry associations and standards bodies. A comparison between the approaches is provided at Liberty (2003c).

The message formats relating to identities need to be exchanged, and that requires a standardised protocol. An example of such a protocol is Xtsensible Name Service (XNS), which is "an open, XML-based [peer-to-peer] protocol for identifying and linking any resource participating in any kind of digital transaction" (XNS 2003).

A further language is required that can enable delegated decision-making about access to personal data held by an identity manager. A draft specification for such a language is W3C’s ‘A P3P Preference Exchange Language’ (APPEL). This is "a language for describing collections of preferences regarding [data accessibility] policies between ... agents. Using this language, a user can express her preferences in a set of preference-rules (called a 'ruleset'), which can then be used by her user agent to make automated or semi-automated decisions regarding the
acceptability of machine-readable privacy policies from P3P enabled Web sites” (W3C 2002).

Another draft in the same family is Enterprise Privacy Authorization Language (EPAL). It originated in IBM’s Zürich research laboratories, but had been submitted to W3C. EPAL is intended to complement APPEL, in that APPEL is for negotiations between agents for the requestor and the identity manager, whereas EPAL is 'a fine-grained enterprise-internal privacy policy language' intended for internal use within organisations (W3C 2003).

(4) Practicability

The business and technical architectures for the federated approach to identity management bear a resemblance to that which was attempted for certification authorities (CAs) for inter-operable public key infrastructure (PKI). That round of investment largely failed. That failure needs to be examined, to see whether there may be aspects of the architecture which are untenable in practice.
4. Demand-Side Architectures and Products

Almost all of the momentum in the identity management arena has been, and continues to be, generated by information technology providers. The marketing activities target the clients for their services, who are perceived to be the owners of web-sites. There is, on the other hand, little evidence of demand-side involvement in any of the identity management initiatives considered in the previous section. This is further discussed in section 6.4 below.

This section considers a number of other schemes and research projects, which are driven by the needs of consumer/citizens rather than the needs of business and government. Such schemes adopt the perspective of 'user-centric identity management', a term used in Koch & Woerndl (2001).

The section commences by considering the users' interests. It then expands the range of architectures beyond that contemplated by the business-oriented schemes discussed in section 3. This is followed by discussions of two categories of tool, one of which is user-controlled through contractual arrangements, and the other of which is directly under the user's control. Consideration is also given to the scope for individuals to obscure their identities and data, and to subvert schemes run by business and government.

4.1 Consumer/Citizen Interests

Individuals are concerned about the exercise of power over them by others. In some cases, the 'others' are individuals, such as relatives, neighbours, stalkers, and competitors in various walks of life. In many cases, the 'others' are corporations and government agencies.

In all such cases, information in the hands of those 'others' increases the power that those 'others' can exercise. In the case of organisations, that power is often already substantial, because of their size and access to resources, their 'market power' (in the case not only of consumer marketing corporations but also of monopoly providers of goods and services within government), and their statutory powers (in the case of government agencies performing social control functions). Individuals therefore have an interest in exercising control over information about themselves, and often in denying it to other parties.

The last century has seen increasing data-intensity in administrative procedures. One of the most effective protections against that data-intensity has been the compartmentalisation of people's lives into many roles, and the accumulation of data about those roles in separate collections. Conversely, one of the greatest threats to individuals is the breaking down of those compartments. The correlation of people's many identifiers, and the imposition of multi-purpose identifiers, are two of the most significant vehicles whereby organisations can enhance their power over individuals (Clarke 1988, 1994, 1997b).
The interests of consumer/citizens therefore lie in retaining control over identifiers and other personal data, and over decisions to release identifiers and other data to other parties.

4.2 An Extended Set of Architectural Alternatives

A vital aspect of control over identifiers and personal data is the combination of the location of the device that stores the data and performs the functions, and the organisational control over the device and data. Exhibit 4.2 identifies a range of alternatives. Numbers 1-3 are business-centric, and were addressed in the previous section. Numbers 4 and 5 are user-centric and are addressed in this section.

Exhibit 4.2:
Alternatives for the Location and Control of Devices and Data

1 **Physically Centralised Identity Management.** This features central storage, under the control of a single organisation. This is the approach adopted by Microsoft Passport, as discussed in sections 2.4(2) and 3.3, and by inhabitant registration schemes as discussed in section 3.4. Social control objectives dominate, and user choice is very limited, because the conditions are dictated by the company or government agency. On a large scale, however, this approach is technically impracticable because of the performance bottlenecking and fragility it would entail.

2 **Virtually Centralised Identity Management.** This involves geographically distributed storage, but still under the control of a single organisation. For example, in some countries such as Switzerland and The Netherlands, the national data register is operated at local government level; and Microsoft could choose to hold Passport holder data regionally (e.g. in order to achieve network-resource efficiencies, robustness and resilience; to address national sovereignty concerns; and to enable personal data to be handled in manners consistent with local data protection laws). Social control still dominates personal choice.

3 **Federated Identity Management.** In this case, the storage is geographically distributed, and the devices and data are controlled by different organisations, but within a common architecture. This was examined in section 3.6 above. Some choice exists, but social control still dominates, and the primary beneficiaries of the design are the organisations that sponsor it and the organisations that arrange for access to the identifiers and data.

4 **User-Selected Intermediary Identity Management.** This also features storage that is geographically distributed, and devices that are controlled by different organisations within a common architecture; but in this case the data is controlled by the individual. Service providers might be government agencies, the person’s Internet Access Provider (IAP), or Internet Service Providers (ISPs) more generally, possibly network-distant from the individual. This establishes a degree of user choice, but at the cost of some
compromise to social control objectives. This alternative is examined in section 4.3 below.

5 **User-Device Identity Management.** Under this arrangement, the identifiers and data for each individual are stored on dispersed devices that are under the physical and logical control of that person. A common architecture is essential, to enable users’ devices and remote services to converse and negotiate. Section 4.4 examines several variants of this approach. They offer advantages for consumer/citizens, but at some cost to social control interests.

In each of the 'user-centric' alternatives (4 and 5), an organisation seeking access to authenticate a user, or to acquire an identifier or other personal data, would have to negotiate that access with the user's agent. Provision needs to be made for authority-of-law access, and this in turn needs to be subject to controls such as checking of the validity of an agency demand, or of a court order such as a search warrant.

The following sub-sections examine schemes and projects that can be categorised into the user-centric alternatives.

### 4.3 User-Selected Intermediaries

The federated approach described in section 3.6 above is heavily oriented towards the needs of business and government; but a very similar architecture can be applied to suit the users instead, or as well. An early examination of the scope of this approach was undertaken by Hagel et al. (1996, 1997, 1999), who coined the term 'info-mediaries' for service providers that were hired by consumers to provide intermediary services between the consumer and organisations. Exhibit 4.3 provides a graphical representation of such a scheme.

**Exhibit 4.3: Identity Management by a User-Selected Intermediary**
A commercial offering that evidences some aspects of this architecture is Ascio's Digital Identity. This stores personal data for open display on web-pages, and includes the capacity to store username/password pairs. It is limited to a singular, unauthenticated identity associated with a personal web-site and email-address, in effect with the registrant recorded in the domain name system (DNS) for that domain. Another example is Yodlee, which presents itself as an account aggregator, but performs similar functions. Privacy Inc's MPP operates a proxy-server and provides users with interaction-specific email-addresses.

This market segment does not, or at least not yet, appear to have achieved much success, because several other services have come and gone, including Privada, privaseek/persona and iFay. One explanation may be that "[although they] support clustering users and making the information about the affiliation to clusters available for personalisation ..., these services either do not offer sufficient user control or are too concentrated on marketing and personalisation issues so that they cannot be used for configuration or initialisation" (Koch & Woerndl 2001).

An open-source initiative, Nareau Sunshine, driven by Rahul Dave of the University of Pennsylvania, describes identity in the following terms: "The 'identity' is the unit of interaction with the platform. Users may bind identities to devices, or to the persona's they assume in their lives. I may prefer a lower grade security identity when logging on from internet kiosks. To protect my privacy while surfing, I may want to use a pseudonymous identity. At porn sites, I may want to be anonymous. For my workplace, I am likely to have a different persona, with different roles and responsibilities than at my ISP. The identity management system must allow a user to manage all their personas".

Another project that appears to provide a user-controlled proxy-server supporting multiple relationship-specific pseudonyms, and perhaps anonymity, is IBM Zürich's Research Laboratories' idemix.

4.4 Own-Device as Identity Manager

The essence of this architectural approach is that the user's exposure of identifiers and of personal data is entirely under their own logical control, and the identifiers and data are stored on a machine that is under their own physical control. There are two variants, which are described in the following two sub-sections.

(1) Own-PC Identity Managers

At the most simplistic level, the user operates from a single PC or workstation, and can manage their identities on that device.

A number of partial implementations have been in existence for some years. Email clients enable a sender to sculpt their identity, as disclosed by headers such as From: and Reply-To:. Web-browsers permit users to create multiple ' personas', and to select which to present to a web-site. Cookie-managers can enable some manipulation of apparent identity (e.g. by denying cookies, and
thereby making each visit appear to be the first by a new user). Exhibit 4.4-1 provides a graphical representation of such a scheme.

Exhibit 4.4-1: Own-Device Identity Management

Another example of a product that runs on the user's machine is Novell's digitalme. This enables the person to store personal data, and release selected segments of it to others. It provides a repository for username/password pairs for remote services, which it claims can be accessed with a single click.


The systems software on consumer devices has been to date seriously insecure. Microsoft's security initiative, initially code-named Palladium and now 'Trusted Computing', is fraught with difficulties, because it attempts to overlay security features over a seriously insecure base, and because the company is building a great deal of spyware into its products, and seeking ways to make users more dependent on and integrated with remote services. The steadily increasing availability of *nix operating systems, through the BSD-based Mac OSX, and BSD and Linux distributions, may offer more promise in terms of addressing the vulnerabilities of personal devices.

(2) Own-Proxy Identity Managers

The notion of one-person/one-device was only ever applicable to a proportion of people, and has quickly become outdated. Many people already use more than one device, some at work and at home, others in airport lounges, and others again in Internet cafes and public libraries. Portable and handheld PCs added to the brew. Consumer products such as mobile/cell-phones, cameras, playstations and music-players are merging with handhelds to produce various kinds of
hybrid device, any and all of which may be the user's means to connect with remote services.

Wireless networks are no longer only wide-area (cellular and satellite), but also local (e.g. WiFi) and personal (e.g. Bluetooth). A review of wireless transmission and mobile technologies is at Clarke (2003a). Mobile/cell-phones can be rented on arrival at airports, and handsets can be personalised (or, indeed, pseudonymised or perhaps even anonymised) depending on the SIM-card that is inserted. Near-future Internet usage features not only mobility but also plurality of a person's access-points, both over time and at the same time.

Within closed corporate networks, it has long been essential that individuals be able to operate from multiple devices in multiple locations. This requirement now exists for consumers as well. The user needs to have their identifiers and data available to them on whichever device they happen to be utilising to access remote services. And to the extent that this involves replication of content, there is a need for real-time content synchronisation.

People who have a home network and a host performing intermediating functions as a hub or router are well-positioned to implement servers on that device, including a proxy-server to intermediate between their browser and the remote web-server. Critical to the proxy-server functionality would be an identity management server. Exhibit 4.4-2 provides a graphical representation of such a scheme.

**Exhibit 4.4-2: Own-Proxy Identity Management**

![Identity Management Diagram]

It is also feasible for the function to be located on machines managed by ISPs, but with measures in place to prevent the ISP from having access to the data it stores, from interfering with the function, and even from being aware of the function being performed. The more involved the ISP becomes in the function, the more the approach resembles alternative 4 – identity management by an intermediary.

The advent of personal area networks such as Bluetooth suggests that each individual will carry an intermediating device functioning as their personal hub,
router and proxy-server, perhaps clipped to their belt, or intrinsic to their belt-buckle or necklace. One potential solution to the problem of how to manage access to the user's identity data is to include identity management functionality within that proxy-server.

Another approach is for every device to be capable of being personalised by means of an external device. To provide security, this needs to be a computer, most likely a chip housed in some conveniently portable carrier such as a 'smartcard', watch, bracelet or ring. The 'personaliser' could be physically connected to the device (e.g. using a smartcard reader, or through a USB port), or could communicate with the device by wireless means (e.g. using a connectionless smartcard or RFID tag and infra-red or WiFi-spectrum radiation).

There do not appear to be any products currently available which directly target this emergent market. On the other hand, user-centric identity management servers such as Nareau Sunshine could be as easily run on a device under the control of an individual as on a device hosted by an ISP.

4.5 Nymity Services

A wide variety of services is already available which operate as proxy-servers on the user's behalf, and thereby enable interactions to take place between the user and a remote service without disclosing the user's IP-address. The user's net-location is obscured from remote services, and the identities of the remote services that the user is accessing are obscured from the user's ISP.

The term used for such functionality is usually 'anonymity services'. Whether that term is appropriate, or whether it should instead refer to 'pseudonymity', depends on the manner in which the service is implemented. At one extremity, those based on mix networks (Chaum 1981) can achieve effective anonymity; whereas those which involve a single proxy-server with logs of inbound and outbound traffic are properly referred to as being pseudonymous. These aspects are further considered below.

Well-known nymity techniques and services include Crowds (Reiter & Rubin 1997), Onion Routing, Anonymizer, and Freedom WebSecure. Use of nymity services is in some cases bundled with other personal security tools, e.g. in GhostSurf. Lists of nymity services are maintained by a number of people, including EPIC and Russ Haynal.

Depending on the pre-authentication procedures that they conduct, remote services, and business-oriented identity management services, may detect the use of proxies and anonymisers, and adopt countermeasures against them. Despite this, nymity services may have a significant role to play in protecting users' privacy, should the approaches to identity management schemes examined in section 3 make real headway.

4.6 Identity Management Subversion Tools

Corporations and government agencies can establish countermeasures against known techniques used by individuals to obscure their identities and data. But
countermeasures can be adopted by individuals too, in order to work around various aspects of identity management schemes.

To ease the onerousness of submitting applications, web-forms can be filled with pre-recorded data; but they can be just as easily (or even more easily) filled with convenient data (such as the first choice in the list of choices provided by the site), with pseudo-random data, or with intentionally erroneous data. Personal data can be automatically varied for each remote service, in order to detect data-leakage, e.g. through spelling-variants of name and address and numerical variants of date-of-birth.

Data can be automatically varied for the same remote service on successive occasions (to pollute the remote service's data-store and hence confuse the user-profile the organisation is developing). Another approach is for users to exchange cookies, such that data aggregators end up with compound profiles rather than profiles that actually reflect an individual user's behaviour. One example of such a product is Cookie-Cutter. Others are catalogued by sites such as EPIC.

Tools of this kind can be used in an endeavour to undermine the social control objectives of any of the business-oriented identity management architecture discussed in section 3, and in conjunction with nymity services. Of course, business and government organisations can also apply countermeasures against some of these countermeasures. Some that have been used in the pre-Internet world continue to be applicable in the Internet context, such as data-scrubbing, front-end validation of submitted data, and data matching.
5. The Multi-Mediated Super-Architecture

The preceding sections have described a diverse set of architectures for identity management services. There is a high probability that products and services will be deployed using most if not all of them.

It is therefore inevitable that identity managers will come into conflict: users will depend on their agents to perform the function, running variously in their personal devices or proxy-servers; but the web-sites they are seeking access to will rely on one or more identity managers of the site-operators' choosing. Exhibit 5 provides a consolidated graphical overview of the multiple approaches to identity management.

As this complex super-architecture emerges, there will be a desperate need for mediation among the various competing identity managers. This will require application of agent negotiation principles (Rosenheim & Zlotkin 1994), and enhancements to standards and protocols.
Exhibit 5: The Multi-Mediated Super-Architecture

- Own-Device I.M.
- Own-Proxy I.M.
- User-Selected Intermediary I.M.
- Federated, Multi-Organisation Single-SignOn I.M.
- Silo’d Single-Organisation Single-SignOn I.M.

Identity Management Service

The Organisation’s Applications and Web-Sites
6. Conceptual Inadequacies

This section examines the concepts that underlie identity management schemes. The documentation that describes the various services shows widely divergent interpretations of those concepts. Usages differ considerably not merely between organisations, but even within the same scheme, the same document, and sometimes the same paragraph or sentence. This section accordingly also highlights many conceptual misunderstandings embodied in current identity management schemes, and the wide range of practical problems that arise from those misunderstandings.

The section commences by examining 'authentication', and then the substantial cluster of concepts associated with 'identity' and 'identifier'. This leads to discussion of the processes of 'identification' and 'identity authentication'. A final sub-section discusses the questions of natural versus legal persons, and of principals and agents.

6.1 Authentication

The term 'authentication' refers to a process whereby confidence in some assertion is gained, or the degree of confidence that is justified about the truth of some assertion is assessed. The concept has nothing to do with 'identity' in particular; it relates to assertions of all kinds.

It is an unfortunate accident of the history of applied cryptography that a specialised usage of the term by computer scientists was carried over into the eBusiness world, with the result that 'authentication' has been widely used for the last five years to mean exclusively what the term 'identity authentication' much more precisely denotes. As a result, a great deal of discussion in this area commences with a misguided assumption inherent in the language used. The following sub-section raises questions about the term 'identity', and suggests that a much deeper appreciation is needed in that area as well.

An example of this error is in the OASIS Glossary, which defines authentication as being "to confirm a system entity’s asserted principal identity with a specified, or understood, level of confidence" (OASIS 2002).

Even more confusingly, Liberty Alliance defines authentication as "the process of verifying the ability of a communication party to "talk" in the name of a Principal", where 'Principal' means "an entity that can acquire a federated identity, that is capable of making decisions, and to which [sic – for which?] authenticated actions are performed on its behalf" (Liberty Alliance 2003e, pp. 28, 29).

The effective conduct of eBusiness is dependent on the reliability of a range of assertion-types sometimes involving identity, but often involving value or attributes (Clarke 2001b). Unfortunately, most organisations fail to conduct risk assessments, and hence fail to clarify, in their particular context, what the assertions are that are most in need of authentication.
The process of authentication tests the truth or reliability of the assertion in question. It depends on evidence. A useful term for an item of evidence used for this purpose is an 'authenticator'. RFC2828 (IETF 2000) uses the alternative but more restricted term 'authentication information' to refer to "information used to verify an identity claimed by or for an entity". Categories of authenticator include:

- demonstration of knowledge, or provision of information that is only supposed to be known by the (or an) appropriate person (e.g. a password or other shared secret);
- demonstration of the ability to perform a particular act (e.g. execute a written signature that bears a resemblance to a prior copy, or generation of a digital signature that decrypts to the appropriate value using a particular public key);
- acquisition or production of a 'credential', discussed below, which has two important sub-categories:
  - 'document'; and
  - 'token'.

The term 'credential' refers to a particular category of authenticators, specifically those that have physical or digital existence (as distinct from the actions of demonstrating either the possession of information or the ability to perform an act).

Where scheme documents define 'credential', the scope of the term is inappropriately broad. Liberty Alliance defines a credential as "known data attesting to the truth of certain stated facts" (Liberty 2003b and 2003e, pp. 28). This is equivalent to the meaning of the restricted term 'authentication information' as defined by RFC2828 (IETF 2000). OASIS makes the same mistake, defining credential as "data that is transferred to establish a claimed principal identity" (OASIS 2002).

One kind of credential is a 'document', which is writing or printing on paper, or its equivalent in digital form. Physical examples include letters of introduction, birth certificates, drivers' licences, statutory declarations, and invoices. Digital documents are increasingly being used, e.g. an emailed confirmation from a previously registered email-address, and an emailed copy of a facsimile of a university testamur.

A 'token' is a particular form of a credential that is designed to provide a relatively high level of confidence in an assertion. A credit-card may be regarded as being more than just a document, because it bears a copy of the signature. A card that appears to have been issued by an employer may be regarded as a token rather than a mere document, particularly if it carries a photograph of the employee. Turnaround documents are such a token (e.g. the tear-off strip at the bottom of an invoice, intended to be returned with the payment). So are tickets for sporting and entertainment venues, and tickets issued to people waiting in a queue. So too is a smartcard carrying either or both of the bearer’s private digital signature key or biometric.
The degree of confidence that is engendered by an authentication process is commonly referred to as 'authentication strength'. Strength derives from a combination of the support that the evidence provides to the assertion, and the degree of likelihood that the evidence is in error or has been intentionally created in order to procure a desired outcome. The Liberty Glossary uses the term 'authentication quality' in a similar manner, to mean "the level of assurance that a service provider can place in an authentication assertion it receives from an identity provider" (Liberty 2003b).

As was noted earlier, the authentication strength of the majority of identity management schemes is undermined by the failure to specify and control pre-authentication procedures. In many cases, there is also little attention paid to the security of passwords or private keys in the possession of users.

6.2 Entity and Identity

Human identity is an excruciatingly complex notion (Clarke 1994). The documents that explain identity management schemes provide ample evidence that the designers have very limited appreciation of that complexity. This and the immediately following sub-sections provide a brief review of the key ideas.

Information systems of all kinds adopt the philosophical position that there is 'a real world' of physical existence, and 'an abstract world' of information. In the real world, actors of various kinds perform actions. Conventional terms used in this sphere are:

- 'entity', which refers to any real-world thing, but especially things with the ability to act as well as to be acted upon, such as people and organisations;
- 'event', which refers to an occurrence in the real world; and
- 'attribute', which refers to characteristics of entities (such as name and age) and of events (such as the time at which they occurred and their duration).

Entities may present in many contexts, and play many roles. Each such presentation of an entity is an 'identity', i.e. an identity exists in the real world. A car may present as the next one in the queue at a toll-booth, the winner of a race, the one being driven by a particular person at a particular time, or the unknown vehicle that sped away from the scene of a particular crime. People perform many roles, within work, home and community contexts. Business enterprises act in many markets, and project themselves by means of multiple business names, logos and brands.

Liberty Alliance Glossary defines 'identity' as "the essence of an entity and often described by its characteristics" (Liberty 2003b, 2003e p.29). This is very different from the definition provided in this document, and far less useful, because:

- an entity may have more than one identity associated with it (and, in most cases, it does); and
- the notion of 'essence' is unduly ethereal and mysterious, whereas 'presentation' draws attention to the idea of a role being played, or mask being worn.
Yet Liberty Alliance then defines 'identity federation' without even mentioning 'identity'. It instead refers to an 'account', which, as explained below, are an abstract-world rather than a real-world notion.

The Liberty Glossary also defines the term 'network identity' as "the abstraction of the global set of attributes composed from all of a Principal’s existing accounts" (Liberty 2003b). This confuses real-world attributes with abstract-world data-items and accounts. It also explicitly denies multiple identities, because it envisages the data-items being drawn from all accounts.

Many scheme documents fail to define 'attribute'. OASIS refers to it in a manner consistent with the usage in this document, as "a distinct characteristic of an object" (OASIS 2002). The Liberty Glossary similarly defines attribute as "a distinct characteristic of a Principal"; but its definition of 'attribute class' as "a predefined set of attributes, such as the constituents of a Principal’s name (prefix, first name, middle name, last name, and suffix)" demonstrates confusion between real-world attributes and abstract-world data-items (Liberty 2003b).

These confusions in Liberty Alliance’s use of terminology are already so great as to throw doubt on whether the scheme’s design could possibly satisfy the needs of the organisations it is meant to serve.

6.3 Data Representing Entities and Identities

Information systems 'capture' (i.e. express in recordable form) data about selected real-world entities, events and attributes. These expressions (in the sense of the recording on paper or in magnetic form) are part of the real world; but what they convey – the data – is part of the abstract world. The value of the expression in data lies in our ability to manipulate it, store it, recover it, and draw conclusions from it about the real world, and about what actions we should take in the real world.

Each entity and identity is reflected in one or more 'records' or data-sets. An event has its abstract-world correlate in a 'transaction'. The selected attributes of entities and identities, and of events, are mirrored in the 'data-items' that make up respectively the records, and the transactions.

Among the data-items, some may be of particular significance, in that they may enable an observer to distinguish one or more records as being associated with a particular real-world entity or identity. A useful term for such sets of data-items, made popular by relational modelling theory, is a 'candidate key'.

An example of a candidate key for a motor vehicle entity is the combination of make, model, year, colour and pattern of dents in the bodywork. Other, much more administratively convenient examples are the serial numbers recorded on the externally-visible registration-plates, the engine, and the chassis. For a human entity, candidate keys include patterns of behaviour, mannerisms, overall appearance, and, more precisely, biometrics.

Candidate keys are used to distinguish not only entities of the same class (such as cars and humans), but also identities of the same class (such as presentations of cars, and roles played by humans such as customers and employees). For
identities associated with human beings, candidate keys include names assigned by people (variously their parents, their friends and themselves) and codes assigned by organisations.

The common term for a candidate key for an identity is 'identifier'. A rare instance of a clear definition of identifier is provided by OASIS: "a representation (for example, a string) mapped to a system entity that uniquely refers to it" (OASIS 2002).

It is indicative of longstanding muddy thinking that there is no commonly-used term for a candidate key for an entity (apart from the unhelpfully ambiguous use of 'identifier'). The term 'entifier' is an obvious possibility. An entifier for a human being is by definition a biometric. A possible entifier for a device is a processor-ID, or perhaps a proxy such as the identifier of the network interface card installed in it (in particular, an Ethernet NICId).

An organisation manages an external party's access to data and services by means of an 'account'. Remarkably, glossaries are almost entirely silent about what is meant by this much-used term. An 'account' is a set of data-items that defines the relationship between two parties. The data-items include:

- an identifier, as defined above (generally a username);
- one or more authenticators, as defined above (most commonly a password);
- an entry in an access control list that expresses the permissions associated with that identifier, which enable access to system resources such as data and software; and
- any relevant descriptive data-items. These are commonly referred to collectively as a 'profile' (or 'preferences', 'settings', or other equivalent terms).

An extended interpretation of 'account' may contain a trail of transaction data generated as a result of interactions, especially interactions between the two parties.

The authors of the documentation describing identity management schemes appear in most cases to be entirely ignorant of even the basic notions, let alone the many subtleties that have been drawn to attention in this sub-section. It is common to see the term 'identity' used to mean all of what was defined above to be 'entity', 'identity', 'identifier', 'entifier', 'record' and 'account'. Sometimes the intended meaning is clear, even though the word is used in a different sense elsewhere in the same document, section or even paragraph. For the most part, however, scheme documentation evidences problems that are not merely semantic, but rather are a result of a failure to think through the problems at hand, and to establish a model rich enough to support the design.

A quotation that is indicative of the problem is as follows: "'Network identity' refers to the global set of attributes that are contained in an individual's various accounts with different service providers" (Liberty Alliance FAQ). This fails to distinguish real-world 'identity' and 'attribute' from abstract-world 'identifier'
and 'data-item', and compounds the problem by using 'account' without making clear what is meant by the term.

The issue is yet further confused when Liberty Alliance uses the term 'trait' in a manner completely foreign to dictionaries, and refers to 'credentials' issued by governments as 'identities'. Liberty (2003c), although classified as a 'White Paper', is particularly seriously flawed.

Within another of the industry associations, confusion is evident in the definition of 'identity' as 'an identifier that is held in or presented to computer systems, and that identifies the person' (Open Group 2002, p.6). This definition is circular, it shows a failure to distinguish between the real and abstract worlds, and it uses one word to mean merely a restricted sub-set of the ideas encompassed by another (i.e. 'identity' is defined a sub-set of 'identifier'). Open Group appears, on the one hand, to recognise that "the number of identities could be from one upwards, possibly to over 100" (p.9); but, on the other hand, it says that "everyone has a unique identity" (p.13). This conflation of multiple ideas into one term reflects a serious lack of clarity of thought and modelling.

The Liberty Glossary is one of the few to mention the term 'account'. But it defines account as "a formal business agreement for providing regular dealings and services between a Principal and service providers" (Liberty 2003b). This fails to capture the elements that are critical for the implementation of infrastructure to enable the dealings to be undertaken.

These misunderstandings are deeply embedded in the schemes brought forward to date. It is not straightforward to work out what implications they have; but seriously flawed models and seriously inadequate language seldom lead to successful implementations.

### 6.4 Nymity

A party that wants to know who they are dealing with may encounter difficulties. The party may acquire an identifier for the other party, but be unable to reach back behind it to discover the underlying person's entifier. Where the linkage cannot be discovered at all, the appropriate descriptor is 'anonymity', and the identifier is categorised as an 'anonym'. Where the linkage can be discovered, but only if particular conditions are satisfied (e.g. a court order to gain access to an index), then the appropriate term is 'pseudonymity', and the identifier is a 'pseudonym'. The two kinds of identifiers are usefully referred to together as 'nyms', and the two conditions together as 'nymity'. For treatments of nymity, see McCullagh (1998-), Clarke (1999) and Köhntopp & Pfitzmann (2001).

The documentation relating to identity management schemes demonstrates considerable confusion about nymity among scheme proponents. OASIS uses the RFC2828 (IETF 2000) definition of anonymity as "the quality or state of being anonymous, which is the condition of having a name or identity that is unknown or concealed" (OASIS 2002). This definition evidences thoroughgoing confusion, and is a seriously inadequate basis for the design of an identity management service. It is clumsily expressed, and it confuses 'identity' and 'identifier'. But, most crucially, it misses the point that the identifier (the nym)
may be known, and indeed commonly is known. What is "unknown or concealed" is the linkage between the identifier/nym and the entifier of the underlying, real-world entity.

Liberty Alliance's Glossary includes no definition (Liberty Alliance 2003e, pp. 28-29); but the same document uses anonymity to refer to what is called in this document pseudonymity, e.g. "Anonymous Identity Protocols: ... a transient name identifier is given to the Service Provider for each session that the Identity Provider can map to its account for the Principal" (p. 20).

Some schemes acknowledge the existence of anonymity and/or pseudonymity, some even their inevitability, and a few even recognise their desirability; but most scheme sponsors are 'in denial', committed to the notion that identity managers genuinely enable their relying parties to 'know their customer'.

Exhibit 6.4, from Clarke (2001b), provides a graphical representation of the model and language that is needed in order to reflect the subtleties of human activities. Many scheme designs are unable to cope with those subtleties, resulting in serious restrictions on their applicability.

**Exhibit 6.4: A Model of Human (Id)entities and (Id)entifiers**

![Diagram of human (Id)entities and (Id)entifiers]

- **Record:**
  - **Entifier + Data-Items**
  - **Identifier + Data-Items**
  - **Nym + Data-Items**

- **Abstract World**
  - **Real World**

- **Entity and Attributes**

- **Identity and Attributes**

- Connections: 1:n, m:n
6.5 (Id)entification and (Id)entity Authentication

Most transactions in the real world are conducted between actors who have only a modest amount of information about one another. But in some circumstances there is a need or desire by one party or the other to 'know the identity of' the other. In the terms used here, one party 'acquires an identifier for' the other party. The term 'identification' refers to the process whereby data is associated with a particular identity through the acquisition of an identifier.

In a hitherto very small proportion of circumstances, one party or the other may have a need or desire to strike through the identity to reach the underlying entity. The party therefore 'acquires an entifier' for the other party (in the case of a human, a biometric), rather than an 'identifier'. Rather than using the term 'identification' ambiguously, it is preferable to use 'entification' to refer to the process whereby data is associated with a particular entity, by acquiring an entifier.

There may be a need for some level of confidence in the assertion that data is being associated with the right identifier. If so, then the assertion needs to be authenticated. The term 'identity authentication' refers to the process whereby confidence is established in an assertion of identity. It is performed by cross-checking the information available (the identifier) against one or more authenticators.

Authenticators for identity assertions are of various kinds. In the security literature, e.g. RFC2828 (IETF 2000), they are conventionally depicted as comprising:

- what the person knows (such as a password or PIN);
- what the person has (such as a document or token); and
- what the person is (i.e. biometrics).

This conventional list is seriously deficient, on two counts:

1. it omits the important category of 'things a person can do' (such as the act of providing a written signature, or pronouncing a shibboleth or test-word – Judges 12:4-6); and

2. it accidentally embeds within the class 'identity authentication' the very different notion of 'entity authentication'. The two are not equivalent, and the distinction can be very important. For example, the identity 'shift-leader', 'case-manager', 'purchasing manager' or 'agent for an institutionalised person' may be performed by different people over a long period of time, over a short period of time, or even at the same time.

The term 'entity authentication' refers to the process whereby confidence is established in an assertion of entity. It is performed through the acquisition of an entifier (in the case of a natural person, a biometric), and the cross-checking of that entifier against a pre-recorded copy of that entifier.

The treatment of 'authentication' in identity management scheme descriptions and specifications demonstrates inadequate appreciation of the registration or
enrolment process. It is vital to understand that, when a user seeks access to a remote service and authentication is performed, the assertion that is being checked is of the form 'I am a person who is permitted to use this account'; whereas the assertion 'I am the entity that underlies the identity that is represented by that identifier' is not something that can be authenticated in the context of logging into a web-site.

In circumstances where the identity really needs to be linked to the underlying entity, that function must be performed in the registration or enrolment phase. The term 'pre-authentication' is useful to distinguish the actions taken at that stage. The scheme descriptions are generally silent about the registration phase as a whole, and about the pre-authentication processes that are to be undertaken.

There is discussion in some schemes about the strength of the identity authentication process. There is a wide range of possible techniques, which have differing vulnerability profiles and hence are useful for addressing different kinds of risk. They can therefore give rise to widely varying degrees of confidence in the assertion. Available techniques include call-back, password (for which various techniques can achieve varying degrees of strength), protected password, weakly-protected digital signature key, multi-factor authentication, physical or digital token, one-time password, and strongly-protected digital signature key. The benefits need to be prioritised on the basis of a risk assessment, and balanced against other objectives such as cost, inconvenience and intrusiveness.

To the extent that confidence is needed in an assertion about a specific human entity, the far greater cost and intrusiveness of entity authentication has to be balanced against the benefits.

Given that the fundamental concepts are so poorly understood by sponsors of identity management schemes, it is no surprise that derivative terms also lack clarity of usage. The organisations that have devised existing identity management schemes have failed to develop an adequate appreciation of these aspects, and their designs consequently fail to accommodate them.

### 6.6 Natural Persons, Organisations and Agents

Almost all of the schemes make the assumption that the user is a natural person acting as themselves. This implies that they are not representing some other natural person, nor are they performing a role on behalf of a body corporate (i.e. a corporation, incorporated association, trust, or any other legal person recognised by law), or a body politic (such as a nation-state). In a few cases the assumption is explicit, but in most cases it is implicit, or appears simply not to have been factor considered by the scheme sponsors. The law formalises the capacity of one party (the 'agent') to act on behalf of another (the 'principal').

An approach that could be taken to this would be to focus on attributes of usernames rather than on the identities behind the usernames. A company, or indeed a high net worth individual, may well agree in contract to be bound by particular kinds of transactions entered into by any person who utilises a particular username to operate a particular account, subject to designated
authentication and security safeguards. But this scenario implies particular requirements of the registration process, and of the contracts, and of the nature of the assertion that is being authenticated when the user logs on. Those requirements are fulfilled by very few of the so-called 'identity management' schemes that have been deployed or proposed to date.

One scheme that does squarely address this issue is Identrus. This involves banks leveraging off their knowledge of their corporate clients by signing digital certificates that attest to their clients' public keys. At this stage at least, it is targeted specifically at B2B commerce rather than consumers.

There are early signs of maturation in some other schemes. For example, OASIS defines the term 'proxy' as "an entity authorized to act for another", which is very similar to the definition provided here for 'agent' (OASIS 2002); and the Liberty Glossary defines 'delegation' as "enabling a system entity to operate on behalf of a principal to access an identity service" (Liberty 2003b).

The lack of attention to organisations, to accounts, to attributes, and to principal-agent relationships, is further evidence that scheme sponsors have not achieved adequate conceptual understanding of the contexts of use of their services. Moreover, it suggests that they have either not performed meaningful risk assessments, have performed them at a highly superficial level, or have performed them but ignored the conclusions that they must have reached. Because of these conceptual inadequacies, the schemes' investors are far less likely to enjoy returns than they might have expected.
7. Social Impacts

The majority of this report has focussed on the conceptual foundations, architecture and technologies of identity management schemes. This section turns to the broader implications of scheme designs, and the extent to which projects have involved the users whose identities are intended to be managed.

The first sub-section considers the privacy aspects. This leads into discussion of two key privacy issues: each entity's multiple identities, and nymity. The final sub-section is concerned with participation in the conception and design of schemes by users, and by their representatives and advocates. The theme that emerges is that a lack of appreciation of human values represents a further and perhaps very significant barrier to the adoption of identity management schemes as they are currently envisaged.

7.1 Understanding and Valuation of the Privacy Concept

The documentation relating to schemes generally at least mentions privacy, and in some cases addresses it at some level of detail. There are some serious problems with the treatment, however. The following sub-sections discuss the severely limited conception of privacy that is evident in the schemes, the dominance of 'opt-out' mechanisms over consent, and the entirely justified lack of trust by consumers in the identity management schemes that have been released to date.

(1) Limited Conception of Privacy

The most substantial document in this area is Liberty Alliance's 'Privacy and Security Best Practices' document (Liberty 2003e). This states that privacy is "extremely important" (pp. 2, 4); but it also makes clear that "Liberty Alliance cannot and does not ... condition use of the Liberty Specifications on adoption of a particular set of fair information practices [nor] monitor, audit or enforce compliance with [anything]" (p.4).

Warm assurances such as "extremely important" are completely undermined by the extraordinarily limited conception of privacy evident in this and all other documents published by scheme sponsors. Exhibit 7.1 describes three kinds of limitations.

A further noticeable feature of the documents provided by scheme sponsors is that they commonly assert that privacy has to be compromised (e.g. "But the desire for privacy and individual dignity must be reconciled with the desire for effective government and with legal needs and national security needs" Open Group 2002, p.14). That assumption is shared with privacy advocates, because privacy is one interest among many. The point of concern is that scheme sponsors further assert that the actions of business and government merely need to be compliant with local laws. There is no acknowledgement that the interests...
of business and government agencies might also need to be 'compromised' against people’s psychological, social and democratic needs for privacy.

Exhibit 7.1:  
Inadequacies in Scheme Sponsors' Conception of Privacy

- The term 'privacy' is not used in its full richness, but only in the narrow sense of 'information privacy' / 'data protection' / 'fair information practices' (e.g. "proper handling of personal information throughout its life-cycle, consistent with the preferences of the data subject" – (Liberty 2003b) and Liberty 2003e, p. 29). There are multiple dimensions of the privacy interest (Clarke 1997). Identity management proposals have potentially significant impact on privacy of the person, privacy of personal behaviour, and privacy of personal communications, as well as on privacy of personal data

- Even within that narrow sense, the concept of privacy that is evident in the schemes' documents falls well short of contemporary expectations (Clarke 2000). The world-wide norms are set by the OECD Guidelines of 1980 (OECD 1980). These are highly inadequate, because they reflect the technology of the 1970s and they have never been adapted to cope with the vastly more powerful and intrusive technologies of the 21st century. Yet when the emasculated and entirely unenforced 'principles' enunciated by scheme proponents are compared against the OECD Guidelines, the OECD's formulation seems like a draconian imposition that has the potential to bring business to its economic knees. Identity management schemes, particularly those discussed in section 3, are almost exclusively initiatives of American corporations and U.S.-dominated industry associations. Those organisations have worked assiduously for substantial watering down of the 'fair information practices' notion, and have gained the support of the U.S. Federal Trade Commission (FTC). As a result, each new document that they publish is yet weaker than the previous one. Liberty 2003e references a veritable flotilla of industry association 'fair information principles' formulations, and presents yet another set that offers a pretence of safeguards in return for even less actual protection than the incoherent and utterly inadequate provisions that current U.S. law already affords

- In some documents, even the narrow sense of 'privacy as a limited application of fair information practices' is abandoned, and privacy is used to refer to something totally foreign both to the public and to the privacy literature, e.g. 'privacy is content security during transmission over communications channels' or "privacy is a security policy applied to an individual" (Liberty 2003d, p.14)

(2) 'Opt-Out' in Lieu of Consent / 'Opt-In'

Consent is a central characteristic of information privacy protection, and is embedded in the privacy laws of most advanced nations. For an analysis of the
nature of consent, and of processes for acquiring consent in an online environment, see Clarke (2002).

But most identity management schemes follow the approach preferred by American corporations, which reject consent as the appropriate basis for dealings between people and organisations. In the U.S., corporations have adopted the mantra of 'opt-out'. This is permissive of data-usage until and unless the person that the data relates to actively objects. 'Opt-out' is completely inconsistent with a consensual arrangement, which in American parlance requires 'opt-in' arrangements to be in place. The American public does not agree with the corporations that dominate U.S. government agencies and the U.S. Congress. This was amply demonstrated when the Federal Trade Commission launched its Telemarketing Do-Not-Call Registry in October 2003. Within weeks, tens of millions of American consumers had registered (EPIC 2003b). It seems reasonable to infer that what they really want is an 'opt-in', consensual arrangement.

Identity management initiatives give very little attention to the acquisition from individuals of specific, informed and freely-given consent. Most organisations impose conditions without any scope for negotiation, and no sense of choice beyond 'accept these conditions or go away'. Moreover, the conditions imposed are generally vague, highly permissive, and very broad in scope. It is very difficult to interpret them as representing meaningful consent.

The European Union, in common with all regimes that are consistent with the OECD Guidelines, requires consent as the basis for data collection, use and disclosure. Microsoft’s Passport fell foul of the European Union’s requirements. Smith (2002) depicts its violations of the European Union Data Privacy Directive as arising because Passport's conditions purported to authorise "blind transfers to unidentified parties", and lack of "full knowledge and understanding of what Microsoft would do with their data". Press reports in January 2003 indicated that Microsoft had agreed to make appropriate changes to their conditions and sign-up processes.

(3) Lack of Consumer Trust

Each time that scheme sponsors broach the privacy issue they fall short of recognising that the public may be serious distrustful of identity management. For example, when The Open Group observed that Microsoft Passport’s acceptance was less than universal, they attributed it to "the reluctance of the public to trust any single organization to provide a universal identity management solution, reinforced by the fact that security question marks have been raised relating to the specific Passport implementation" (2002, p28). Indeed, the distrust was thoroughly justified: privacy advocacy organisations had drawn attention to serious problems and urged people to 'sign-out of Passport!' (e.g. EPIC 2002). But what was overlooked was the possibility that the public might be reluctant to trust any and every such organisation, not just Microsoft.

There is a serious risk of a trans-Atlantic rift in this area. As Hansen et al. (2003) depicts it: "On the one hand, in particular legal contexts reliable identification of
a person is necessary; and, on the other, the structuring and representation of identity (Gestaltbarkeit der Identität) is based in human rights law (Persönlichkeitsrechten)" (p.551, my translation). The hitherto US-dominated identity management scene has not merely overlooked the second strand; it has sought to stifle it.

7.2 The Value of Multiple Identities

A couple of particularly important mis-matches exist between the attitudes prevalent in scheme designs and the interests of human beings.

Many scheme designers fail to demonstrate any appreciation of the need that individuals have to sustain many identities, and to avoid linkage among them. This has been one of the most important forms of privacy protections in the past, and people naturally resist it being broken down. In short, 'silos' are good, at least for privacy. People are, moreover, capable of putting considerable obstacles in the way of business and government if this interest is not respected.

Many schemes acknowledge that individuals have multiple identities (e.g. Open Group, WS-Federation and Liberty Alliance). But elsewhere Liberty Alliance's documents abandon that idea. Its 'network identity' is "the abstraction of the global set of attributes composed from all of a Principal’s existing accounts". So its notion of 'identity' is actually singular: a person has multiple elements, but they are combined to suit the convenience of the organisations that are the intended beneficiaries of Liberty's services.

Moreover, the fact that individuals have multiple identities is assumed to be a problem for them, and not to be a positive form of protection for their privacy. The Liberty Alliance scheme is meant to benefit individuals by tying all of the disparate pieces together, "to gain access to portions of the user’s identity information that may be distributed across multiple providers". That will benefit individuals in some circumstances, but will seriously harm their interests in others. What it will definitely do is benefit the social control interests of businesses and government agencies.

PingId (2002, p.4) also expressly acknowledges that each individual has "a growing number of digital identities". But it then makes the leap to "The issue is ... how to manage the linking or sharing of the ones that already exist". So this association also overlooks the possibility that people might actually want to keep them separate. Some proposals go so far as to be explicitly designed to break down the separation among identities, e.g. RSA (2003) talks of "identity mapping" in order to correlate identifiers that relate to the same person (p.4).

7.3 Anonymity and Pseudonymity

A second critical mis-match arises from the lack of appreciation shown by scheme sponsors that individuals are in many circumstances opposed to the conduct of transactions in an identified manner when they could be conducted anonymously or pseudonymously.
Important though separation between a person's various identities remains, modern technologies provide organisations with the capability to break down the barriers. Consequently, there is a desire for nyms, both anonyms and pseudonyms. It is entirely feasible for nyms to be used for persistent communications, and for profiles to be associated with them; hence many of the interests of business and government can be satisfied, although not all.

Where scheme sponsors declare requirements, they typically omit all mention of nymity (e.g. Open Group 2002, pp. 23-24). Commentators frequently make unwarranted assertions such as "virtually every application in the future will make use of identity information" (Dyson 2002, p.1), without analysing the real needs, the costs, and the objections.

Liberty omits 'anonymity' from its Glossary, but its text uses a greatly debased concept of it, denying that a person could function for a wide variety of purposes without any linkage of data to them at all, and substituting the limited notion that, say, a weather information provider could request the user's attributes without knowing the identity. This is valuable, but is only 'attribute authentication without identity', and is far from the full capabilities of anonymity.

Liberty does define 'pseudonymity', but in a debased manner, as "an arbitrary name assigned by the identity or service provider to identify a Principal to a given relying party so that the name has meaning only in the context of the relationship between the relying parties" (Liberty 2003b). Firstly it assumes that the identity provider knows who the identity is behind the nym (which is only one form of pseudonymity, and the very weakest and least credible form at that); and secondly it assumes that the identity provider assigns the nym rather than the individual creating or selecting it themselves.

One of the few initiatives that discusses the issue in a reasonably satisfactory manner is Shibboleth, whose intent is stated to be that the user's ISP (in this case the educational institution in which they are employed or enrolled) provide the target site with attribute assertions about the user rather than the user's identity. But even in Shibboleth that intention appears to be a mere aspiration, and it is not clear that it has been expressed as a design requirement and implemented in the protocols and business processes.

The XNS concept includes recognition of the need for anonymity, and for pseudonymity. It confuses the ideas, however, by coining 'veronymity', which is not 'nymity' at all, but rather 'strongly authenticated entity' (XNS 2002, p.13).

On the other hand, "In addition to attribute services, there may also be pseudonym services. A pseudonym service allows a principal to have different aliases at different resources/services or in different domains/realms. Some identity providers use fixed identities in their security tokens. In some scenarios it is desired to ensure anonymity of the tokens; pseudonyms provide a mechanism for enabling this anonymity. There is often a trade-off of manageability that must be determined by the principal (i.e., the more identities, the greater potential for management issues)” (WS-Federation 2003, p.12). But despite the promise in that paragraph, it confuses anonymity and pseudonymity,
and the paper contains no further discussion of them. So it is not clear that the text is anything more than a discussion draft, an aspiration, or a token offering to privacy advocates.

It is entirely feasible for strongly protected pseudonymity to be designed into identity management schemes. The proposal in Engberg & Harning (2002) embodies it; and Rannenberg (2003) draws attention to the anonymity and pseudonymity inherent in GSM mobile/cell-phones.

Because pre-authentication during the registration phase is seldom considered, many of the schemes would, in their present configurations, support pseudonymity by default, and in some cases anonymity. Put another way, the assertion that the authentication phase assists with is merely ‘the person connecting via this username provided the relevant password’. Nothing arising from the identity management system provides any confidence about the assertion ‘this is the normal user of the following identity’. Hence existing schemes could be interpreted as being privacy-friendly, because they fail to actually deliver on the promise inherent in the term ‘identity management’.

On the other hand, those identity management schemes that are extended to perform pre-authentication will deservedly attract considerable suspicion from people, because they fail to support the full richness that nymity offers.

### 7.4 Representation of Consumer Interests

This section considers the extent to which consumers have a voice in the development of identity management schemes.

**1. The Need**

Scheme designs embody some key assumptions, such as that:

- consumers are concerned about having to remember multiple username/password pairs;
- consumers are concerned about the requirement to re-authenticate on successive sites;
- consumers want data on multiple sites to be consistent; and
- consumers want dealings with multiple organisations to be seamless.

Consumers may or may not be concerned about these things. And they may also be concerned about many other things. For example, it is reasonable to assume that they would like to avoid being subjected to manipulation by corporations and government agencies that have access to large amounts of personal data, and that are able to continually add to that data in order to locate and track them.

Evidence exists that, when people register with and transact with organisations’ web-sites, they make mistakes at least semi-intentionally, and even utter downright lies. This does not appear to be reflected in the always-up-beat identity management brochureware, White Papers and specifications. Research needs to
be undertaken to establish the extent and nature of distrust by individuals about organisations and their web-sites.

Furthermore, it is likely that there are conflicts among the various interests that consumers have, and conflicts between their interests and those of corporations and government agencies. Hence there is a need for information about how people would prefer to achieve a suitable balance, through trade-off among the various interests.

(2) Consumer Involvement

There is little evidence that the assumptions outlined above have been tested, and none at all that consumers have been asked about appropriate balances among the various interests.

By definition, web services involve users who are remote from the service-providers. Moreover, cyberspace behaviour is not a science, nor even much of an art at this early stage, a mere decade into the Internet era. It would therefore be foolhardy for service-providers to assume that they fully understand their customers, and still moreso for third-party identity managers to be so presumptuous.

Clearly it would be very expensive to consult widely with large numbers of consumers. Structured surveys are also impractical, because they are applicable to topics that are relatively well-understood by the respondents, which is not the case here. A more appropriate tool, although still a reasonably expensive one, is focus groups. However, there is no mention of the use of focus groups on the web-sites of any of the scheme sponsors.

(3) Involvement of Representative and Advocacy Groups

An alternative approach, which is especially appropriate in complex public policy contexts, is engagement with representative and advocacy groups. These can claim to have deep appreciation of the needs of a population or population-segment (through a membership structure and/or longstanding and continuing contact) and/or special competence in the area (e.g. as a result of research conducted).

It is rare that a single such organisation can act as a proxy for large populations. Even amongst consumer advocates and amongst privacy advocates, there are considerable divergencies of perspective. It is therefore strongly advisable to use a panel of organisations. Resourcing is commonly a problem for such groups, and financial support is essential if they are to be able to contribute meaningfully to discussions.

One category of 'engagement' of such groups is 'consultation'. This may be unstructured ('tell us what you think about X'), or structured ('tell us what you think about the attached concept paper / requirements statement / specification'). To be most effective, however, interactions with representative and advocacy organisations need to be ongoing, from conception, through the requirements definition and prototyping phases, through the design specification phase,
through construction and testing, to deployment. Scheme sponsors can extract considerable benefits from discussions and negotiations, and avoid the high costs of re-work and feature retro-fit. The need for sponsors to provide funding to enable these groups' participation can be balanced against those benefits.

Regrettably, there is almost no evidence of active participation by public interest representative and advocacy groups in the conception, expression of requirements, design, or indeed any other phases of the business-oriented schemes described in section 3, nor even the user-centric products described in section 4.3. Indeed, there is only very limited evidence of even the most casual involvement of such groups.

Microsoft and AOL appear to have provided no information about consultations with consumers and consumer representative and privacy advocacy organisations. There also seems to be nothing on the OASIS, PingId, Shibboleth, The Open Group or Web Services Federation sites addressing the question of how they conduct consultations with the individuals whose identities they are seeking to manage. Even the Identrus site shows no evidence of consultations having been undertaken with bank customers or their representative associations.

The Liberty Alliance site refers to a Public Policy Expert Group, which "drives dialogue with government and non-government groups concerned with the many issues pertaining to identity and data management. It also ensures that the Liberty specifications adhere to pertinent laws and regulations". On the other hand, the 'Expert Group' comprises members, and not representative and advocacy groups. The organisation has only a single member that could be seen as a being such an organisation, that member is at the low level of 'Affiliate', and Affiliates are precluded from participation in the formation of specifications.

Moreover, Liberty Alliance's Expert Group does not appear to have anything even vaguely resembling a program to involve such groups. Even the most recently-published document, (Liberty 2003e), which purports to define 'Privacy and Security Best Practices', makes no mention whatsoever of any dialogue, and shows scant evidence of familiarity with the relevant organisations and literature.

One rare instance of involvement appears to have actually been driven by an advocacy group rather than by scheme sponsors. In response to the explosion in identity management schemes, the Washington-based Center for Democracy & Technology (CDT) – which is also Liberty Alliance's sole public interest group Affiliate – convened "a working group comprised of companies and public interest groups", which drafted "basic privacy principles that should be considered in the design and implementation of authentication systems" (CDT 2003).

This Working Group was not widely representative of public interest groups, however. It contained only two, neither of which were specialist consumer representatives or privacy advocates, and three individuals. CDT's ability to withstand pressure from powerful industry participants, and its room for manoeuvre, were therefore tightly circumscribed.
The International Dimension

In almost all schemes, the U.S.-centricity is striking. It is clear that a very high proportion of initiatives in this area, as in many others, are driven by U.S. corporations. On the other hand, these applications are in many cases subject to the laws of other jurisdictions as well as the U.S.A., and they affect individuals who are not directly subject to U.S. jurisdiction.

Moreover, ‘the average Internet user’ is no longer American. The U.S.A. is a mature market, with penetration stable at about 160 million Internet users among the population of about 287 million. It has been stable for some years, with no growth in user-population since 2000. In terms of Internet user count, the rest of the world combined overtook the U.S.A. in the same year. By 2003, there would appear to be about 3 times as many Internet users outside the U.S.A. as there are in it.

The process coordinated by CDT to produce an 'authentication principles' document included no participants who were from outside the U.S.A. The target regulator was the Federal Trade Commission (FTC), which has set the bar a vast distance below the requirements of the several score countries around the world that have legislation that accords with the OECD Guidelines (OECD 1980). Under these circumstances, the likelihood of an outcome that reflects the values of cultures outside the U.S. is low.

The traffic-volume generated per Internet user, and the level of economically motivated eCommerce and eGovernment usage per Internet user, is likely to still be much greater among U.S. users. Nonetheless, adoption is likely to be retarded by scheme sponsors’ failure to appreciate the often distinctly different perspectives of non-U.S. users, and indeed of non-U.S. web-site operators.

It would be quite wrong to suggest that existing schemes are completely unaware of individuals' interests, or that they are completely unaware of the diversity of perspectives among the world’s Internet users, or that they totally fail to reflect users’ concerns. On the other hand, there is little evidence that sponsors have coherent programs in place, even to gather views, let alone to ensure that those views are reflected in scheme designs.
8. The Scope for Balanced Solutions

This report reaches conclusions radically different from the up-beat outlook of scheme sponsors' documents. The initiatives are strong on supply-side push, and very weak indeed on demand-side pull. They are based on many misconceptions, and do not reflect values that are important to individuals.

Part of the problem is the failure to address the tension between organisations' social control aims and the interests of individuals. It is feasible for identity management schemes to achieve reconciliation between those two sets of interests. But that can only come about if schemes commence with a comprehensive set of requirements that reflect not only the interests of corporations and government, but also those of consumers and citizens.

Missing requirements were discussed in sections 5-7 above, and are also addressed also in Hansen et al. (2003). Critical among the aspects that need to be addressed are:

- distinctions between each human entity and their multiple identities;
- support for effective and credible pseudonymity;
- support for the management of identity by individuals themselves and by service-providers to individuals, rather than only by service-providers to corporations and government agencies;
- much more focus on accounts than on people and their identities;
- greater focus on attribute authentication, not only in conjunction with identity, but also without identity; and
- support for the especially important attributes that relate to the powers of an agent, particularly for legal persons such as corporations.

Anonymity is widely regarded as undermining accountability, because a person who is confident that they cannot be identified or located is much less likely to be subject to sanctions, and hence more likely to indulge in behaviour that is harmful to others. Pseudonymity is in principle capable of delivering a balance between the desires for, on the one hand, avoidance of identity-correlation and data-merger, and, on the other, traceability and hence accountability. Engberg 2002 refers to this approach as depending on pseudonyms that are 'non-identified but accountable'. Adoption of eBusiness and eGovernment may prove to be much higher if effective pseudonymity is available.

There are many sources of information that sponsors of identity management schemes can draw upon in order to overcome the problems identified in this report. Some of these are adjacent to identity management, rather than directly part of it, such as:

- approaches that focus on authorisation rather than authentication, such as Blaze et al. (1999);
• closed-community approaches that focus on 'demonstrated authority to operate an account' rather than on identity, e.g. the Account Authority Digital Signature (AADS) model (Wheeler 1998); and

• digital certificate formats and PKI that are designed to support pseudonymity, such as PGP (Zimmerman 1995) and Brands (2000).

In addition, this report has identified a number of products, projects and documents that specifically address identity management, but are more comprehensive, and more consumer-friendly. These are:

• user-selected intermediaries, as described in section 4.3 above;

• own-PCs and own-proxies as identity manager, as described in section 4.4 above;

• developments in the U.S.A., including Nareau Sunshine and those aspects of Shibboleth that expressly implement pseudonymity;

• developments in Germany, including Clauss & Köhntopp (2001), (Clauss & Kriegelstein 2003), ATUS (2003), Rannenberg (2003), and Hansen et al. (2003);

• developments in Switzerland, including IBM Research Laboratories' idemix project on pseudonymity for e-transactions; and

• developments in Denmark, including Engberg 2(002) and Engberg & Harning (2002).

Until and unless these matters are addressed, the current crop of identity management schemes may well be doomed to the same fate that was suffered by so many digital signature services. Those that do achieve traction in the marketplace are likely either to be restricted to narrow niches for which their particular features are a reasonable fit, or to require substantial overhaul in order to be attractive to both users and web-site operators.
References


IPCR (1995) 'Privacy-Enhancing Technologies: The Path to Anonymity' Information and Privacy Commissioner (Ontario, Canada) and Registratiekamer (The Netherlands), 2 vols., August 1995, at http://www.ipc.on.ca/web%5Fsite.eng/matters/sum%5Fpap/papers/anon%2De.htm


Appendix: Industry Participants

Service-Providers

- **Ascio Digital Identity**, which stores personal data for open display on the person's web-site, and includes the capacity to store username/password pairs. See http://www.digital-identity.info/Home/Introduction

- **AOL Screen Name**, a single-sign-on service used across AOL's product-range and is offered to third parties. A Screen Name has associated with it user-profile data. An extended form is provided, variously branded Quick Checkout or AOL Wallet, which also associates with the Screen Name a person's credit-card details and default delivery address. The code-name Magic Carpet is also used from time to time. See http://my.screenname.aol.com/_cqr/homePg/hpController/controller.psp?siteId=snhhomepage&siteState=&hpState=hpHelp


- **GhostSurf**, which provides users with a client-side product that combines access to nymity servers, purging of cookies and history files, detection and elimination of spyware, blocking of pop-up ads, and viewing of data exposed in outgoing messages. See http://www.tenebril.com/products/ghostsurf/

- **IBM Tivoli Identity Manager**, which is a single-organisation single-signon product. See http://www-306.ibm.com/software/tivoli/products/identity-mgr/

- **Microsoft Passport**, a single-organisation single-signon product that has been extended into a multi-organisation single-signon service, and has been considered for a variety of further extensions. See http://www.passport.com

- **Novell digitalme**, which is a repository for username/password pairs for remote services, and for personal data, which can be selectively disclosed. See http://www.digitalme.com

- **Novell eDirectory**, which is a single-organisation single-signon product. See http://www.novell.com/products/edirectory/

- **Passlogix v-GO Single Sign-On® (SSO)**, which is a single-organisation single-signon product. See http://www.passlogix.com/

- **Privacy Inc's MPP**, which provides users with multiple email-addresses, each one specific to a particular interaction. See http://www.privacyinc.com

- **RSA Security**, which offers products service to identity managers, particularly within the federated context. See http://www.rsasecurity.com/microsite/federatedidentity.asp

- **Yodlee**, which comes to identity management from the account aggregation direction. See http://www.yodlee.com
Industry Associations

- **Identrus**, a company formed to coordinate financial industry public key infrastructure, and, through its Digital Signature Trust operation, to act as the peak certification authority for banks that sign digital certificates for their clients. See http://www.identrus.com/ and http://www.digsigtrust.com/

- **Liberty Alliance Project**, an industry association established to develop an open standard for federated network identity. See http://www.projectliberty.org/


- **OpenSAML**, made available by the Internet2 consortium, is a set of open-source Java and C++ libraries that implement the SAML specifications. See http://www.opensaml.org/

- **PingId**, an industry association intended to facilitate the development of commercial relationships in federated identity management schemes. See http://www.pingid.com/

- **Shibboleth**, a project of the Internet 2 association of universities and technology providers. It is focussed on a federated mechanism for authenticating the assertion that a browser-user has permission to access a remote resource, based on an attribute such as being a staff-member of the institution, or being an enrolled student in a particular class. Shibboleth data-exchanges use the OpenSAML standard. See http://shibboleth.internet2.edu/ and http://www.internet2.edu/

- **SourceID**, an industry association of developers of open source tools, application and infrastructure for federated identity management. Its objective is to deliver tools that will enable inter-operability among at least Liberty Alliance, SAML and WS-Federation. See http://www.sourceid.org/

- **The Open Group**, an industry association of information technology providers, which is endeavouring to establish a policy position on identity management. See http://www.opengroup.org/ and http://www.opengroup.org/dif/dirday20/idmrep.htm

- **Web Services Federation (WS-Federation)**, an unincorporated industry association of a small number of large technology providers (BEA, IBM, Microsoft, RSA Security, and VeriSign), which has proposed the WS-Federation Language. This is a specification of processes rather than data formats. See http://www.ibm.com/developerworks/library/ws-fed/
Projects

- **ATUS (A Toolkit for Usable Security)**, which provides a user-interface simulation of the use of an own-device identity manager. See http://www.iig.uni-freiburg.de/telematik/atus/idm.html

- **DRIM (DResden Identity Management)**, a code-library for and prototype of a user-proxy identity management server. See http://drim.inf.tu-dresden.de

- **IBM Research Laboratories' idemix** project on pseudonymity for e-transactions. See http://www.zurich.ibm.com/security/idemix/

- **Icepick**. See http://sourceforge.net/projects/icepick/

- **RAPID (Roadmap for Advanced Research in Privacy and Identity Management)**. See http://www.ra-pid.org

- **Sunshine**, an open-source initiative to produce a peer to peer identity management system. See http://nareau.weblogs.com/stories/storyReader$44
Glossary

Access
The use by an Entity of a Capability in relation to a System Resource. The Entity that is afforded the Capability may be a Natural Person or an Artefact.

Access Control
The protection of System Resources against unauthorised Access. In particular, the application of Privileges and Restrictions accorded to Usernames or Roles, in accordance with an Access Control List (ACL).

Access Control List (ACL)
A data structure that enumerates Usernames and/or Roles, and possibly also groups of Usernames and/or Roles, together with the Permissions and Restrictions that they enjoy in relation to System Resources.

Account
A set of Data-Items held by an organisation, which relates to a particular Identity external to the organisation, and defines the relationship between the two parties.

Agent
A Legal Entity that has the capacity to act on behalf of another Legal Entity. The Legal Entity that is represented is referred to as a Principal.

Anonym
An Identifier that cannot be associated with any particular Entity.

Anonymity
A characteristic of Records and Transactions, such that they cannot be associated with any particular Entity, whether from the data itself, or by combining it with other data.

Artefact
A human-made Entity. Artefacts include such devices as workstations, smart cards and robots, and software agents that exhibit more or less intelligent behaviour, and whose Entity or Identity may need to be subjected to Authentication.

Assertion
A statement that declares that one or more putative facts are true.

Attribute
A characteristic of a real-world Entity, Identity or Event. Attributes of a Natural Person include the
person's gender, age-range, qualifications (such as being a registered counsellor), and capacity to act as an Agent for another Entity.

Authentication
The process of testing of an Assertion, in order to establish a level of confidence in the Assertion’s reliability. Categories of Assertion that may be subjected to Authentication may refer to Agents, Attributes, Credentials, Data Integrity, Entities, Identities, Location, and/or Value.

Authentication Strength
The degree of confidence that is engendered by an Authentication process. Also referred to as Authentication Quality.

Authenticator
An item of Evidence used in the process of Authentication. It may comprise an ephemeral act such as the demonstration of knowledge (such as a Password or the maiden name of a person’s mother), or the demonstration of the ability to perform a particular act (such as the writing of a signature); or it may have a physical or digital existence in the form of a Credential, including a Token or a Document.

Authorisation
A synonym for Permission.

Authorisation Process
A procedure for granting Permissions, which are then stored in an Access Control List.

Biometric
A measure of an Attribute of a Natural Person’s physical self, or of their physical behaviour. In principle at least, a Biometric can be used as an Entifier for a Natural Person; as an Authenticator for an Assertion involving a human Entity; and as a means of restricting the use of a personalised Token to the appropriate Natural Person.

Business Enterprise
A for-profit organisation. It may be an incorporated body (in particular a corporation) recognised at law as a Legal Person, or may be unincorporated, and treated by the law as indistinguishable from the individuals who constitute it.

Call-Back
A technique whereby a System does not permit Access by a User directly, but only accepts from a User a request for Access, and then initiates a connection to a location previously recorded for that User (e.g. a telephone-number or IP-Address).

Candidate Key
One of more Data-Items within a Record or Transaction that potentially enables the Record or
Transaction to be associated with a particular real-world Entity or Identity.

**Challenge-Response**

An Authentication technique whereby a System does not permit Access by a User, until the User has given the correct answer (or ‘response’) to a question (or ‘challenge’). A Password is a form of Challenge-Response authentication. Other examples include requests for date of birth, invoicing address, and the most recent transaction on the User’s account.

**Credential**

An Authenticator that has physical or digital existence. Examples include a Document and a Token. The concept of Credential does not include an ephemeral act such as demonstration of the possession of knowledge (such as a Password, or the person’s mother’s maiden name), nor the ability to perform an action (such as providing a written signature).

**Data-Item**

An element within a Record or Transaction.

**Document**

A Credential comprising writing or printing on paper, or its equivalent in electronic form. Examples include birth certificates, certificates of naturalisation, marriage certificates, passports, drivers’ licences (and, in some jurisdictions, non-drivers' 'licences'), employer-issued building security cards, credit cards, club membership cards, statutory declarations, affidavits, letters of introduction, and invoices from utilities.

**Enrolment**

Alternative term for Registration.

**Entifier**

One or more data-items concerning an Entity that are sufficient to distinguish it from other Entities, and that are used to signify that Entity. For a Natural Person, an Entifier is of necessity a Biometric. A Legal Person does not have corporeal existence, and hence cannot have an Entifier. An Artefact may have an Entifier, e.g. a Processor-ID or the Network Interface Card (NIC) Id of an Ethernet card.

**Entification**

The process whereby data is associated with a particular Entity. It is performed through the acquisition of data that constitutes an Entifier for that Entity.

**Entity**

A real-world thing. Categories include objects, animals, Artefacts, Natural Persons, and Legal
Persons (such as corporations, trusts, superannuation funds, and incorporated associations).

**Entity Authentication**
The process of testing an Assertion that data is associated with a particular Entity, in order to establish a level of confidence in the Assertion’s reliability. In particular, the process of cross-checking a newly-acquired Entifier against a pre-recorded Entifier.

**Event**
An occurrence in the real world.

**Evidence**
Something that assists in resolving facts at issue.

**Evidence of Identity (EOI)**
Evidence that assists in Authentication of an Assertion relating to Identity. Sometimes referred to by the less appropriate term Proof of Identity.

**Evidence of Ownership (EOO)**
Evidence that assists in Authentication of an Assertion that a particular Entity is the appropriate possessor of a Credential. Sometimes referred to by the less appropriate term Proof of Ownership.

**False Acceptance**
A decision to accept an Assertion, which is not correct.

**False Rejection**
A decision to reject an Assertion, which is not correct.

**Federated Identity Management**
Performance of the Identity Management function by multiple organisations, in order to deliver a Single Sign-On service to multiple organisations.

**Identification**
The process whereby data is associated with a particular Identity. It is performed through the acquisition of data that constitutes an Identifier for that Identity.

**Identifier**
One or more data-items concerning an Identity that are sufficient to distinguish it from other Identities, and that are used to signify that Identity. Identifiers for Identities used by Natural Persons include names assigned by people. Identifiers also include ‘id numbers’ or ‘id codes’ issued by other Entities that the Entity interacts with. An Entity may be assigned many such numbers and codes. A Natural Person may use many Identifiers, including variants of names. A Legal Person may have many names (e.g. associated with business units, divisions, branches, trading-names,
trademarks and brandnames), and multiple ‘id numbers’ and ‘id codes’ assigned by other Entities that the Entity interacts with.

Identity

A particular presentation of an Entity. An Identity may correspond to a Role played by the Entity. An Identity may be used by the Entity in its dealings with one other Entity, or with many other Entities. An organisation may maintain an Account within its records that corresponds to an Identity.

Identity Authentication

The process of testing an Assertion that data is appropriately associated with a particular Identity, in order to establish a level of confidence in the Assertion’s reliability. In particular, the process of cross-checking, against additional Evidence of Identity (EOI), the Identity signified by an Identifier acquired during an Identification process.

Identity Management

A set of processes that enable the Authentication of Assertions relating to Identity. The term is often used in a more restrictive sense, however, to apply to the specific context of online access over open public networks.

Identity Management System

A system that provides a cluster of services relating to Identity Management. The central service is Authentication. The system may also support other services, such as Pre-Authentication, Authorisation, Single Sign-On, Identity repository management, a synchronisation management facility, user self-service registration, user self-service capabilities, and audit.

Individual

A Natural Person.

Legal Entity

An Entity that is recognised at law as having the capacity to act.

Legal Person

A Legal Entity that is recognised at law, but is not a Natural Person. Examples include corporations, incorporated associations and trusts. Some government agencies are Legal Persons, in particular those established under statute, and those formed under the Corporations Law. All other government agencies form part of a single Legal Person called a body politic, such as the Commonwealth of Australia, and the State of
A Legal Person may perform Roles, including as Agent for other Legal Entities.

**Login**

An action by an Entity whereby they seek Access to System Resources. Usually involves the provision of a Username/Password pair to an Access Control System.

**LoginId**

Alternative term for User Name.

**Multi-Factor Authentication**

An Authentication process in which multiple forms of Evidence are used, in order to increase the level of confidence in the Assertion. In the case of Identity Authentication, this involves two or more of the following: an additional Identifier provided by the person; knowledge demonstrated by the person (‘something you know’); an act performed by the person (something you can do); a Credential provided by the person (‘something you have’); a Biometric surrendered by the person (‘something you are’ or something you do).

**Natural Person**

A human being, and a particular category of Legal Entity. Distinguished from a Legal Person. A Natural Person performs social, economic and political functions in various Roles, e.g. as citizens, consumers, sole traders, and members of partnerships and unincorporated solutions; and as Agents both for other Natural Persons and for Legal Persons.

**Nym**

A generic term encompassing both Anonym and Pseudonym.

**Nymity**

A generic term encompassing both Anonymity and Pseudonymity.

**Password**

A form of Challenge-Response Authentication in which a string of characters is used to assist in the Authentication of the Assertion that a person has the right to use a Username. The effectiveness of the technique is predicated on the assumption that the Password is known only by the appropriate Entity (and, in less secure schemes, also by the System conducting the Authentication).

**Permission**

A Capability, associated with a Username, which enables Access to System Resources. It is usually recorded in an Access Control List (ACL). Authorisation and Privilege are used as synonyms for Permission.
Persistent Nym

A Nym that is capable of being used on a continuing basis, to support a succession of communications.

Pre-Authentication

A series of steps undertaken during a Registration process, to simplify subsequent Authentication processes. The steps include the collection of Evidence in order to establish a level of confidence in an Assertion. It may involve the issue of a Credential. The term is commonly used to refer to Pre-Authentication of Identity, resulting in the issue of some kind of Token. It is equally applicable, however, to Attribute and Agency Authentication.

Principal

The Legal Entity on whose behalf an Agent acts.

Privacy

The interests that Natural Persons have in sustaining a 'personal space', free from interference by other people and organisations, and in controlling information about themselves. It has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data. A variety of privacy rights are conferred by international instruments, and by the laws of most jurisdictions. The term is often used in a misleading manner by security specialists, as a synonym for what they also call 'data confidentiality', or even to refer merely to the protection of the content of data during transmission.

Privilege

A synonym for Permission and for Authorisation.

Profile

Data associated with a Username. It is intended that the data reflect Attributes of the Entity issued with the particular Username that are useful in enhancing the service provided to it.

Proof of Identity (POI)

Evidence that is determinative of truth in relation to an Assertion relating to Identity. Such a concept is inconsistent with the notion of risk-managed security. Hence the concept of Evidence of Identity is to be strongly preferred.

Proof of Ownership (POO)

Evidence that is determinative of truth in relation to an Assertion that a particular Entity is the appropriate possessor of a Credential. The concept is inconsistent with the notion of risk-managed security. Hence the concept of Evidence of Ownership is to be strongly preferred.
Pseudonym: An Identifier that cannot be associated with any particular Entity unless legal, organisational and technical constraints are overcome.

Pseudonymity: A characteristic of Records and Transactions, such that they cannot be associated with any particular Entity, unless legal, organisational and technical constraints are overcome.

Record: A collection of Data-Items, expressed in the abstract world in order to represent an Entity or Identity in the real world.

Registration: A process comprising a series of steps intended to simplify subsequent Authentication processes. Also referred to as Enrolment. One important aspect is Pre-Authentication.

Relying Party: An Entity that relies on an Assertion. Of particular importance is an Assertion that another Assertion (e.g. of Value, Identity, Attribute or Agency) has been subjected to particular Pre-Authentication or Authentication processes.

Restriction: A limitation on a capability associated with a Username in respect of System Resources. It is typically recorded in an Access Control List.

Role: A pattern of behaviour adopted by an Entity. An Entity may adopt one Identity in respect of each Role, or may use the same Identity when performing multiple Roles. Examples of Roles played by Legal Entities include seller and buyer, supplier and receiver, debtor and creditor, payer and payee, principal and agent, franchisor and franchisee, lessor and lessee, copyright licensor and licensee, employer and employee, contractor and contractee, trustee and beneficiary, tax-assessor and tax-assessee, business licensor and licensee, plaintiff and respondent, investigator and investigatee, and prosecutor and defendant.

Role-Based Access Control (RBAC): An approach to Access Control whereby Usernames are associated with Roles (or functional positions), within an organisation or process, rather than with individual Users.

Silo Identity Management: Performance of the Identity Management function by an organisation in order to deliver a Single Sign-On service within a single organisation.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplified Sign-On</td>
<td>A system that reduces the number of Passwords that Users have to remember in order to gain Access to multiple systems.</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>A system that enables an Entity to Access multiple sets of System Resources after being authenticated just once (e.g. by keying a Username/Password pair). The concept originated within organisations, but is capable of being applied across multiple organisations as well.</td>
</tr>
<tr>
<td>System Resource</td>
<td>A Resource, Access to which is provided by an Access Control System. Examples of System Resources include data-files, data-records within data-files, Data-Items within data-records, software and specific services provided by software.</td>
</tr>
<tr>
<td>Three-Factor Authentication</td>
<td>A form of Multi-Factor Authentication. It is most commonly described as involving ‘something you know’, ‘something you have’, and ‘something you are’.</td>
</tr>
<tr>
<td>Token</td>
<td>A Credential issued by a Legal Entity to another Legal Entity in which a third Entity places some degree of trust. A Token is designed to provide a relatively high level of confidence in some kind of Assertion, and is likely to include security features intended to render it difficult to forge, and tying it in some manner with the particular Entity. Examples include ‘identity cards’ (especially ‘photo-id’), turnaround documents, tickets issued to Natural Persons required to wait in a queue, and smartcards and ‘dongles’ designed to be used in conjunction with standalone and networked workstations.</td>
</tr>
<tr>
<td>Transaction</td>
<td>A collection of Data-Items, expressed in the abstract world in order to represent an Event in the real world.</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>A form of Multi-Factor Authentication. It is most commonly described as involving ‘something you know’, and ‘something you have’.</td>
</tr>
<tr>
<td>User</td>
<td>In the context of Usernames and Access Control, a Natural Person who seeks Access to System Resources.</td>
</tr>
<tr>
<td>Username</td>
<td>A string of characters that is issued to an Identity, and is included within an Access Control List, and which thereby has Permissions, and is subject to Restrictions, in relation to Access to System</td>
</tr>
</tbody>
</table>
Resources. Also referred to as LoginID and User ID. Normally used in conjunction with a Password or PIN, and possibly also a Token, in order to enable Authentication. Usernames are often treated as thought they constitute an Identifier. This is inadvisable.

**Validation**
The process of establishing the truth of an Assertion. Also referred to as Verification. The concept is inconsistent with the notion of risk-managed security. Hence the concept of Authentication is to be strongly preferred.

**Verification**
The process of establishing the truth of an Assertion. Also referred to as Validation. The concept is inconsistent with the notion of risk-managed security. Hence the concept of Authentication is to be strongly preferred.