PLEASE AMEND YOUR HOTLINKS TO www.rogerclarke.com (previously www.anu.edu.au/people/Roger.Clarke).

(Id)Entities (Mis)Management
The Mythologies underlying the Business Failures

Roger Clarke **

Emergent Draft of 5 April 2008

Prepared for an Invited Keynote at 'Managing Identity in New Zealand', Wellington NZ, 29-30 April 2008

This document is at http://www.rogerclarke.com/EC/IdMngt-0804.html

The supporting slide-set is at http://www.rogerclarke.com/EC/IdMngt-0804.ppt

Abstract

The identity management arena is full of misunderstandings and mythologies. This presentation highlights why most initiatives have fallen far short of their promise, and why they will continue to do so until technology providers change their mind-set, and user-organisations are offered much more appropriate products. The analysis has substantial implications for government agencies concerned with public policy. It also delivers important messages for the strategies of user-organisations in both the public and private sectors, and technology vendors.

Introduction

Organisations have been assiduously applying information technologies (IT) to the management of people for over half a century now. The original focus was on the capture of data about individuals into machine-processable form. This was followed by the increases in the volume of data sought, increases in the number of sources from which it was acquired, and the consolidation of data from a variety of sources into a single record. All of these activities depend upon means for achieving reliable associations between stored data and the human beings the data is believed to relate to.

What appears to have been the first comprehensive consideration of human identification in information systems was undertaken in Clarke (1994). During the 15 years since that paper was drafted, the governments of several among the relatively free nations have pursued campaigns to impose draconian identification schemes on their populations, utilising technologies such as bar-codes, smartcards, RFID tags and biometrics to address the identification aspects, coupled with centralised databases or hub databases to manage the vast quantities of

personal data involved.

Meanwhile, corporations and individual government agencies have pursued a parallel path in the virtual world. Successive waves of marketer activity have used such buzz-phrases as 'digital signatures', 'authentication', 'single sign-on' and, currently, 'identity management'. Failure rates have been high, and overall return on investment very low. Unrealistic visions and designs abound, particularly in complex multi-organisational settings such as 'Joined Up Government'.

The reasons for the succession of failures in this area are straightforward:

> *Technology providers have created a great many myths.*
>
> *User organisations have swallowed them.*

The purpose of this paper is to identify some of these myths, and explain why they're misleading and harmful. The series in which 18 selected Myths are presented has been devised so as to enable key underlying concepts to be exposed, and two models to be progressively developed. The Myths are the primary focus, but their implications are also briefly outlined.

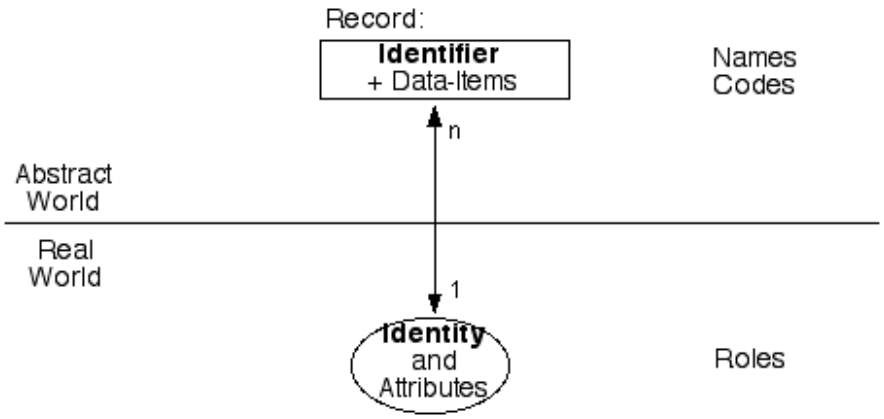
Myth 1 - An identity exists in an organisation's database

Before tackling the more complex issues, it's necessary to go back to fundamentals. In terms like 'identity management' and 'identity provisioning', technology providers adopt the pretence that they create and maintain identities, and then grant people the right to use them.

But identities long pre-date the existence of information technology suppliers. An identity is a presentation or role of some underlying entity. It exists in the real-world.

What organisations have on their disk-drives are collections of data. That data has some degree of correspondence with the attributes of real-world identities. The association between a record and an identity is achieved by means of an identifier. An identifier is one or more data-items that are used to distinguish the identity from other, similar identities. Exhibit 1 shows these relationships in diagrammatic form.

Exhibit 1: Identities and Identifiers



Note: The definitions of 'identity' and 'identifier' used in this section, like other definitions used throughout this paper, are drawn from this author's key publications in the area over the last two decades, which are indexed below. They are summarised in glossary form in Clarke (2004b) and explained in greater detail in Clarke (2004c).

Myth 2 - You only have one identity

Myth 3 - Each identity is used by only one person

Technology providers like to pretend that each person 'out there' is a singular identity. Their simplistic notion is that 'You are who your birth certificate or your passport says you are'. Many go further, and accuse people who have more than one identity of being cheats and criminals. They are upset about this partly on moral grounds, but also because their products are presaged on simple models in which there is a reliable one-to-one relationship between person and identity.

In the real world, however, each of us plays many roles. And each of us is only partially known to each of the people and organisations that we deal with. Each of us may be, and present to particular others, as child, lover, spouse, parent, employee, licensee, bank-account holder, taxpayer, benefit-recipient, and many other things besides.

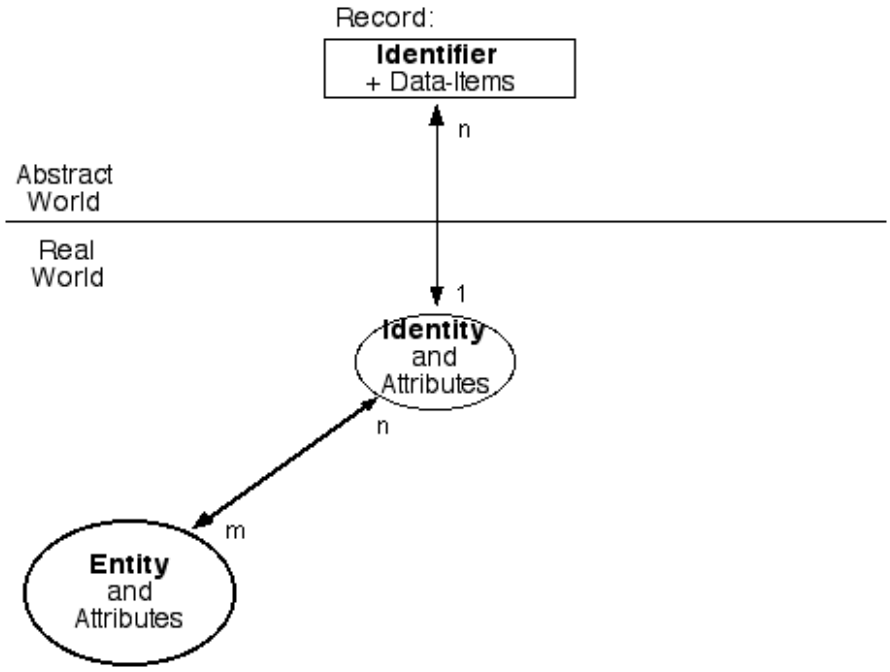
Each of those 'partials' (as some sci-fi writers like to call them) have records in databases. In many cases, organisations do not link the records they hold that reflect different relationships with the same underlying entity. For example, many people buy from, pay tax to, receive benefits from, or are licensed by, the same organisation with which they are employed, or for which they perform contract work. In few such cases is their employee-identifier the same as the identifier under which their other records are filed. As far as the organisation is concerned, they are distinct identities, even though they are the same person.

A further consideration is that none of the databases held by organisations is in any sense complete. And there are considerable inconsistencies among the data the databases contain, because the data was collected for different reasons, using different questions, in different contexts, and at different times.

Looking at the relationship from the other direction, many identities are used by more than one person. Every job-description and community role is filled by different people at different times, and in some cases by different people at the same time. Examples include parent, club treasurer, and shift-supervisor in a 24-hour business process. Furthermore, masquerade and identity fraud expressly involve one person appropriating an identity that is normally used by another person. So a naïve model that assumes a one-to-one relationship between identity and person is incapable of dealing with miscreants.

Exhibit 2 shows how records and identities link to the underlying entities (in this case, people - although the diagram can serve equally well for PCs, mobile-phones, and even inactive objects like pallets and packages). The 1:n (one-to-many) and m:n (many-to-many) relationships underline the real-world complexities that many so-called 'identity management' products fail to reflect.

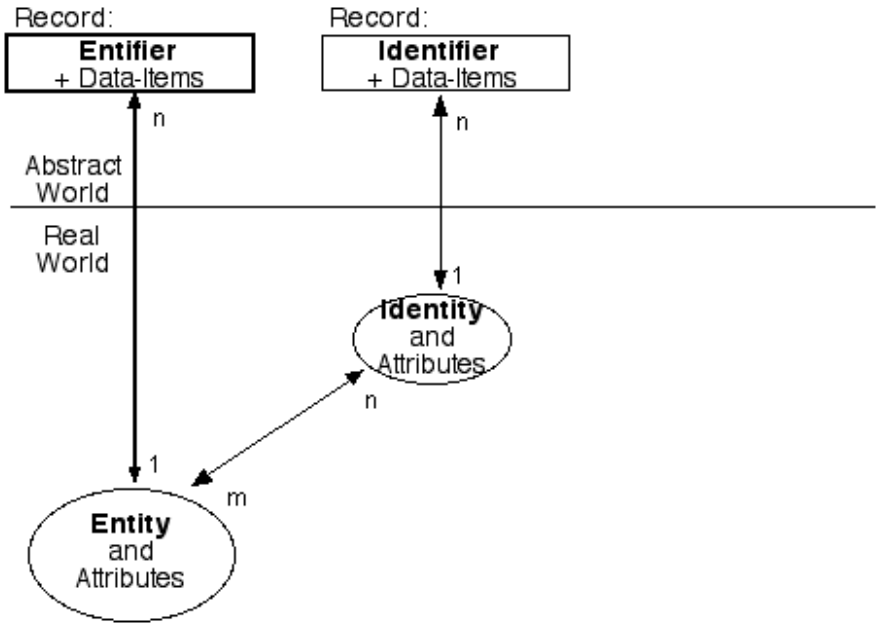
Exhibit 2: Identities and Underlying Entities



Myth 4 - A biometric is a human identifier

A biometric is not associated with an identity, but directly with an entity. No commonly-used term exists to describe data that distinguishes between similar entities; so for some years now I've used the term 'entifier'. Exhibit 3 shows the relationships between entities and entifier-based records in databases.

Exhibit 3: Entities and Entifiers



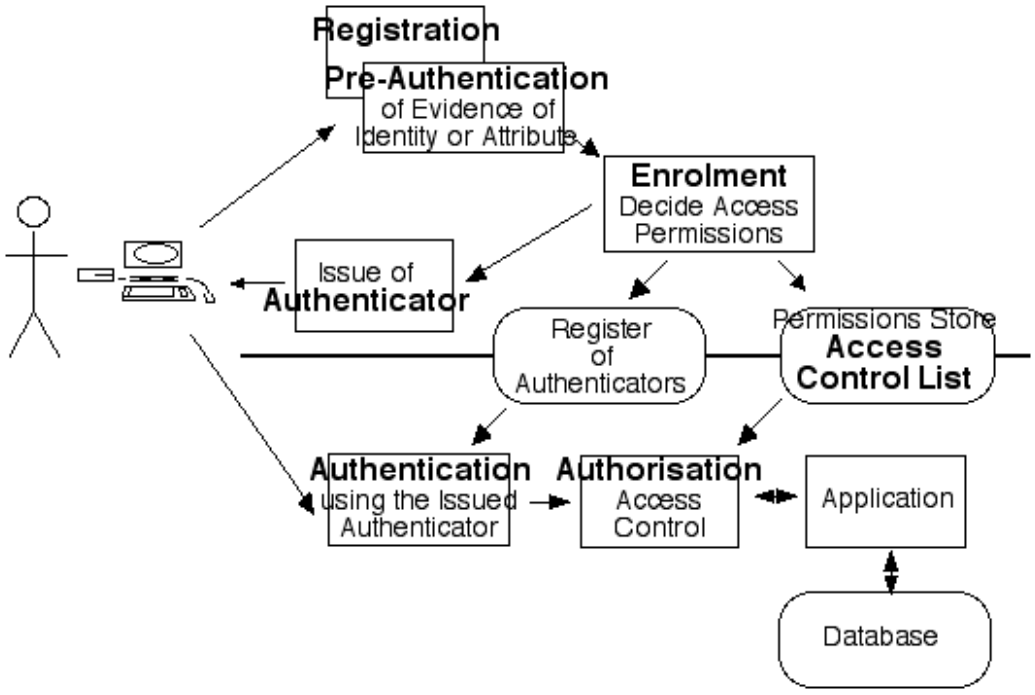
Technology providers whose products do not reflect this model have seriously negative impacts on important human values, because products based on inadequately rich models undermine the separation of partial identities that has long been the single most important form of privacy protection.

Myth 5 - Organisations create and manage identities

The earlier Myths lead naturally to this common misapprehension. It is meaningful to talk of organisations performing 'data management' and 'identifier provisioning' (and, as will be discussed in later sections, 'authenticator provisioning'). The terms 'identity management' and 'identity provisioning', on the other hand, are misleading, and implicitly claim powers that organisations do not have.

What organisations really do in the area of online access control is modelled in Exhibit 4.

Exhibit 4: Online Access Control



The elements of the access control process are as follows:

- a person (or, increasingly, a person's software agent) makes electronic contact with an organisation's access control system, and is required to undergo a **'Registration'** process. This comprises the capture of some data (minimally a username, possibly also a password)
- some form of **'Pre-Authentication'** may be undertaken, such as the provision of additional data or documents. If pre-authentication is successful, an **'Enrolment'** process is performed
- the system issues the person (or software agent) with an identifier and probably one or more **'Authenticators'**. The most common authenticator is a password, but many other possibilities exist. The system stores some means whereby the authenticator can be tested on each occasion that the user logs in
- the system also determines and records what 'privileges' or 'permissions' the user has. A commonly-used term to describe the data is an **'Access Control List'**
- when the person (or their software agent) makes contact with the organisation on subsequent occasions, they undergo **'Authentication'**, by which is meant that they are challenged for an authenticator
- if the user is successfully authenticated, the system performs the **'Authorisation'** step, which involves looking up the access control list to see what permissions the user has. It then makes the appropriate applications and databases available to the user

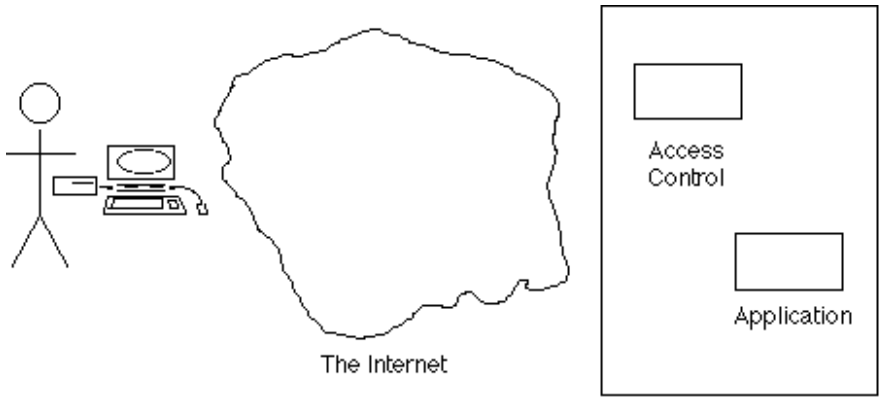
These processes are important, valuable, and reasonably well-supported by technology providers. The mythology lies in the way in which suppliers would like their customers to believe that online access control systems do much more than this, in particular that they create and manage identities.

Myth 6 - Identity Management Products Actually Work

The ground has now been laid, and the mythology of the current round of product offerings can be explained. This section commences by providing an overview of the phases of the 'identity management' movement, in order to be able to demonstrate where the myths begin.

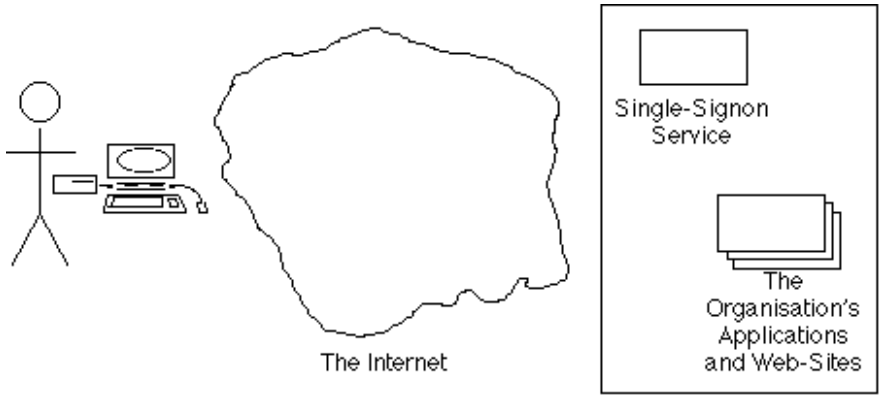
User access originally (roughly, from the 1960s onwards) involved software referred to here as 'Access Control', being placed in front of an application, to protect it and the data it managed from unauthorised users. Exhibit 5A depicts the contemporary pattern of use in diagrammatic form.

Exhibit 5A: Access Control for a Single Application



From as early as the 1970s onwards, organisations were running many applications, and each had its own Access Control sub-system. It's desirable that each person be able to access all appropriate applications by means of a single username and a 'single sign-on'. Exhibit 5B depicts this phase. However, remarkably few organisations have fully solved the challenges of signgle-signon even for their staff, let alone for people outside the organisation such as customers and suppliers.

Exhibit 5B: Single-Organisation Single-SignOn



Since the widespread availability of the Internet from the mid-1990s, service-providers have offered generalised Access Control systems as Internet Services. These can be configured to enable access to the applications run by or for many organisations. Exhibit 5C depicts the arrangement. (For the reader's convenience, the mainstream term 'Identity Management Service' is used, even though the term is criticised in this paper as being materially misleading).

Exhibit 5C: Multi-Organisation Single-SignOn

A competitive market exists for such Internet Services. Initially they were entirely segregated. So, in order to access an application run by a particular organisation, a person had to login to whichever service that organisation was connected to. Progressively, inter-operability arrangements emerged, and in principle at least, a person should be able to login to any third-party Access Control or Identity Management Service, and reach any application in any organisation. Exhibit 5D depicts the still somewhat imaginary, 'federated identity management' arrangement.

Exhibit 5D: 'Federated Identity Management' (or Interoperable Multi-Supplier Multi-Organisation Single-SignOn)

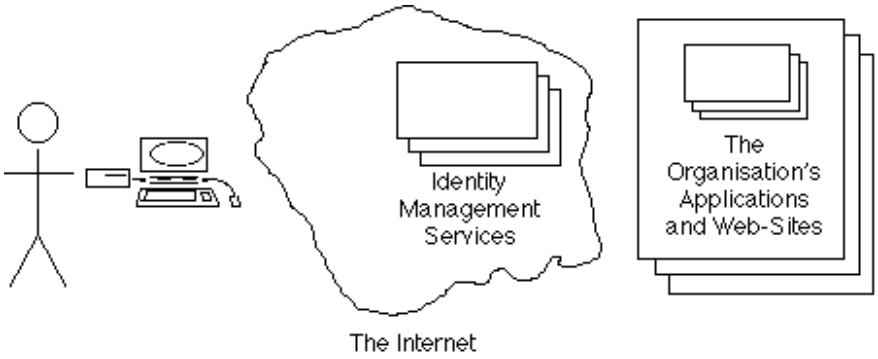


Exhibit 5D represents the current state of play. But it is deficient, because it models only the supply-side, locked in to what might be termed the 'corporate supremacist' perspective, whereby organisations design and deliver, and people consume.

Toffler coined the word 'prosumer' in 1970. The open public Internet gave rise to the culture of appropriation of digital content, and enabled the 'proactive producer-consumer' to finally emerge. One aspect of prosumerism is active participation in 'identity management', and active projection of 'identity' rather than mere passive acceptance of what organisations impose on people.

Exhibit 5E draws to attention the existence of software on individuals' own devices that presents data to the Access Control software depended on by organisations, and that does so in the interests of the user not the organisation. For example, such software may work autonomously, as an agent for the user. It may submit randomised or nonsense data rather than accurate data (e.g. by registering for the New York Times site as a male, U.S., high-income, Accountant/Auditor, in Accounting, in a small company - in each case the first option in the drop-down lists that the site provides). Importantly, it may also conduct successive transactions with the same organisation using different identities (e.g. in order to avoid the accumulation of a consumer profile).

Exhibit 5E: Identity Management by the User's Own Device

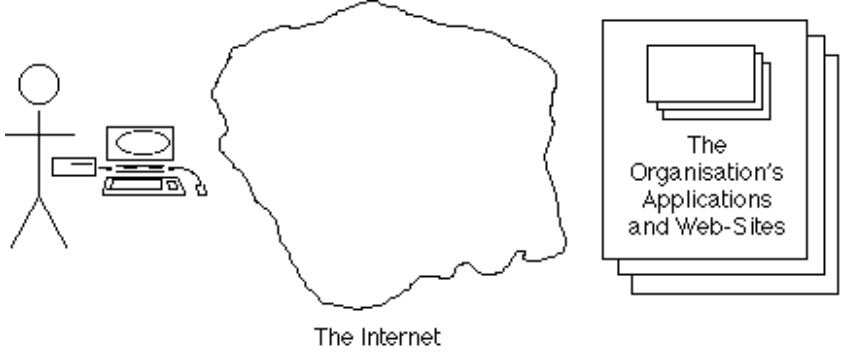
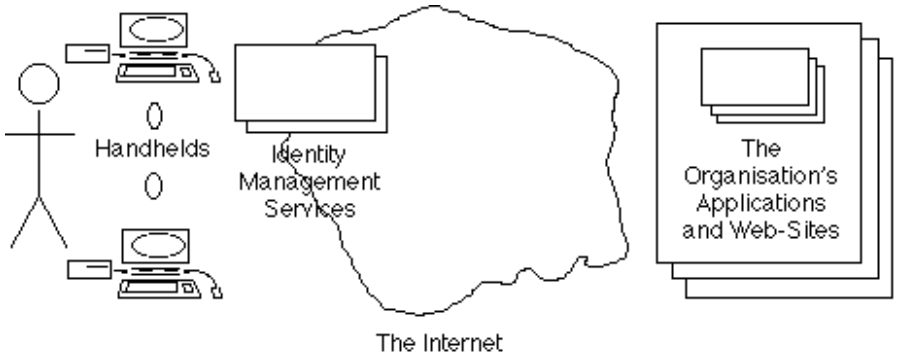


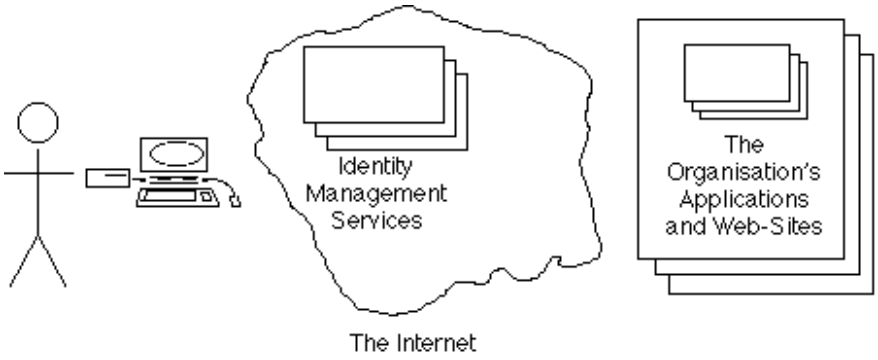
Exhibit 5F represents a further level of end-user sophistication, whereby a user installs their own proxy-server to manage flows between the many devices that they use and the organisations that they deal with. This may manage a consolidated identity (e.g. for the organisations that they trust), or many different identities (e.g. for organisations that they don't know, or know and don't trust).

Exhibit 5F: Identity Management by a User-Managed Proxy-Server



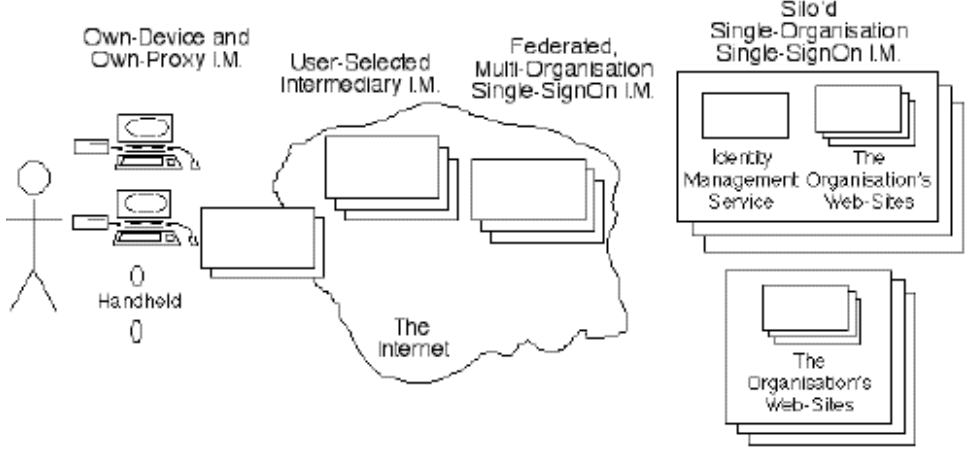
Similar kinds of proxy-service can be offered by Internet Service Providers that work as agents for the individual rather than for the organisations at the other end of the network. These intermediaries can offer all of the demand-driven services mentioned in the last couple of paragraphs, but can also merge the identities of many users, in order to present a composite identity to organisations. This arrangement is depicted in Exhibit G.

Exhibit 5G: Identity Management by a User-Selected Proxy-Service



The myth perpetrated by technology providers is that they manage identity, and can deliver accuracy, reliability and security to their corporate clients. They project the architecture as being 'federated identity management' as depicted in Exhibit 5D above, whereas Exhibit 5H below depicts what might be called the 'multi-mediated super-architecture' that actually exists.

Exhibit 5H: How Identity Management Really Works



Myth 7 - It's generally necessary to authenticate identity

Because so much stress is placed on 'identity management', it comes as a surprise to organisations when they examine their business processes and establish how few transactions actually require an authenticated identity. Enquiries and hypotheticals, payments, and many kinds of trading events can be performed safely without any great confidence in who the other party is.

The fundamental misrepresentation that technology providers have made is that 'authentication' means 'identity authentication'. Authentication is a process whereby confidence is established in an assertion. It is performed by cross-checking the assertion against one or more items of evidence. But the assertion may have little or noithing to do with identity.

Authentication is costly and time-consuming for all parties, and may be unduly onerous and intrusive for the humans who are conducting transactions with an organisation. It is therefore important to consider what the assertion is that actually matters. The assertion whose truth needs to be established may be one of fact, or that value has been or is being transferred, or that the other party is in a particular location, or that a particular document was actually issued by some authority. A common need is to check an attribute of the other party to a transaction (e.g. is the person over 18, over 65, a Veteran, a plumber who gets a trade discount, a subscriber who gets a member's discount?). In a great many circumstances, the party's identity is unimportant and even irrelevant.

Reflecting these realities, the Australian Government Authentication Framework (AGAF) stipulates the conduct of an analysis of what statements are relevant to each particular transaction, and risk assessment in order to establish both what assertion needs to be authenticated, and what level or strength of authentication is justified.

Myth 8 - An organisation's identity can be authenticated

Since the mid-1990s, it has been technically feasible to use digital signatures to perform some kind of authentication of the parties participating in Internet transactions. The means to do this is provided by the Secure Sockets Layer protocol, later standardised as Transport Layer Security (SSL/TLS, more familiar to most users as the https protocol in their web-browser).

In principle, SSL/TLS could be used to authenticate users, but in practice hardly any normal user has a digital signature key. Its primary use is to authenticate the web-sites that people visit.

Unfortunately, this aspect of SSL/TLS is almost entirely valueless. What are usually referred to as 'Verisign certificates' come with virtually no warranties. This is not surprising, because pre-authentication processes are expensive, and no-one wants to pay the money to conduct them. So no-one takes much notice of them, and most people ignore the warnings that appear when unknown or outdated certificates are detected.

There is a further difficulty, which is that organisations have no physical existence, and hence cannot themselves perform any act that would enable Verisign or anyone else to pre-authenticate them. People perform those acts on behalf of organisations. Yet, to date, there are virtually no mechanisms available whereby an assertion can be authenticated that a particular user has authority to perform an act on behalf of a particular organisation.

In short, as consumers and citizens, we all conduct eCommerce and eGovernment in the blind faith that we're dealing with who we think we are.

Not a Myth 9 - Privacy is for people with something to hide

In order to address some further myths that undermine eCommerce and eGovernment, it's necessary to venture into the privacy arena. The first step is to acknowledge the truth of a rallying call used by anti-privacy businesspeople. It's quite true that privacy is for people with something to hide.

Myth 9A - Only crims / cheats / wimps have something to hide

But the sub-text underlying Not-A-Myth 9 is quite false. The people who use the phrase mean it to imply that honest people have nothing to hide (and therefore shouldn't be concerned about privacy).

There are many data-items and tokens that each of us is contractually bound to hide, such as our passwords and PINs, and our passport and driver's licence. In principle, this applies to every authenticator that we use, in all circumstances (including a lot of public data, such as our date of birth, and our mother's maiden name). House keys and digital signature keys alike belong on the same list. Anyone who has a home, a passport or a user-account, or conducts bank transactions electronically, and attacks people for having something to hide, commits hypocrisy.

In addition, it's a rare person that has no attributes at all that are, or may become, a basis for bias and bigotry. There is a vast variety of possibilities in such areas as health, ethnicity, beliefs, convictions, family arrangements, gender preferences and sexual peccadillos. Merely being known to have had an education recently cost a significant proportion of about 2 million people their lives (Kampuchea, late 1970s).

At a more prosaic level, the following is a general guide to categories of 'persons at risk', who have very good reasons to hide a wide range of personal data from public view:

- people hiding, or on the run, from other people who threaten them with violence, including:
  - people concealing themselves from previous criminal associates;
  - victims of domestic violence;
  - protected witnesses; and
  - people under fatwa;
- celebrities, notorieties and VIPs, who are subject to the unwanted attention of excessively zealous fans and of stalkers, extortionists and kidnappers, including:
  - politicians;
  - entertainers and sportspeople;
  - people 'in the public eye', such as lottery-winners; and
  - people in security-sensitive roles such as national security operatives, undercover police, prison warders, and staff in psychiatric institutions.

Not a Myth 10 - Privacy advocates protect crims / cheats / terrorists

Again, the statement is true, but the sub-text is a refined lie.

Myth 10A - Privacy advocates don't realise that privacy protects crims / cheats / terrorists
Myth 10B - Crims / cheats / terrorists can be deterred, prevented and caught, without

creating a society worse than one that contains crims / cheats / terrorists

The position adopted by anti-privacy businesspeople is that anyone who is in favour of something that protects bad people is themselves a bad person (which is a variant of the jingoistic 'the friend of my enemy is my enemy') .

Bad people use money, buses and trains and eat food. Bad people also take advantage of the privacy protections that good people rely upon as part of the cluster of freedoms that make life worth living. The bad people can't be denied the ability to abuse those freedoms without also denying the good people the ability to use them.

Myth 11 - Nyms are for cheats

A 'nym' is a particular form of identifier. Like other identifiers, it comprises one or more attributes of an identity (represented in transactions and records as one or more data-items) that are sufficient to distinguish that identity from other instances of its class, but with the additional characteristic that the available data is not sufficient to enable association with the underlying entity.

An anonym is a nym for which it is not possible to establish an association between the identity and the underlying entity; whereas a pseudonym is a nym for which that association is feasible, but has not been made.

It is a common misconception that anonymity and pseudonymity are in themselves bad, and that they need to be denied and defeated. In fact, nymity is normal. For a simple demonstration of how mainstream the idea is, consider the number of synonyms that exist (in alphabetical order):

> *aka ('also-known-as'), alias, avatar, character, nickname,* nom de guerre, nom de plume, *manifestation, moniker, personality, profile, pseudonym, pseudo-identifier, sobriquet, and stage-name*

Cyberspace has spawned many more, including:

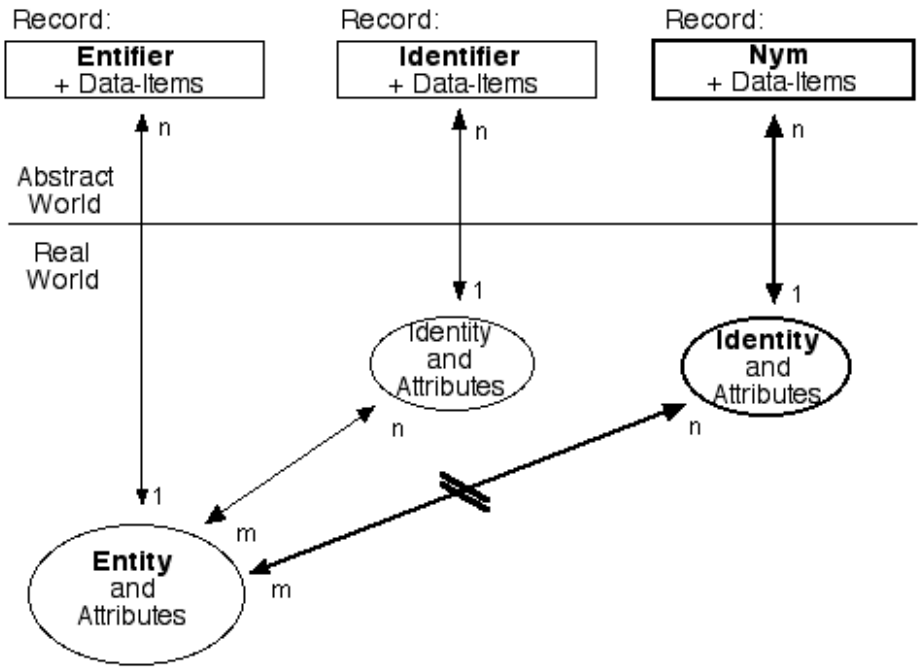
> *account, avatar, handle, nick and persona*

Nymity is much-used in transactions, such as:

- visits to enquiry counters in government agencies
- telephone enquiries, both direct and to third-party / outsourced call-centres
- inspection of publications on library premises
- access to public documents by electronic means, at a kiosk or over the Internet
- barter transactions
- cash transactions, including the myriad daily payments for inexpensive goods and services, gambling and road-tolls
- voting in secret ballots
- treatment at discreet clinics, e.g. for sexually transmitted diseases
- epidemiological research and social network research (e.g. re HIV/AIDS)
- financial exchanges, including dealing in commodities, stocks, shares, derivatives, and foreign currencies
- nominee trading and ownership
- political speech
- artistic speech
- counselling

Exhibit 6 completes the series begun with Exhibits 1 to 3, by depicting the broken link between the Identity and underlying Entity. It also shows the characteristic, inherited from identifiers generally, whereby an entity may use more than one nym, and a nym may be used by one or more entities.

Exhibit 6: Nyms



Myth 12 - Privacy-Enhancing Technologies (PETs) don't pay

Many information technologies are neutral with respect to privacy. Some are actively Privacy-Invasive Technologies ('the PITs'). The term Privacy-Enhancing Technologies (PETs) refers to applications of technology that actively assist in the protection of privacy. The term was coined in 1995, although key examples pre-date its coinage by at least 15 years (Clarke 2001a).

The PETs scene has been confused during the last decade because of a number of Pseudo-PETs that have been put forward by technology providers. These include 'meta-brands' that purport to provide 'good housekeeping' 'seals of approval', but which provide no tangible privacy benefits (Clarke 2001d), and ineffectual protocols such as Platform for Privacy Preferences (P3P) (Clarke 1998c, 1998d, 2001c).

Real PETs can be usefully divided into three categories:

- countermeasures against PITs
- tools for uncrackable anonymity ('savage PETs')
- 'gentle PETs', which seek a balance between nymity and accountability

Distrust is a major impediment to all forms of eCommerce and eGovernment, and privacy is a crucial element of distrust. PETs represent opportunities to signal privacy-sensitivity, and to earn trust. Some specific ways in which organisations can seek payback from PETs include (Clarke 2008):

- by promoting PETs
- by funding research into PETs, and development of PETs, by the organisation itself, and by others
- by distributing PETs
- by supporting open source licensing of PET software, in order to enhance its availability, and increase confidence in its integrity
- by designing and adapting eBusiness services to ensure that they work with PETs, and not against them

Concrete outcomes that can be sought by implementing PETs include:

- the attraction of particularly sensitive client segments
- the attraction of non-users:
  - who value choice
  - who value a provider that is aware of and sensitive to client needs

- enhanced privacy image
- enhanced service delivery
- enhanced market-share, transaction revenue and profit

Myth 13 - Data silos are bad

The term 'data silo' refers to collections of data that are segregated from one another. The term is mostly used where the speaker is urging the breakdown of the silos, in order to extract more value from the inter-related or consolidated collection. Clearly, there are many circumstances in which the benefits of breaking down barriers and inconsistencies and achieving inter-operability exceed the costs and dis-benefits.

Where the data silos contain personal data, however, far greater care is needed. There are contexts in which people actively want separate data collections to be inter-related. But there are many more contexts in which they don't, and in which considerable harm can arise if the segregation is broken down.

Data from multiple sources is inevitably inconsistent in meaning and quality, the inconsistencies give rise to inferences that are often negative, and the inconsistencies and suspicions seldom work to the advantage of the people to whom the data relates. The combination of data from multiple sources also provides the organisation or organisations with additional data-based power over the individual.

Data silos are one of the most fundamental and most effective forms of privacy protection. The negative privacy impact of breaking down data silos makes it imperative that proposals be considered carefully, and that costs, benefits and dis-benefits be evaluated rather than assumed. Proposals to join up complex systems require particularly convincing justification, because such projects result in even more complexity, and hence in diseconomies of scale and scope that are likely to render the apparent benefits illusory.

Myth 14 - Identity silos are bad

The term 'identity silos' is little-used, but quite crucial to a proper understanding of identity matters. The term refers to the segregation of a person's many 'partial identities' each of which is known to particular individuals or organisations. Identity silos are one of the most fundamental and most effective forms of privacy protection, and breaking down those barriers represents a very substantial threat to privacy.

There are two broad ways in which identity silos can be broken down. One is through the use of one identifier for multiple purposes, rather than separate identifiers for each purpose. A common motivation for doing this is to share across multiple systems the costs of issuing and managing identifiers. The second way in which identity silos are broken down is by having multiple separate identifiers, but setting up a scheme whereby they can be correlated.

The private sector breaks down identity silos when, in addition to collecting basic identifiers such as name and data of birth, and assigning its own code to its customers and employees, it also gathers identifiers associated with other systems, such as drivers' licence numbers, passport numbers, and registration numbers with taxation and benefits agencies.

The public sector destroys identity silos when it uses a common number for multiple programs, or in multiple agencies, but also when a database carries identifiers for multiple schemes in one place. The Centrelink agency in Australia, the delivery mechanism for all c. 100 benefits programs managed by c. 20 agencies, includes a hub database that stores everything needed to correlate the many partial identities each recipient of benefits has with each of the agencies that they deal with or have dealt with.

Hub schemes like Centrelink's go well beyond the 'inhabitant registration schemes' that are common in European countries. These are mostly restricted to specific clusters of programs - typically taxation and health insurance - and little-used outside those designated contexts.

The extreme case of identity silo destruction is a national identification scheme, of the kind dreamt of in the U.S.A. (under the name Real Id), proposed in the U.K. (as the National Identity Register - NIR), and defeated in Australia in 1985-87 (as the Australia Card), withdrawn following a campaign in 2005-06 (tagged as a 'national identity system') and collapsed following a campaign in 2006-07 (as the Access Card). Analyses of the elements of national identification schemes are in Clarke (2006a) and No2ID (2008).

Myth 15 - Biometric schemes actually work

Biometrics lobbyists have been working for many years to try to get their schemes accepted. Most biometric technologies have failed. Many biometrics companies have failed, and most extant biometrics operations are supported by cross-subsidy from more successful divisions within the same company.

Biometrics tackles a very difficult challenge, and a host of factors have to be confronted that undermine quality. The scope for error is vast, the prevention of masquerade is very difficult and very expensive, and the cost of false-positives is often prohibitive (Clarke 2002). Only a small number of technologies are tenable, and all of those can be applied effectively only in very specific contexts. Meanwhile, from the viewpoint of the people subjected to it, biometrics procedures are demeaning, intrusive and onerous (Clarke 2001).

The biometrics lobbyists received a massive boost from the 12 September 2001 phenomenon. Whereas 11 September 2001 was a genuine public safety issue that needed to be addressed, the 'national security' agencies harnessed counter-terrorist hysteria to achieve massive and completely unjustified inroads into civil freedoms. These included mindless attempts to impose biometrics. US and Australian government agencies alike have prostituted themselves by contriving testing regimes and reports that give biometric technologies an appearance of workability - extraordinarily so in the case of the pseudo-biometric usually mis-described as 'face recognition'.

Linked with this movement have been unholy alliances between technology providers and user organisations. The self-styled 'Biometrics Institute'
is such an alliance, fraudulently declaring itself to be a source of "unbiased information" about biometrics.

Myth 16 - Biometric schemes combat terrorism

The most extreme justification advanced for the introduction of biometric schemes is that it is necessary to combat terrorism. This is readily shown to be false (e.g. Schneier 2001, Ackerman 2003, Clarke 2003), because terrorists are defined by the acts that they perform, not by their entifier. But the myth continues to circulate.

Myth 17 - Imposed biometric schemes will work

In 1992-93, I had great difficulty convincing the editor of a learned journal that what I referred to as "imposed physical characteristics (e.g. dog-tags, collars, bracelets and anklets; brands and bar-codes; embedded micro-chips and transponders)" should be referred to in a serious work, because they regarded such talk as pseudo-scientific and scare-mongering.

The material was published in Clarke (1994)
mainly because I was able to provide evidence that the techniques were already emergent. Since then, an industry has exploded, and such devices are being increasingly imposed on "institutionalised persons, including patients, particularly new-born babies and those who are comatose or suffering senile dementia), and prisoners in gaol, on day-release schemes, and on bail", as that paper explained they would be.

The technologies have been far less successful than their proponents suggested they would be. Location technologies are wildly inaccurate, costs are very high, error-rates are high, and subversion is easy. Yet the de-humanisation of controlled populations continues, and is already being extended. Applications in schools are particularly insidious, because they represent training of children to expect and accept highly intrusive identity authentication, and continuous surveillance.

Myth 18 - An id scheme is just another business system

Organisations naturally seek to manage (id)entification and (id)entity authentication arrangements in such a way that they address risks, and cost the organisation as little as practicable (e.g. by transferring costs to others, particularly the individuals whose identity is being managed). It is therefore tempting for organisations' CIOs to perceive 'identity management' as just another part of their application portfolio.

It is highly advisable to instead recognise that 'identity management' is infrastructure that underpins other applications, and to appreciate the highly charged atmosphere that surrounds it. Identity schemes invite massively negative reactions by the public, and offer the media enormous scope for stories that depict the organisation as the villain, imposing on the freedoms of individual customers, employees and students. The risks spiral upwards as the identity scheme moves up the scale from single-purpose to multi-purpose, and as single-purpose identifiers are subsumed by or correlated into a national identity scheme.

Implications

The primary purpose this paper has been to identify 18 conventional views relevant to identity management, and provide sufficient evidence to support the contention that they are Myths. This has consumed almost all of the space available in a paper of conventional length. The following brief, positive comments can be inferred from the largely negative exposition above.

Identity management schemes need to pass a test of acceptability by the public generally, and by the individuals they are imposed upon. A failure in that test represents an impediment to adoption, and translates into slow and low adoption rates. Beyond that lie the risks of public backlash, rejection, opposition and even eActivism. The natural outcomes are project failure, and not merely a failure to get ROI but outright waste of the funds of shareholders and/or taxpayers, and harm to the careers of those left holding the parcel when the balloon goes up.

Identity management schemes therefore demand a strategic approach. They are best developed within the context of a privacy strategy (Clarke 1996b, 2006b). They need to be risk-managed, with public consultation, open information and the exercise of great scepticism about the many Myths outlined in this paper.

More specifically, the following guidance is offered:

- Analyse your requirements
- Appreciate the sensitivities involved in (id)entity
- Carefully justify your uses of all forms of (id)entity management
- Assess and manage risk
- Conduct a privacy impact assessment (Stewart 1996, Clarke 1998a, NZPC 2002, OFPC 2006, ICO 2007)
- Publish information and consult with affected people and their representatives and advocates
- Authenticate appropriate assertions
- Impose identity authentication that is only as onerous ('strong') as the risk assessment warrants
- Sustain data silos
- Sustain identity silos
- Support pseudonymity
- Impose entity authentication only with the most stringent justification, with no central storage, and with no templates that enable masquerade

The identity management movement, and its predecessor digital signature and authentication initiatives, have appeared to consumers and citizens to be aggressive and authoritarian, and designed by big organisations for big organisations, with little attention paid to the interests of the people who are expected to submit to the dictates of the scheme.

The collection of any form of identification needs to be justified. And frequently the assertions that need to be authenticated don't relate to identity. The kinds of things the organisation needs to be confidence about are

assertions of fact (or the accuracy of data), assertions of value ('Here's the money. Check it now'), and attribute assertions ('I am over 18'; or 'I'm a plumber and I get the trade discount'). Much greater understanding of human (id)entity is needed, and much more balance between organisational desires and human needs.

Resources

Clarke R. (1988) 'Information Technology and **Dataveillance**' Commun. ACM 31,5 (May 1988) 498-512, at http://www.rogerclarke.com/DV/CACM88.html

Clarke R. (1994) '**Human Identification**
in Information Systems: Management Challenges and Public Policy Issues' Info. Technology & People 7,4 (December 1994), at http://www.rogerclarke.com/DV/HumanID.html

Clarke R. (1996a) '**Cryptography in Plain Text**', Privacy Law & Policy Reporter 3, 4 (May 1996), at http://www.rogerclarke.com/II/CryptoSecy.html

Clarke R. (1996b) '**Privacy, Dataveillance, Organisational Strategy**' Keynote Address for the I.S. Audit & Control Association Conf. (EDPAC'96), Perth, 28 May 1996, at http://www.rogerclarke.com/DV/PStrat.html

Greenleaf G.W. & Clarke R. (1997) '**Privacy Implications of Digital Signatures**', IBC Conference on Digital Signatures, Sydney (March 1997), at http://www.rogerclarke.com/DV/DigSig.html

Clarke R. (1997) '**Chip-Based ID: Promise and Peril**', for the International Conference on Privacy, Montreal (September 1997), at http://www.rogerclarke.com/DV/IDCards97.htmlClarke R. (1998a) '**Privacy Impact Assessment Guidelines**' Xamax Consultancy Pty Ltd, February 1998, at http://www.xamax.com.au/DV/PIA.html

Clarke R. (1998b) '**Public Key Infrastructure**: Position Statement' Xamax Consultancy Pty Ltd, May 1998, at http://www.rogerclarke.com/DV/PKIPosn.html

Clarke R. (1998c) '**Platform for Privacy Preferences**: An Overview' (April 1998), Privacy Law & Policy Reporter 5, 2 (July 1998) 35-39, at http://www.rogerclarke.com/DV/P3POview.html

Clarke R. (1998d) '**Platform for Privacy Preferences**: A Critique' (April 1998), Privacy Law & Policy Reporter 5, 3 (August 1998) 46-48, at http://www.rogerclarke.com/DV/P3PCrit.htmlClarke R. (1999a) '**Anonymous, Pseudonymous and Identified Transactions: The Spectrum of Choice** ', Proc. IFIP User Identification & Privacy Protection Conference, Stockholm, June 1999, at http://www.rogerclarke.com/DV/UIPP99.html

Clarke R. (1999b) '**Person-Location and Person-Tracking**: Technologies, Risks and Policy Implications' Proc. 21st Int'l Conf. on Privacy and Personal Data Protection, pp.131-150, Hong Kong, 13-15 September 1999. Revised version in Information Technology & People 14, 2 (Summer 2001) 206-231, at http://www.rogerclarke.com/DV/PLT.html

Clarke R. (2001a) '**Introducing PITs and PETs**: Technologies Affecting Privacy' Privacy Law & Policy Reporter 7, 9 (March 2001), at http://www.rogerclarke.com/DV/PITsPETs.html

Clarke R. (2001b) '**Biometrics** and Privacy' Xamax Consultancy Pty Ltd, April 2001, at http://www.rogerclarke.com/DV/Biometrics.html

Clarke R. (2001c) '**P3P Re-visited**' Privacy Law & Policy Reporter 7, 10 (April 2001), at http://www.rogerclarke.com/DV/P3PRev.htmlClarke R. (2001d) '**Meta-Brands**' Privacy Law & Policy Reporter 7, 11 (May 2001), at http://www.rogerclarke.com/DV/MetaBrands.html

Clarke R. (2001e) 'The Fundamental Inadequacies of **Conventional Public Key Infrastructure**' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, at http://www.rogerclarke.com/II/ECIS2001.html

Clarke R. (2001f) '**Authentication: A Sufficiently Rich Model** to Enable e-Business' Xamax Consultancy Pty Ltd, December 2001, at http://www.rogerclarke.com/EC/AuthModel.html

Clarke R. (2003) '**Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper**' Proc. 16th Int'l eCommerce Conf., at Bled, Slovenia, 9-11 June 2003, at http://www.rogerclarke.com/EC/Bled03.html

Clarke R. (2004a) '**Identity Management**: The Technologies, Their Business Value, Their Problems, and Their Prospects' Xamax Consultancy Pty Ltd, March 2004, from http://www.xamax.com.au/EC/IdMngt.html

Clarke R. (2004b) '**Identification and Authentication Glossary**' Xamax Consultancy Pty Ltd, March 2004, extract from Clarke (2004a), at http://www.rogerclarke.com/EC/IdAuthGloss.html

Clarke R. (2004c) '**Identification and Authentication Fundamentals**' Xamax Consultancy Pty Ltd, May 2004, at http://www.rogerclarke.com/DV/IdAuthFundas.html

Clarke R. (2006a) '**National Identity Schemes** - The Elements' Xamax Consultancy Pty Ltd, February 2006, at http://www.rogerclarke.com/DV/NatIDSchemeElms.html

Clarke R. (2006b) '**Make Privacy a Strategic Factor - The Why and the How**' Cutter IT Journal 19, 11 (October 2006), at http://www.rogerclarke.com/DV/APBD-0609.html

Clarke R. (2008) '**Business Cases for Privacy-Enhancing Technologies**' in Subramanian R. (Ed.) 'Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions' IDEA Group, 2008, at http://www.rogerclarke.com/EC/PETsBusCase.html

---

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., a Visiting Professor in the E-Commerce Programme at the University of Hong Kong, and a Visiting Professor in the Department of Computer Science at the Australian National University.

Acknowledgements

This paper builds on a long series of prior publications and presentations over the last twenty years. In addition to the papers formally referenced above, invited presentations were made in Washington DC in 2001, in Sydney in 2002 aand 2003, in Toronto and Ottawa in 2004, to Australian Computer Society Branches nationwide in 2004, and in Victoria (British Columbia) and Canberra in 2006.

Sponsored by Bunhybee Grasslands and the extended Clarke Family

---

Created: 27 February 2008 - Last Amended: 5 April 2008 by Roger Clarke - Site Last Verified: 15 February 2009
This document is at www.rogerclarke.com/EC/IdMngt-0804.html