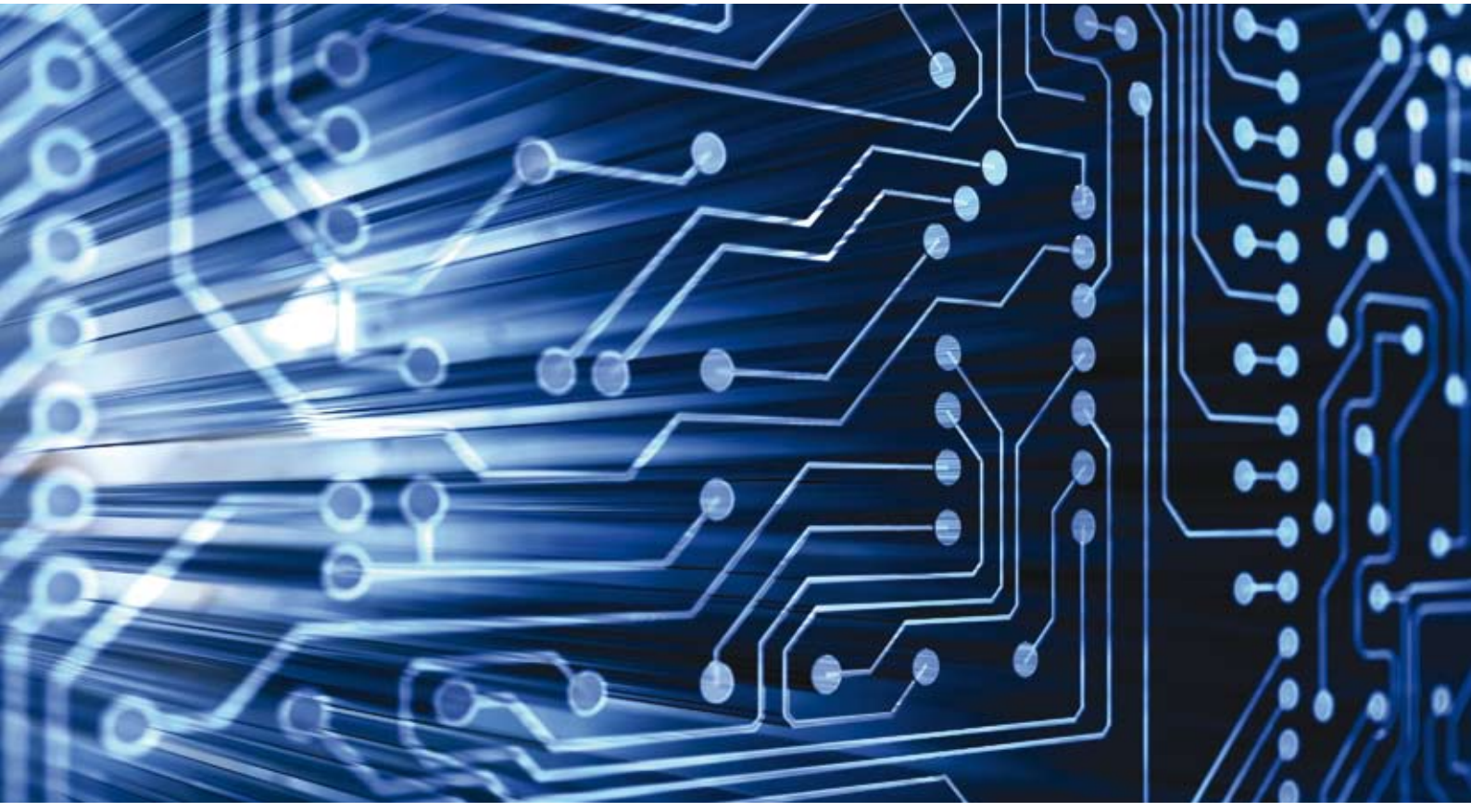
Identity management, trust and security on-line

An NCC Research Report



NCC National Computing Centre

Identity management, trust and security on-line

An NCC Research Report focussed on ID management and trust and security in the on-line environment

Authors: Dr Andrew Hopkirk and Stefan Foster

Edited by: Ian Jones

NCC Research Report

November 2007

Contents

page

ISBN 0-85012-922-2

Disclaimer
Every care has been taken by the authors, and the National Computing Centre, and associated working groups, in the preparation of this publication, but no liability whatsoever can be accepted by the authors or by National Computing Centre, or associated NCC working groups, for actions taken based on information contained in this document.

1. Foreword

The National Computing Centre's purpose is to help its members make effective use of IT and the Centre continually keeps pace with new technologies that businesses will benefit from. As you would expect, new technologies emerge in different ways and some appear to 'creep in from the sides' somewhat unexpectedly rather than make a sudden, explosive entrance and as such they appear in our day to day lives almost by stealth. Online Digital Identity Management is one such technology that has a potential significance that extends way beyond mere new functionality on our desktops and in our systems. As such this report gives independent insight that all manner of businesses and users will have to take seriously in the next few years

We're all familiar and quite often frustrated with the present endless repetition and input of our personal and business details into on-line service providers and payment mechanisms. We are all also challenged by the proliferation of passwords and ID character strings of ever increasing complexity that are practically impossible to memorise over a period of time. This complexity and frustration is exaggerated by our concerns and inhibitions driven by how far we can trust on-line information exchange, commerce and traders. We are not really sure sometime who are we really dealing with. Efficient and effective identity management solutions that are all pervasive and an integral part of the Internet's infrastructure are therefore needed right now so that online trade and information is not inhibited.

New technologies just coming onto the market from individual and collaborative efforts by the global technology vendors such as IBM, Microsoft, Novell and Sun complimented by the offerings from the diverse open source community are all promising to move us quickly into a new paradigm: one where identity management effectively becomes an intrinsic part of the Internet's basic infrastructure.

Critical to making this paradigm shift is clear and simple information about what these technologies are and the problems they are addressing, their underlying conceptual basis and how and where they are being piloted by early adopters. In this paper we have provided some straightforward, inclusive and objective information which we hope you will find both informative and useful in helping you to consider the opportunities that you could exploit both professionally and individually.

We at the National Computing Centre, who have worked on this project, would like to extend our thanks to those who have supported this work and given us the benefit of their expertise and insight. Of particular note are all those that have been prepared to let us quote their personal comments such as Microsoft Corporation, Sun Microsystems and the other participants in the proof of concept case studies from London Borough of Newham, Government Gateway and Directgov, Derby City Council, the Cabinet Office and GBTV.

The Identity Management environment is moving at an extremely fast pace and we encourage you to visit the electronic version of this document via www.ncc.co.uk where relevant updates will add further context, detail and industry advancements as they become publicly available.

Michael Gough
Chief Executive Officer
The National Computing Centre

2. Executive summary

There is already today a mass market of consumers using the web as a platform for financial, retail and information transactions with a wide range of Public and Private Sector organisations. However, considerable growth potential is unrealised through lack of confidence in on-line systems and the complexities of using them.

It has become clear that much of the data captured and processed on-line is ultimately linked to both an individual's personal identity and at least one organisational identity, raising significant identity management issues needing urgent resolution. There also needs to be a long term view of how we manage and exploit identity related technology and policy so that expedient solutions do not build in problems for the future.

Whether as consumers and citizens, businesses or governments, or as technology suppliers, we all need to be confident that identities are securely managed so that we can all obtain common benefits such as:

'It has become clear that much of the data captured and processed on-line is ultimately linked to both an individual's personal identity and at least one organisational identity, raising significant identity management issues needing urgent resolution'

- On-line commerce and trade growing in volume and value because it is trusted by customers.
- More efficient public services used by more citizens and businesses.
- More products and services, public and private, being available to more people and businesses through online channels.
- There is confidence in auditability and traceability for assurance and regulatory purposes.
- Wholly new products and services are enabled.

The private and public sectors have different identity management issues and requirements for solutions. The private sector has a relatively straightforward problem versus opportunity as it is relatively more in control of its destiny. In contrast, the public sector has to move more cautiously as there are a plethora of interlinked and complex problem versus opportunities there. However, in terms of service quality, for example in more reliable delivery and trustworthiness, both sectors are faced with the same problems and are looking to the technology suppliers to solve these.

Simultaneously, individuals are becoming more educated and aware of the issues surrounding their on-line and off-line identities and want to be able to manage both proactively. Both Central Government and the private sector are responding and gearing up to offer such services and a lack of coherence in action; risks making the situation worse before it gets better.

The technology community has worked hard to define and develop what could become a common identity management layer of the Internet that is both all pervasive and an integral part of the infrastructure. Recognising that mass understanding and adoption are critical success factors for them, they are proactively collaborating and raising awareness through partnerships with consumers, business and government, developing and delivering educational programmes and proof of concept demonstrators.

The first introduction of the digital Information Card concept is a unique opportunity to exploit the obvious similarities with familiar off-line, physical card based identity solutions. This position achieved, virtuous circles will build momentum, trust and credibility in the whole system very quickly indeed.

3. Identity management opportunities and issues

3.1. The general position today

The advent of common use of the World Wide Web and the global Internet in the 1990's almost immediately established a mass market of individual consumers using the web as a new platform for financial and information transactions with organisations of a wide range of types – some long established, others brand new and wholly Internet-based.

It has become clear that much of the information captured, stored and required on-line is ultimately linked to both an individual's personal identity and also an organisation's identity. This outcome raises many identity management issues the resolution of which requires mature stakeholders to take a longer term view of

where 'identity' fits into their world view and the avoidance of serial short term technical solutions to long term issues. These mature stakeholders are now looking for comprehensive identity management systems solutions with global Internet scale potential for mass deployment and long term utility.

'…mature stakeholders are now looking for comprehensive identity management systems solutions with global Internet scale potential for mass deployment and long term utility'

These considerations are shaped by distinct drivers for change for each major stakeholder grouping and a set of common benefits that all are seeking as defined below:

Drivers for change in identity management practices

IT used by the Citizen – Consumer led

- There is a requirement for smooth and seamless 'customer journeys' through the multiple online services they are being encouraged to use. A critical requirement is to minimise the amount of repeated requests for the same information from individuals.
- Assurance of the safety and security of personal data is critical and as such a series of trusted and reliable sources of data are needed.
- A much more individually driven and managed control of the use and re-distribution of personal data.
- Independence and interoperability of devices, for example the ability to easily access personal data across a series of devices without and risk to security and integrity of that data.

Business and government led

- Public and Private Sector organisations alike are demanding efficiency savings from the increasing automation of processes with the ability to share data safely and much wider use of online self-service facilities by individuals as customers, users or employees.
- Exploiting a more solid identity standards foundation to deploy new related services more rapidly and reliably.
- An increased need for compliance with growing requirements for audit and traceability of service provision to individuals and businesses.

Technology supplier led

- The lack of an effective identity management system is hindering the adoption of new ways of using existing IT. This has a consequential effect on efficiency and market growth.
- An effective identity management system is negatively effecting consumer, business and government trust in IT suppliers.
- New business models, products and services are being held back by the lack of an effective identity management system and therefore, this is seen as a barrier to general economic growth.

There is an emerging series of common benefits that are both sought and required by the above stakeholder groupings and these benefits are gaining increasing buy-in and momentum. These are summarised as:

- On-line commerce and trade will grow in volume and value because it is trusted by customers. Customers would like to use on-line systems in their personal lives and business.
- More efficient public services are used by more citizens and businesses enabled by the adoption of a robust identity management system.
- More products and services, public and private, are available to more people and businesses through online channels.
- There is confidence in auditability and traceability for assurance and regulatory purposes.
- Wholly new products and services could be either developed or enabled by robust personal and business identities.

3.2 Organisational issues

Many in the private sector will have a well bounded and relatively tractable problem versus opportunity with identity management and can set about it with vigour. In contrast, however, and by its very nature, the public sector has a much more

complex series of interlinked problems and opportunities and therefore has to move more cautiously than the private sector. The public sector as a whole must ensure its actions have a relatively precise desired effect with a context that requires subtle society, legal, regulatory and political matters to be appropriately handled or respected.

By way of illustration within the public sector, the medium term programme to introduce a UK national identity card will not complete until at least 2010 and even then it will not have achieved comprehensive coverage within the population. Yet achieving such a comprehensive coverage is precisely required to facilitate many other government activities demanded now in 2007 in terms of the way identities need to be managed. This is particularly relevant to transactions through portals such as Directgov and Businesslink and in diverse IT-enabled transformation programmes which urgently need identity solutions today. At the very least there is a need to urgently progress to new levels of sophistication of service provision so that the following questions can be addressed:

- Is this individual or business who or what they purport to be?
- Do they have a right to ask for a particular service or information?
- Who has a right to see, share or act upon data about this individual or business within the public sector organisation?
- Who has a right to see, share or act upon data about this individual or business outside the public sector?
- Who is my employee or contractor (that I know and trust)?

'Whilst private sector organisations are much freer to both act and quickly set up systems and services, they have to do so within larger regulatory and legal frameworks set by government and the wider public services'

The private sector is trying to meet similar expectations of service quality and problems in terms of trustworthy and reliable delivery. Whilst private sector organisations are much freer to both act and quickly set up systems and services, they have to do so within larger regulatory and legal frameworks set by government and the wider public services. Importantly, the financial services and IT solutions providers also force significant governance components to be considered. There has to be well orchestrated deployments of new processes and technologies or else confusion and partial solutions will proliferate.

The differing agendas between the public and private sectors and the potential areas for action are currently coming together in both the pan-Whitehall Identity Management Strategy Group, chaired by Sir David Normington, and also in the Public-Private Forum on Identity Management, chaired by Sir James Crosby. The latter Forum has four working groups – Convergence, International best practice, Consumer protection and Legislative barriers – that are particularly relevant to the issues discussed in this report. The Forum's terms of reference are:

- Review the current and emerging use of identity management in the private and public sectors and identify best practice.
- Consider how public and private sectors can work together, harnessing the best identity technology to maximise efficiency and effectiveness.
- Produce a preliminary report for the Chancellor of the Exchequer and the Ministerial Committee on identity management by Easter 2007.

The Forum will make proposals to the Chancellor and the Ministerial Committee on identity management in early 2008.

Somewhat independently, but also importantly from a concept convergence point of view, the academic and research communities are also actively addressing their specific identity management needs. They are particularly concerned with controlled access to on-line research and administration resources, student personal records, teaching and research resources, e-learning services and other electronic databases.

3.3 The individuals issue

An individual is of course just that, an individual, however in practice we perceive ourselves to have many different identities according to our circumstances at a particular point in time. Examples would include as a parent with respect to our children or as a child in relation to our parents, as either a giver or receiver of a particular service or set of services, or as employer or employee. As individuals therefore, we both need, and want to be able to have and to use, one or more

of various unique identities that are meaningful to us at a given time and for a particular purpose.

The new challenge facing us is translating the off-line, arguably more secure, behaviours to on-line commerce and experiences with confidence. We need to develop new risk management behaviours for a new and still changing circumstance which means there is an inescapable and urgent need to put in place the solutions that instil confidence in on-line transactions and activities. The growing pervasiveness of information technologies in both public and private environments is significantly increasing the requirement for us as individuals to identify ourselves successfully, reliably and consistently.

An occasional need to respond to identity requests is intrinsically neither burdensome nor intrusive, but the increasing need go through the same processes repeating the same, if not similar, information much more regularly can quickly become more difficult to accept. This then is the great opportunity for both an intrinsically trusted and much more automated assistance in identity verification. This is where the vendor community are beginning to provide a variety of tools and on-line services which help us as individuals to manage with the different aspects of managing our identities on-line.

Central government is clearly driving towards wider on-line access to public services for citizens. The primary route for access to such services is through the Government Gateway[1] which provides the means for an individual to register themselves by declaring their unique existence at one point of entry and so gain direct access to a wide portfolio of government services which are connected through the Government Gateway portal.

The private sector, whilst dealing with the same identity verification issues as the public sector, has identified a market opportunity in ensuring that individuals can find, audit and change personal information. The proposition is that the individual should remain 'in control' of their on-line identities and will welcome services to do so. Garlik[2] is an example of such a service:

Give power back to you. We give you the tools to manage your personal information.

Help you keep track. You can monitor your personal information online.

Stop data abuse. With total visibility of your online data profile there's less chance of abuse.

Keep you in the spotlight. Data security doesn't mean hiding yourself away. You decide how much or how little of your information is available online.

Offer you comfort and assurance. With your personal data under control you can use the web without the worry.

(www.garlik.com)

3.4. The common issue

While services like the Government Gateway and Garlik do help individuals and organisations handle some identity-related matters, they are effectively service offerings that we may or may not choose to use. As such they are not part of the 'natural infrastructure of the Internet' and therefore not providing the seamless experience that fundamentally does not get in the way of what we want to do on-line. They are no solution to the present fact that there is no 'identity management layer' in the interface to on-line services that the individual has clear control over. What's required is an intrinsic piece of functionality which authenticates identity in a reliable and acceptable manner to all parties involved across the Internet. This functionality cannot be exclusive or unique but instead must be based on a common set of acceptable principles and identity standards that all parties can use.

1 *www.gateway.gov.uk*

2 *www.garlik.com*

4. Solutions

The ability to both establish and manage an on-line digital identity or identities through a common identity management layer that is both all pervasive and an integral part of the infrastructure of the Internet becomes absolutely key to increasing the trust that on-line activities need. Considerable and deep discussion and collaboration has moved meeting this requirement sufficiently far forwards as to become tantalisingly close to reality today.

Kim Cameron's[3] work on defining the problem explicitly by clearly elaborating the boundary conditions of a complete identity system solution is widely regarded as the framework against which the performance of proposed technical solutions can be measured. Cameron identified seven Laws of Identity that together define a specification for a useable and trustworthy identity metasystem for the Internet:

1 ***User Control and Consent*** – Technical identity systems must only reveal information identifying a user with the user's consent.

2 ***Minimal Disclosure*** – The solution that discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 ***Justifiable Parties*** – Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 ***Directed Identity*** – A universal identity system must support both 'omnidirectional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

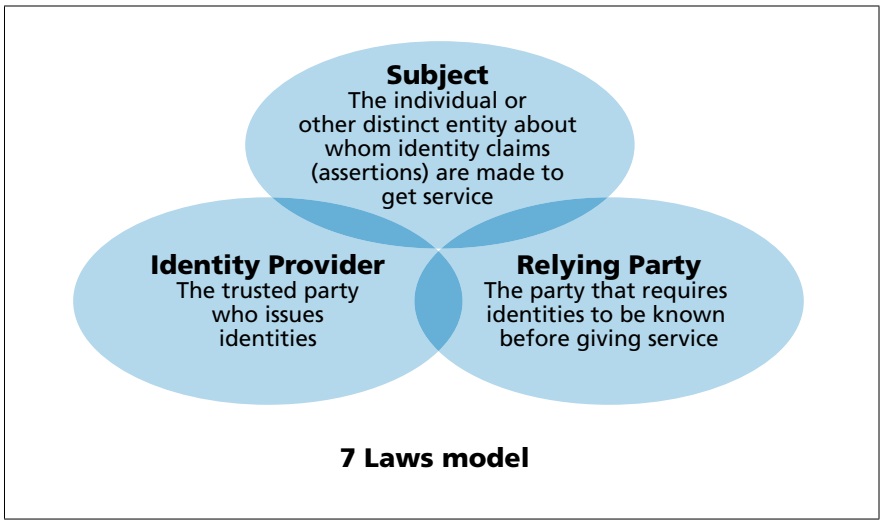
5 ***Pluralism of Operators and Technologies*** – A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 ***Human Integration*** – The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human/machine communication mechanisms, offering protection against identity attacks.

7 ***Consistent Experience*** – The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Cameron also clearly distinguishes the three parties (or roles) that need to interact reliably and with confidence and who lie at the heart of the identity metasystem. These he defines as follows:

- An **Identity** Subject (i.e. the individual) who directs an identity claim, or assertion, at a Relying Party.
- A trusted third party, the **Identity Provider**, validates the Subject's identity claim in a manner that the Relying Party is happy to accept.
- The **Relying Party**, having been assured by the Identity Provider's input, accepts the Subject's claim and provides the service requested.



7 Laws model

3 *www.identityblog.com*

To complete an identity transaction, the three parties participate in a carefully choreographed sequence of electronic messaging first declaring, then validating, then accepting the request to access a service or complete a transaction. Each electronic message has content within it that satisfies the specific requirements of the two participants engaged in each different step in the sequence.

The ability to pre-validate the identity of a subject by allowing the interaction between the Identity Provider and the Subject to take place independently is significant. It is by explicitly involving the familiar concept of a mutually trusted third party, the Identity Provider, that the all-round system trust and reassurance factors are achieved.

The practical utility of this can be illustrated by analogy with a financial transaction using a credit card: the customer's credit card is obtained in advance of any purchases and is, in practice, a 'financial identity credential' provider by a trusted third party – the credit card company – upon whom the retailer depends for payment.

'…it is well recognised that open standards and interoperable systems are a must for widespread customer acceptance of those solutions'

The IT industry has now developed a variety of technical and process solutions for identity management that accommodate some or all of Cameron's laws. Furthermore, it is well recognised that open standards and interoperable systems are a must for widespread customer acceptance of those solutions. Key to the whole succeeding, therefore, is effective deployment and the acceptability of those standards and systems across all three parties involved, which is beginning to happen. An example has been the deployment in OEM software packages of the 'digital wallet' which will contain an individual's digital Information Cards. These are their digital credentials – electronic versions of the familiar cards such as a membership card or cheque guarantee, debit or credit cards.

The Information Cards themselves are obtained from Identity Providers who effectively vouch for you as an individual or organisation as an Identity Subject to a third party – the Relying Party – from whom you are requesting a service. Relying Parties rely upon the Identity Provider and Information Card combination to guarantee that the Identity Subject is who they say they are and that the information that is provided via the card (for example, repetitively required data) is what it purports to be. Being electronically held digital data themselves, Information Cards can be stored and presented to a service provider from any electronic device as required by the individual.

Several major IT Vendors have now developed Information Card technologies and are integrating them in physical devices, software packages and on-line services. Microsoft, for example, provides their version of the digital wallet, Cardspace, as a free upgrade to Windows XP and as an integral part of the new Vista operating system. CardSpace can be found in most PC's Control Panel and can be set-up with ease and no cost to the individual.

4.1. UK public sector identity-related infrastructures

The solutions offered by the IT industry are available for use now and early adopters are already well into practical implementations and beta on-line services offerings.

However, for mass adoption of new ways of managing identity on-line, the overlap – or not – with the various public sector infrastructures being built in the UK, Europe and beyond is likely to be a critical factor.

Implementing presently novel concepts like digital Information Cards in conjunction with the UK National Identity Scheme and or the UK Government Gateway (described below), perhaps as part of publicly backed and regulated on-line Identity Provider services, is certainly technically possible but it has not been committed to as yet. The public sector generally follows rather than leads technology trends yet today it is just as keen and any private organisation to obtain the business advantages of on-line services adoption so perhaps this old pattern has had its day and a new, more innovative, culture will replace it.

4.1.1. UK National Identity Scheme

The Identity Cards Act 2006 gave the UK government powers to introduce national identity cards (ID) in stages spread over several years. In due course, the National Identity Scheme[4], the associated national ID cards and the National Identity Register

4 *www.identitycards.gov.uk*

will provide a personal identification system for all UK residents over the age of 16. Over time, everyone will have to have an ID card in the form of a smartcard containing some of their personal identity information from the Register and equipped with the capability to access the remaining personal information through various officially permitted channels and agencies.

The first phase is expected to collect biometric personal identity characteristics as part of the issuing process for passports and driving licences. This will be followed in 2008 with a voluntary ID card scheme which will begin filling the National Identity Register with personal information linked to new passport applications. By 2010 all new passport applicants will also be issued with National ID cards with full deployment of the cards expected to take several years after this.[5]

Clearly any government run National Identity Register or similar infrastructure[6] has the potential to be an important Identity Provider for a huge number of commercial and public service identity check scenarios. However, the legitimacy of using such nationally driven databases for purposes outside central government requirements is the subject of lively debate. Commercial use of the Register has not yet been ruled out and, potentially, could be an opportunity to part-finance central government's requirements in terms of ID management and data.

A critical component in today's and near-future planning considerations has to be the fact that the National Identity Register doesn't exist as yet and the definition of its use and exploitation is unclear making it an unrealistic option for the real on-line requirements of today.

4.1.2. UK Government Gateway

In contrast to the future UK National Identity Scheme, the Government Gateway[7] is in existence today and is both up and running and expanding in terms of the numbers of public services that are linked to it.

A recent proof of concept study with Microsoft and Sun Microsystems demonstrated that the Gateway can successfully operate with the Information Card model which, if adopted fully, would be a comprehensive environment within which an end to end identity management system would work.

Given its millions of volunteer registrations to date, it seems that the Gateway has an excellent opportunity to become a significant player in the citizen, business and agent Identity Provider marketplace and more. For example, its services could extend to Identity Provider services for managing government contractor and employee access to internal government systems. In its 2007 Pre-Budget Report and Comprehensive Spending Review (published in October 2007), the Government featured the importance of 'improving management of information and identity across the Government's delivery systems to reduce wasted time and inconvenience for citizens, businesses and frontline workers'.

4.2. Technology vendor identity solutions

4.2.1. Microsoft's Information Card solution

Microsoft's CardSpace identity selector implements the Information Card model within an identity metasystem consistent with Cameron's 7 Laws. CardSpace can be retrospectively added to an XP installation and is supplied fully integrated with the new Microsoft Windows Vista operating system.

5 *The details of this programme are controversial. Actual dates and actions may vary from those indicated here. As of August 2007, the government has issued a tender to run a procurement framework for the National Identity Scheme.*

6 *Other major public programmes with an identity dimension to them include 'e-borders' (already underway and due for completion 2014) and various Police and Criminal Justice programmes. The Varney Review (December 2006) called for more seamless government services accessed through a single gateway. The 'Tell Us Once' citizen-centric processes project is in response to this call.*

7 *The Government Gateway (www.gateway.gov.uk) is a service established by the UK Cabinet Office as a cross-government resource for the enrolment of citizens, organisations and appointed agents of citizens or organisations into on-line public services.*

'Windows CardSpace is client software that enables users to provide their digital identity to on-line services in a simple, secure and trusted way. It is what is known as an identity selector: when a user needs to authenticate to a web site or a web service, CardSpace pops up a special security-hardened User Interface with a set of "Information Cards" for the user to choose from. Each card has some identity data associated with it – though this is not actually stored in the card – that has either been given to the user by an identity provider such as their bank, employer or government or created by the user themselves.'
(cardspace.netfx3.com)

'CardSpace is part of Microsoft's implementation of an identity metasystem supported by open standard WS-* protocols. While CardSpace runs on Microsoft Windows, it is compliant with the supported WS-* standards and with other vendors' implementations on other platforms. In addition, other vendors can build implementations of CardSpace-like technologies to run on other platforms.'
('Is CardSpace Microsoft proprietary?' FAQ at cardspace.netfx3.com)

Two example implementations:
February 2007 – The German on-line department store, Otto (www.otto.de) launched the first CardSpace based application for general consumer use. There is a screenshots walk through at: blogs.msdn.com/vbertocci/archive/2007/02/03/otto-store-walking-through-the-cardspace-experience.aspx

October 2007 – In Singapore, myhealth.sg is a pilot web portal to help individuals manage their own health-related information, 'users authenticate with the application using a managed information card, backed by a hard token (Singapore's DORIS token)'. At the time of writing the portal is not open to the public but there is a screenshots walk through at: blogs.msdn.com/vbertocci/archive/2007/10/15/windows-cardspace-silverlight-help-singapore-to-get-easier-and-safer-access-to-health-data.aspx

The Derby City Council proof of concept detailed in the case study section of this report on page16 shows a real UK Public Sector example working for the benefit of all parties requiring access to Local Authority information and services.

4.2.2. Novell's Information Card solution
Novell's identity selector, called DigitalMe, is an open source implementation of Microsoft's Identity Card specification. It extends the range of suitable platform operating systems to include Linux and Macintosh.

'WALTHAM, Mass.— 12 Jun 2006— Novell today announced the creation of Bandit, a groundbreaking open source project with a charter to unify disparate identity systems and provide a consistent approach to securing and managing identity. The identity services in development by the Bandit community are open source and will work with existing industry standards such as WS- * and Liberty Federation, and open source projects including Eclipse Higgins. Novell has already contributed significant engineering resources and code to jump start this effort. Ultimately, the goal of the Bandit project is to provide organizations with a consistent approach to enterprise identity management challenges such as secure, role-based access and regulatory compliance reporting.'
(www.novell.com) (see also www.bandit-project.org)

'SAN FRANCISCO (Catalyst Conference) — 27 Jun 2007— The Bandit Project today hit another key milestone in the development of open source identity services with the availability of an open source, cross- platform information card selector that helps users manage "digital identity cards" used in Web transactions. Based on working code from the Bandit Project and interoperable with components from the Eclipse Higgins Project, the DigitalMe information card selector is functionally equivalent to Microsoft Windows CardSpace and runs on Linux and Macintosh platforms. The DigitalMe information card selector is being demonstrated today at the Burton Group's Catalyst Conference, with a test version now available as an installable package with a graphical interface. This marks an important step forward for user-centric, cross-platform identity management for Web-based services.'
(www.novell.com/news/press)

4.2.3. IBM/Higgins project
The IBM/ Higgins project develops the basic Subject/ Identity Provider/ Relying Party model further by giving additional levels of protection for an individual's data,

particularly aimed at preventing any party from being capable of building up a personal profile by observing an individuals 'digital footprint':

'This project is developing an extensible, platform-independent, identity protocol-independent, software framework to support existing and new applications that give users more convenience, privacy and control over their identity information.

'The initial motivation for Higgins was a desire to have systems that operated on behalf of the user – enabling the user to have more convenience, privacy and control over their identity and profile information. Because people want to share information differently in different contexts, (e.g. people share health information with a doctor, but not with a job search site), we realized that to build these types of applications there needed to be a framework that was aware of context and allowed information to be shared across contexts only in carefully controlled ways based on the underlying relationships.'
(www.eclipse.org/higgins)

'Building Privacy into Eclipse Higgins Open Source Security Project – IBM will contribute its Identity Mixer software to Eclipse Higgins project, an open source effort dedicated to developing software for "user-centric" identity management. The current trend toward a user-centric approach means that individuals can actively and securely control who has access to their on-line personal information, such as bank account and credit card numbers, or medical and employment records, rather than having institutions solely manage that information as they do today.'
(www.03.ibm.com/press)

4.2.4. Sun Microsystems' perspective

Sun offers a suite of products in the area of identity management. It features its commitment to open standards and interoperability in this domain.

'Since its inception, Sun has an ongoing tradition of supporting and leading development of open standards in the industry, such as Berkeley UNIX, TCP/IP, and VME bus. Sun continues to be an active member and leading contributor to a number of industry standards organizations – especially in the identity management space. Through participation in organizations such as OASIS and the Liberty Alliance Project, Sun fully supports the adoption of open standards and is committed to producing groundbreaking solutions that push the boundaries of innovation. At the same time, Sun strives to ensure that its technology is built upon and fully-integrated with established and emerging standards.'
(www.sun.com/software/products/identity/standards/index.xml)

From Robin Wilton, Corporate Architect, Federated Identity, Sun Microsystems, when commenting on identity system interoperability and customer choice of software and hardware device platforms:

'What Sun is interested in is ensuring that there can be interoperability between CardSpace on Microsoft Windows, and other implementations of the credential and identity selector concepts on other mass market devices and software platforms, such as Java-enabled mobile phones (billions of), digital TV set top boxes and the many kinds of smart-cards in circulation. We all want to be free to use the device of our choice to access on-line services provided by the private and the public sectors.

'In a world where there are multiple kinds of identity credentials and widespread expectations of free choice of access device, interoperability between identity solutions is absolutely essential. As a member of the Liberty Alliance, Sun is passionately for open standards for interoperability and identity and recently has worked with Microsoft and the Government Gateway service to ensure that the Government Gateway can handle both Liberty and CardSpace initiated service requests.

'An important consequence of an open and interoperable identity management environment is that service providers can continue to choose the technical infrastructures appropriate to their business needs regardless of the identity management solutions chosen by their customers.'

4.2.5. OpenID

OpenID[8] extends the ideas behind the unique identification of web pages to the concept of the unique identification of people. As each web page has a unique web address known as its Uniform Resource Identifier (URI), so an Identity Provider service can allocate a URI to a specific person after carrying out whatever verification it specifically requires. This approach to identity management requires the individual to memorise their OpenID URI in order to use their digital identity. In much the same way as with Information Cards, when an OpenID URI is used to claim access to a service the Relying Party first validates the identity claimed with the OpenID Identity Provider before allowing access to the service.

Whilst presently being used more widely on-line by the open source community, OpenID is also being taken up commercially. For current examples, see VeriSign's personal Information Provider (PIP) service[9] or Ping International's SignOn.com 'personal log in' service[10] .

4.2.6. Academic and research communities

The UK Access Management Federation for Education and Research provides for 'the communication of authentication, entitlement and attribute information between member organisations'[11]. The underlying technology being exploited is Shibboleth developed by Internet2, a consortium promoting advanced networking within the US research and education community. At the highest level of abstraction Shibboleth is both similar to, and based upon, the same basic principles as other identity management systems.

> 'Educational institutions are demanding a single sign-on solution that supports institutional authentication of all resources whether internal to the institution, through the use of collaborative platforms or to licensed third-party materials.
>
> 'Other countries have been developing their own solutions to the problem of accessing multiple resources with a single identity. A system based on international standards is therefore essential for publishers and other service providers who operate and compete at an international level.
>
> 'Federated access management separates authentication from authorisation. Authentication is controlled by the user's home institution; authorisation is based on user-attributes and controlled by the resource provider. This will mean less work in administering usernames and passwords.'
> *(www.jisc.ac.uk)*

Convergence towards seamless interoperability with the other identity management approaches is a critical component of the UK Access Management Federation's future vision; and likewise for Shibboleth as highlighted by the quotation below:

> 'ANN ARBOR, Mich – May 23, 2007 – Internet2 today announced its plans to develop extensions to Shibboleth to support Microsoft's Windows CardSpace and other compatible identity selectors.'
> *(mail.internet2.edu)*

5. Solutions convergence is happening

It is clear that a comprehensively deployed, working, and trusted identity management system is needed in the very near future. Fortunately there is both push and pull moving the IT industry in the right direction and they are willing to move.

Cameron's 5th law, *Pluralism of Operators and Technologies*, effectively *pushes* the international information technology providers to co-operate in the practical realisation of an identity metasystem. This in turn requires providers to move from individual (i.e. not interoperable) solutions to instead facilitating comprehensive and integrated user experiences at a variety of levels.

On the other hand, attention from law makers concerned to hold the IT industry more accountable for personal Internet security matters is threatening to *pull* providers away from previously entrenched positions, for example:

---

8 openid.net

9 pip.verisignlabs.com

10 www.pingidentity.com/products/signon

11 www.jisc.ac.uk/whatwedo/themes/access_management/federation/animation

'We therefore recommend that the Government explore, at European level, the introduction of the principle of vendor liability within the IT industry. In the short term we recommend that such liability should be imposed on vendors (that is, software and hardware manufacturers), notwithstanding end user licensing agreements, in circumstances where negligence can be demonstrated. In the longer term, as the industry matures, a comprehensive framework of vendor liability and consumer protection should be introduced.'

Personal Internet Security
HOUSE OF LORDS
Science and Technology Committee Report, August 2007

In response, the IT community as a whole is responding positively with new collaborative efforts and opening up intellectual property in a non-threatening and collaborative manner. Interoperability and technology convergence for the greater good at the global level are very much 'the mode of the moment'.

The Concordia Project [12] was recently established to:

'…help drive the development of use-case scenarios where multiple identity specifications, standards and/or other initiatives might co-exist, recognizing heterogeneous deployment environments of the marketplace.'

'The Concordia Working Group recognizes that deployers are working in a constantly shifting heterogeneous environment. In order to advance the identity marketplace, there needs to be a conscientious effort to develop systems, devices, applications and identities that will successfully and seamlessly interoperate. As such, this Group is chartered to:

- Become an active public discussion forum for the development, contribution and analysis of cross-protocol use cases for systems in a wide variety of vertical and horizontal deployment models.
- Drive virtual and public events that allow for discussion and development of use-cases and corresponding solutions.
- Develop, publish, and maintain a detailed roadmap to drive focused output'.

(www.projectconcordia.org)

Concordia needs to be congratulated for its success in bringing together representatives of all the distinct technical approaches in one project[13]. There are two factors that will likely prove to be of critical importance to its success in due course. Firstly, that all have recognised that close end user engagement in helping define the functionalities of the system that the stakeholders are jointly developing is a key success factor for the system. Secondly, that there is a genuine freeing up of intellectual properties via 'covenants not to sue', 'promises of interoperability and openness of standards' and 'waivers of licensing rights'[14].

Solutions convergence would be a substantial and unique achievement in terms of the global significance and impact this could have on the Internet and how the world trades online.

6. National Computing Centre Commentary

6.1. Opportunities for identity providers and potential new entrants to the market

Both Relying Parties and Identity Subjects will require the services of Identity Providers. This presents a series of new business opportunities which will have real market demand. These are summarised as:

12 www.projectconcordia.org

13 See the project's website for a matrix detailing what technical combinations they are covering

14 See the Microsoft Open Specification Promise at www.microsoft.com/interop/osp/default.mspx , the IBM Interoperability Pledge at www-03.ibm.com/linux/opensource/isplist.shtml, and welcoming commentary on the latter commitments from the open source community at osis.netmesh.org

- The requirement to provide digital identity credentials, predominantly Information Cards
- The provision of registration services that validate Identity Subjects' claims and identities before issuing credentials
- The need to provision the physical 'ID' cards or other smartcard based service functions required at the national level, assured by the rigour of the Identity Provider's registration and identity validation services
- Historic information services regarding a Subject's identity data and its use via Internet services – all within the context of the legal and regulatory requirements concerning use and communication of person-related data
- Historic market information services concerning requests to a Relying Party

6.2. Issues and opportunities for relying parties

Individuals will come to expect and require more advanced ways of controlling their personal identity data using different devices whilst at the same time receiving more and more requests to submit such information.

Relying Parties will have to refine and justify their requests for identity information from Subjects as control shifts towards the individual. This means Relying Parties must, at the very least, begin to align their technical architectures and internal processes to accommodate future demand from customers to use a comprehensive identity management system such as the Information Card-based model. This model requires electronic relationships with third party Identity Providers and so the latter become part of the Relying Party's service delivery and business models.

It is also conceivable and realistic that individuals and organisations will require a share of the value of their personal information from Relying Parties in return for giving up said information and certain rights to its use. This has an impact on Relying Party business models where making such data available for reuse for business intelligence and marketing purposes, for example, is envisioned.

As with Identity Providers, the wider identity metasystem will become part of the external context of Relying Parties' own enterprise architectures. A clear and quickly adopted identity management strategy could have a significant impact on mitigating the risk of siloed business systems (silos mean reduced ability to interoperate effectively) and promote greater horizontal process interoperability and agility throughout a relying party's organisation and its partners. The latter point is particularly relevant for those Relying Parties with more mature and sophisticated architectures. They will have new opportunities to 'plug and play' with business intelligence services provided by Identity Providers or other partners, leading to new business opportunities with associated revenue growth.

6.3. Issues and opportunities for public sector infrastructures

Government is both a provider and consumer of identity related services which raises some unique issues with far from straightforward solutions such as:

- Who can and should provide Identity Provider services for citizens and businesses utilising public services?
- What role is there for private sector services provision and for private sector participation in the utilisation of national public identity infrastructures?
- What regulation and levels of security should be applied to such services?
- What identity management services are required for purely internal purposes as opposed to those required for the citizen to access public services?

The business transformational potential of identity management technologies for the public sector is considerable. It could facilitate new options for standardisation and consolidation of the technologies and processes that lie behind public services delivery. Effective identity management also has a part to play in enabling trust and security in shared services and out-sourced environments. The service improvement and cost reduction opportunities could be substantial.

Realising the transformational potential will require considerable and close interworking within the IT professional community inside government, backed

up by close contact between government and wider industry expertise in identity management strategy, deployment and operation. The upcoming outputs from the Public-Private Forum on Identity Management chaired by Sir James Crosby[15] should be awaited with anticipation in this area.

6.4. IT suppliers

IT suppliers have a unique and important role to play as leaders of identity management technology development driven by their customers' business requirements and demands.

The supplier community fully understands the potential and actual technical and business benefits of better identity management if applied within both internal business activities and in the global on-line economy. The IT supplier community are proactively raising awareness through educational programmes and proof of concept demonstrators, showing how to deploy and get benefit from identity management solutions which address the problems and opportunities that businesses are facing today.

In the mass marketplace, individuals are being encouraged to use public and private on-line services despite an element of scepticism surrounding on-line security and potential 'big brother' abuse of their digital identities. The IT supplier community must address the challenge of educating this broad community over time by proving that whilst reducing risk these tools and solutions do provide a massive benefit.

Key to the success of any awareness and education programme for the individual is re-enforcing and proving that technology in general is inherently reliable, trustworthy and secure. This is not an isolated IT supplier issue to resolve. The government, financial institutions, identity providers, online traders and all the other on-line services providers must have a consistent message to convince the public of the same trustworthiness and re-assurance. The public needs to be convinced that technology-based transactions and identity management can be as reliable, trustworthy and secure as their off-line alternatives.

7. Conclusion

The critical success factor for the mass deployment of identity management technologies is therefore meeting the challenge of achieving a critical mass of positive perception in two areas:

- The services needing to trade and transact on-line.
- The general population who will be their customers.

This position achieved, virtuous circles of demand leading to increased use of the technologies leading to yet more demand will build momentum and further trust and credibility very quickly. Proven identity system interoperability delivering seamless access to services online will be a very attractive proposition.

Perhaps obviously, the Information Card concept appears to be a natural extension of the off-line identity world. Exploiting this cultural congruence (as far as it goes) will help their widespread acceptance via educational and marketing campaigns.

8. Case study – Information Cards for online public services

Public services in the UK are being driven to improve the volume and quality of provision of on-line services for citizens, businesses, service delivery partners and for their own employees.

Public service providers must strike a balance between controlled and auditable access to personal and public service information and giving citizens and others ease of access to on-line services under conditions that do not imperil public trust or public security. If either trust or security is compromised, then there will be less use of the on-line services to the disbenefit of all.

In spring 2007 and at the request of Business Link, the Government Gateway (Directgov), the London Borough of Newham and Derby City Council, Microsoft and application partners undertook six proof of concept identity management studies. Each proof of concept used life-like scenarios that illustrated the key identity related processes of:

15 *www.hm-treasury.gov.uk/independent_reviews/identity_management/identity_management_index.cfm*

(a) Obtaining managed Information Cards

(b) Storing cards in a CardSpace 'digital wallet'

(c) Using the CardSpace identity selector to select and present Information Cards to obtain service

(d) Granting controlled, role based access to services appropriate to the entitlements of the Information Card owners.

The scenarios deliberately employed mixed populations of citizens, businesses, service delivery partners and public employees utilising the model on-line services, thus demonstrating that the Information Card approach works both technically and by bringing benefits to both businesses and customers.

The six proof of concept scenarios were:

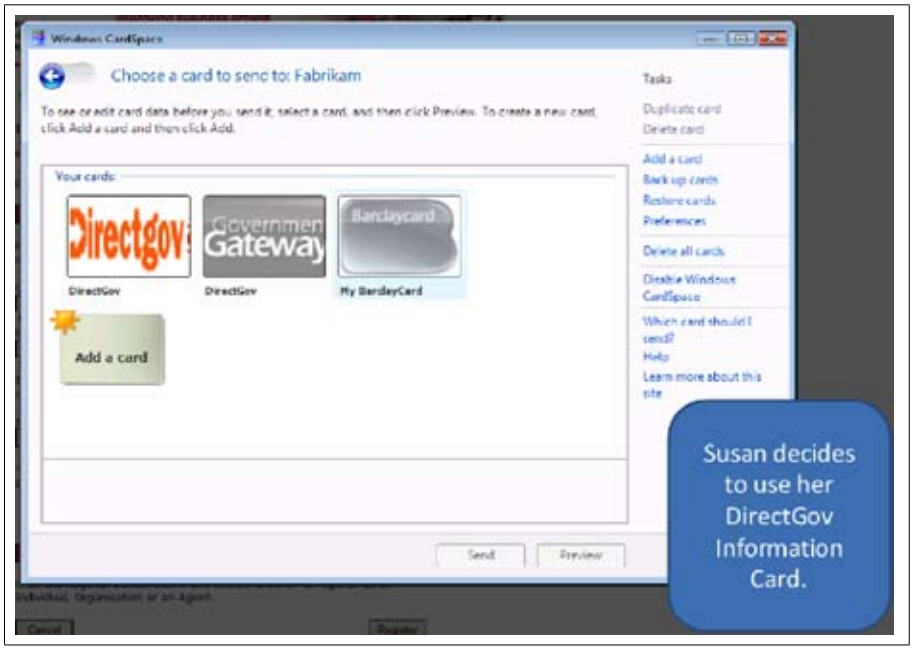
1. Registration for access to on-line VAT and HM Revenue services through the www.businesslink.gov.uk website using a Business Link Information Card.
2. Access services provided by the DVLA using a Directgov Information Card and the Government Gateway.
3. Controlled access services for Council employees dealing with fostering children: accessing Child Social Care Records through the London Borough of Newham's website using a Directgov Information Card.
4. Using Information Cards from both public and third party private service providers to access an individual's citizen account at Derby City Council and then launch, and follow progress with, a service request.
5. Using Information Cards to give a nurse working in the Newham Primary Care Trust controlled access to Newham Council's back office systems via the Council's extranet. Then extend the scenario to include nurse and patient access to a common online service using managed Information Cards.
6. Giving Citizen's Advice Centre staff access to Derby Direct systems to let them create, manage and follow through a client case workflow. In the later stages of this scenario, additional access is granted to a Council member who takes an interest in the case. This scenario shows different types of Information Cards being used to authenticate a government employee, a voluntary sector worker and a citizen, giving each role-based access to the Derby Direct on-line systems.

Some screen shots from scenario 3 illustrate key stages common to all the scenarios:

Susan is a government employee wanting to access children's records on-line. She goes to the Council's Fostering home page. There is a button for 'Online Services'. Susan selects that button, launching a 'sign in' process…

Screen 1

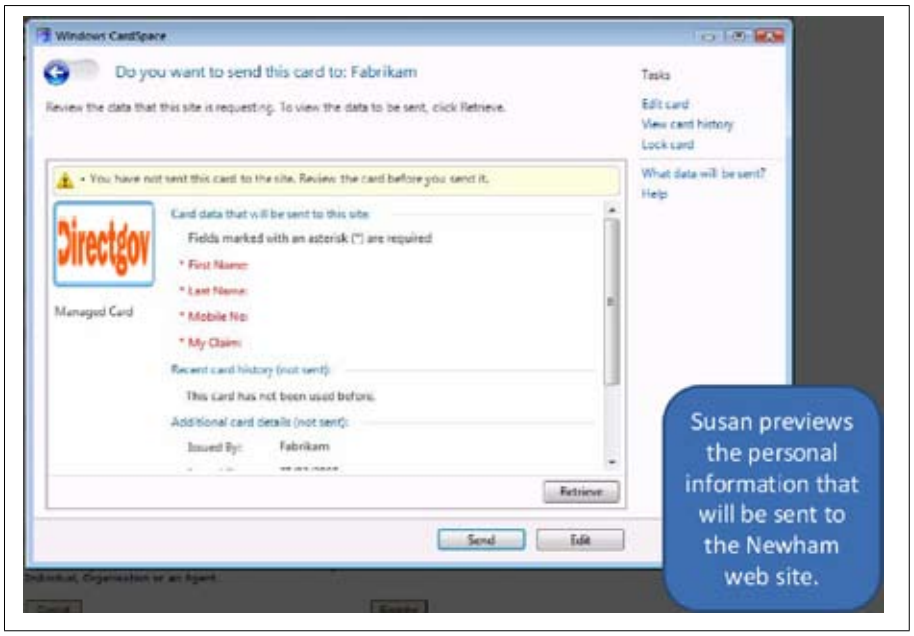
During the 'sign in' process, Susan indicates that she has Information Cards in her CardSpace identity selector and the CardSpace window opens. She'll select the Directgov card to send her personal identity information to the Council's website…



Screen 2

Before the Information Card is sent to the Council's on-line service, Susan has an opportunity to review the personal data contained in the Directgov card she has opted to use – Screen 3.

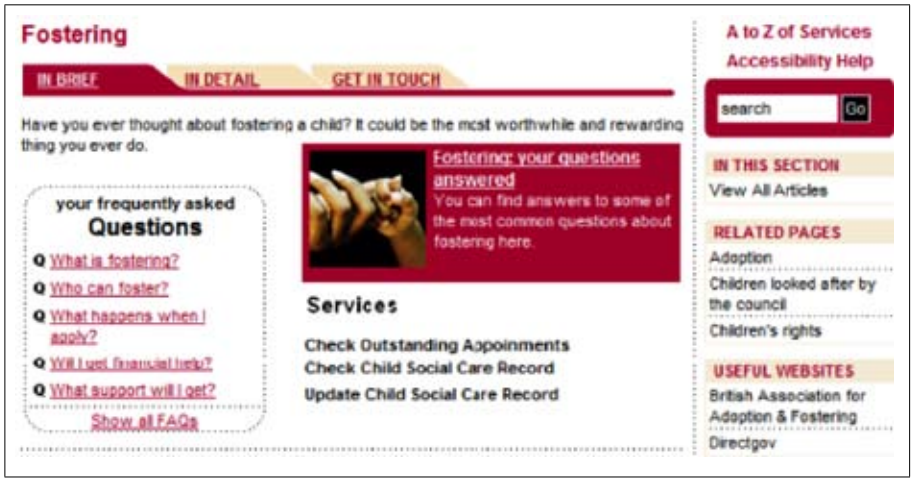
We can see that the card contains personal data that is frequently asked for but tedious to constantly have to re-enter. Sending the Directgov Information Card does that for Susan automatically instead. Here Directgov is the Identity Provider who is assuring the Relying Party, the Council website, that the Subject, Susan, claiming an identity is who she says she is.



Screen 3

Having selected and submitted the personal information she wants to reveal via the Directgov Information Card and completed a further security check, the Council's website re-presents the original web page to Susan slightly modified – Screen 4.

There is now a selection of three services for Susan to select – just the services appropriate to her role in the system. Only Susan sees this web page in this session on-line. Any other random persons visiting the Council's Fostering page at the same time will see Screen 1.



Screen 4

Some commentary from the proof of concept participants:

Richard Steel
CIO, London Borough of Newham
'Personal identity management and the subtleties around it are not yet well understood in government and in the provision of on-line public services.

'Councils want to get as many services on-line as possible for a number of reasons, e.g. less cost, greater efficiency, a better citizen experience. Wherever such services require the use of personal identity related data, satisfactory identity management becomes critical to getting these benefits realised – you need to be 100% sure who you are dealing with.

'Identity management solutions that can be cross-industry supported and federated across multiple organisations' systems are really needed right now. We've now seen Microsoft's implementation of these concepts in Information Cards and CardSpace and I want Newham's employees, citizens and businesses to get the service benefits of these technologies sooner rather than later.'

Chris Haynes
Director Electronic Delivery Team, Cabinet Office*
'The challenge of on-line government has changed in recent times. At one time it was about the accessibility and availability of on-line services. The challenge is now building public and business confidence in those on-line services.

'The Government Gateway is a key player in the pan-government approach to identity management. It is in a unique position to deal with other sector partners, e.g. in the 3rd and private sectors, and together we are coming to a general consensus about how on-line services should be secured.'

Jason Gruber
Head of Information Services, Derby City Council*
'Information cards are a great way for you to manage your own identity on-line. They allow you to get identities that mean something to you as the individual and then to be able to choose which ones you want to use when you're actually accessing websites on-line. This enables trust for the websites and for you.

'Derby City council are interested in Information Cards because they provide a sustainable, long term value for money solution for identity management for customers and businesses.'

Dr Steve Marsh
Intelligence and Security Adviser, Cabinet Office*
'We need to try to get some more familiarity and commonality across the [on-line identity management] mechanisms so that individuals know if they are dealing with a legitimate organisation or whether they are being spoofed by criminals.

'The Information Card concept and mechanism is a way of doing that. We are hoping it will be widely accepted across both the private and public sectors and [come to] provide a very familiar and trustworthy environment that the individual can deal with on-line.'

Jerry Fishenden
UK National Technology Officer, Microsoft*
'The issue of identity management is not going to be solved by a single company or organisation alone.

'So, on the technology side, you're seeing Microsoft, Novell, IBM, Sun and many others pull together and cracking the technology issues. But equally importantly, if not more so, the people that actually issue the identities that we can use online [are cooperating too].'

* Thanks to GBTV (www.gb.tv) for access to the video interviews from which these quotations were extracted. The video can be seen at http://www.localgov.tv/cgi-bin/details.pl?action=pre&id=298

9. Glossary of identity terms

There is a wide variety of identity management terms in use and not all authors use the same semantics. The definitions of the primary terms given below are fairly well fixed, less so the secondary terms derived from combinations of primary terms or from linking primary terms to non-IT enabled processes, and even less so tertiary terms etc.

Primary terms

Subject – The object (usually a person but could be any other distinct entity, for example, a car or a cow) which may direct a claim of identity at another party.

Identity – What is claimed when a Subject requests a service they believe they are entitled to as a consequence of their existence.

Relying Party – The party who is being asked to accept the Subject's claim of Identity and provide service.

Identity Provider – The party who issues Identities to Subjects that are suitable for presentation to Relying Parties. An individual can be their own, i.e. self-asserted, Identity Provider but it may not be trusted by many Relying Parties!

Secondary terms

Verification (of a Subject's identity) is the process by which a Subject's claim of Identity is validated to a pre-determined level of rigor. Verification may be achieved by a number of means: for example, in order of increasing rigor, by self-assertion, by physical or digital Credentials provided by third parties or by biometric information if the Subject is an organic entity.

Credential – An object, a piece of data or some information from a third party that is presented by a Subject to support their claim of Identity. In the physical world, this could be a utility bill, driver's licence or personal/company credit card etc. In the on-line world, this could be an Information Card or other form of digital certificate.

Authentication (or Authorisation) (to get access to/provision of a service) is needed before a service requested by a Subject is given by the Relying Party. If successfully Authenticated, the Subject gets the service. Authenticating service access/ provision may involve one or more Verifications of Identity claims and other conditions such as requiring a physical token (a kind of Credential).

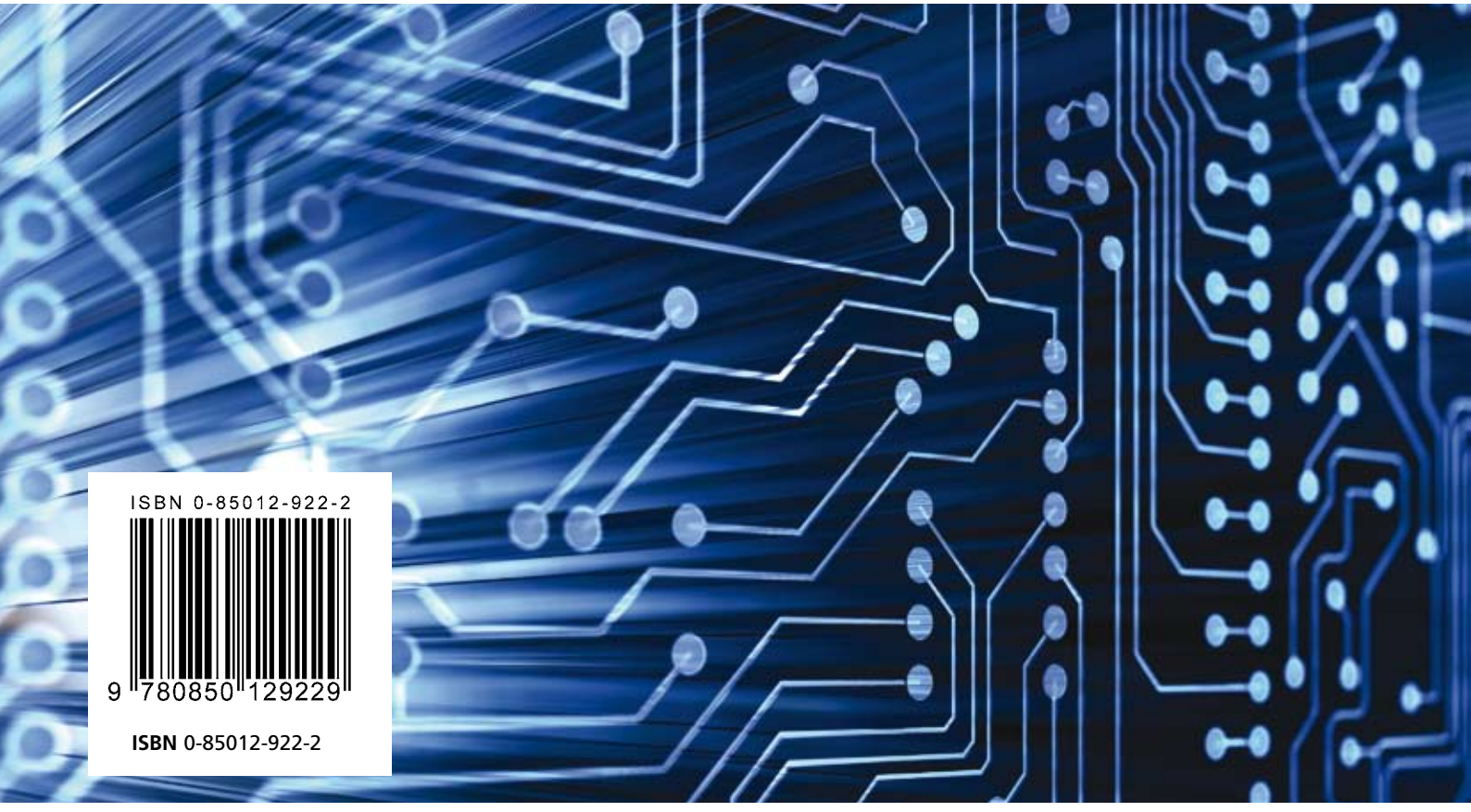
Further derivative terms

Entitlement is a summary statement of the rights of a Subject to a service. If the service is an on-line service, Entitlement is the result of passing the one or more stages of Authentication required by the service provider, i.e. 'by the presentation of acceptable credentials it has been verified that you are indeed permitted to use this service and the necessary authorisation to use the service now is granted'.

Other commonly used terms include ***Enrolment*** and ***Registration***. Descriptions of such generic processes can usually be constructed using combinations of the more fundamental terms above to describe the distinct activity steps performed during the process.

National Computing Centre
Oxford House
Oxford Road
Manchester M1 7ED

Tel: +44 (0) 161 242 2121
Fax: +44 (0) 161 242 2499



ISBN 0-85012-922-2

9 780850 129229

ISBN 0-85012-922-2

NCC National Computing Centre