TOWARDS A USER CENTRIC MODEL FOR IDENTITY AND ACCESS MANAGEMENT WITHIN THE ONLINE ENVIRONMENT

by

Matthew Burns Deas

TREATISE

Submitted in partial fulfilment of the requirements for the degree

M TECH: Business Information Services
in the School of ICT
at the Nelson Mandela Metropolitan University

Supervisor: DR. S.V. FLOWERDAY

January 2008

Author's Declaration

I, Matthew Burns Deas, hereby declare that:

- The work in this treatise is my own work.
- All sources used or referred to have been documented and recognised.
- This treatise has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

_____

Matthew Burns Deas

5 January 2008

Abstract

Today, one is expected to remember multiple user names and passwords for different domains when one wants to access on the Internet. Identity management seeks to solve this problem through creating a digital identity that is exchangeable across organisational boundaries. Through the setup of collaboration agreements between multiple domains, users can easily switch across domains without being required to sign in again. However, use of this technology comes with risks of user identity and personal information being compromised. Criminals make use of spoofed websites and social engineering techniques to gain illegal access to user information. Due to this, the need for users to be protected from online threats has increased. Two processes are required to protect the user login information at the time of sign-on. Firstly, user's information must be protected at the time of sign-on, and secondly, a simple method for the identification of the website is required by the user. This treatise looks at the process for identifying and verifying user information, and how the user can verify the system at sign-in. Three models for identity management are analysed, namely the Microsoft .NET Passport, Liberty Alliance Federated Identity for Single Sign-on and the Mozilla TrustBar for system authentication.

Acknowledgements

I would like to thank the following:

- My supervisor, Dr Stephen Flowerday, for your guidance, support and patience throughout the development of this project.
- Michelle, my love, thank you for all your encouragement and concern throughout this course.
- Thanks to Mrs Janice Richter who was of great assistance in her capacity as proof-reader.
- Special thanks to my family for all of their words of encouragement and support.
- Most of all, God, through Whom all things are possible.

Table of Contents

List of Figures and Tables

Figures:

Tables:

Chapter 1

INTRODUCTION

1.1 Prologue

With the great wave that has swept across the world in the form of the Internet, most people with Internet access have had an online identity created for them, in some cases without the users' direct knowledge. Through the dot net boom of the 1990s and the subsequent crash of a number of these websites, the Internet and online purchasing have become more and more popular. Companies and individuals have placed websites online, selling a variety of items from books to cars, all with online systems that have basic sign-in procedures. These websites, Amazon and EBay for example, make use of complex analysis techniques that continuously build user profiles and user preferences, and offer to remember customer related information such as credit card information. All of this information is being collected through the relatively simplistic method of user sign-in tools such as the username and password. But what are the implications of this simple sign-on methodology that is used in these environments and ultimately how can it be ensured that the user that is connecting to the system is who he claims to be?

In order to understand the full scope of the problem, analysis needs to first take place to show the basics of the online environments and the way in which users act within them and the way in which they maintain their online identities. An online identity is defined as a social identity that network users establish in online communities (Wikipedia, 2007). Essentially an online identity is a representation of a physical person's identity on the Internet. This online entity can have multiple pieces of information attached to it, such as contact information, ID numbers and banking information, depending on the nature of the website. A number of methods of social engineering are used in order to gain access to user information. The most notable of these forms of information theft is the practice of online phishing.

The Oxford English Dictionary defines phishing as, “Fraud perpetrated on the Internet; specifically the impersonation of reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.” (Oxford English Dictionary, 2006). Granova and Eloff (2005) give a comprehensive definition, stating that phishing is, “the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft”. The exact meaning of the word phishing has changed over the past few years as the techniques to acquire information unlawfully have become more complex. Fake websites, key-loggers and the use of Trojan Horse malware are now considered part of phishing attacks (Ollman, 2004).

The sequence of successful phishing attacks can be described as:

- Phisher prepares for attack
- Malicious payload arrives at the recipient through a propagation vector
- The user takes an action as a result of the delivered payload
- User is prompted for confidential information, through the use of a website or through a Trojan Horse
- User compromises confidential information after believing the request to be genuine
- User confidential information is transmitted from the user to a phishing server setup by the phisher
- Confidential information used by phisher to successfully impersonate the user
- Phisher engages in fraud using compromised information (Emigh, 2005).

It has been reported that the Association for Payment Clearing Services recorded fraud losses from online phishing scams in the UK reaching £12 million in 2004 (Caslon Analytics, n.d). It is clear that a simple username and password is not always the best solution to the management of an online identity as it is open to abuse and fraud. In a recent report it was shown that phishing attacks have increased by 8000% over the period from January 2005 to September 2006, mainly due to more organised criminal activity in the phishing area as well

as the increase in awareness for security protocols from the banking industry (Phishing Increases as Users Get Wise, 2007). This claim is shown to be true when examining the banking sector. Standard Bank has implemented numerous security measures, such as one-time password usage per client login, to their banking systems, and is compliant with international Internet security protocols while making use of 128-bit encryption, ensuring that no third party can gain access to client information (Standard Bank, n.d). The same is also seen in Absa Bank's implementation of a similar one-time usage password for each transaction (Absa, 2006).

In order to effectively deal with the risks inherent within this turbulent environment, the use of proper identity management principles need to be applied at the time of users signing on to systems. Identity management is defined as, "a broad administrative area that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity" (SearchVoip, 2006). A simple example of identity management is that of driver licensing, in which drivers are identified by their license numbers and limitations, (such as being specified that a driver must drive with spectacles) and are thereby linked to the license number. Identity management should be viewed as a tool for promoting the reduction of uncertainty between parties and a process to ensure that users are who they claim to be. The process for verifying that a user is who they claim to be is known as authentication.

Authentication is defined as the process of verification of the credentials of the entity attempting to make a connection to the service. The process involves the sending of user credentials from the client to the server via a plaintext or encrypted form in the use of an authentication protocol (Microsoft, 2005). The process of authentication is not to be confused with that of authorisation, defined as the confirmation that the connection attempt to the service is allowed, and occurs after a successful authentication of the user, when access is granted based on user rights (Microsoft, 2005). The difference between the process of

authentication and authorisation can be seen in a basic implementation of user sign-on as performed in the Kerberos System in Figure 1.1

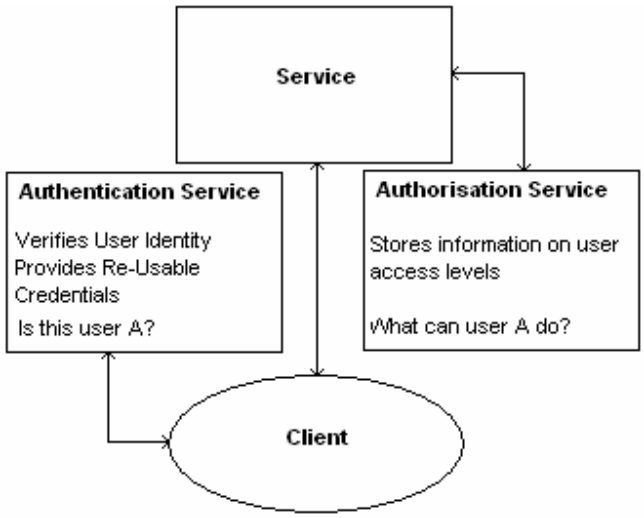

Figure 1.1 – Authentication & Authorisation Interactions in a client/server application (Duke University, n.d)

In Figure 1.1 the client or user makes an attempt to connect to the service. When a connection has been made to the service, the authentication service is called to verify the user's identity and validate that they are whom they claim to be. After the authentication process has completed, the authorisation service will be called by the initial service which was called by the client and will be responsible for the granting of access to the client, based on user roles, for use of the system (Duke University, n.d.).

To ensure users are who they claim to be, especially within an online environment in which stringent controls are required (as in the banking sector for example), the use of an authentication tool other than that of only a single key authentication password is required. This can be shown by the implementation of such processes as Absa's use of a Random Verification Number (RVN), as used for a one time only login key for each electronic banking session (Absa, 2006). The use of dual key authentication over that of single key in the form of passwords promotes a greater feeling of trust from the user to the service provider as the controls used to guarantee the correct user authentication are higher. Depending on the viability of the use of the technology as well as whether the technology is

necessary to meet the security requirements, in certain situations the implementation of a biometric authentication solution may be considered.

Although large corporations have been set up in order to standardise the processes for online identity management and sign-on procedures, the risk still exists that an unauthorised individual could gain access to another person's account information. Larger corporations such as Microsoft are attempting to stabilise the situation through the introduction of their own ideas of standardising the online authentication methods through .NET Passport. There have been a number of problems, even a case where users' online wallets could have been compromised due to a gap in Passport's security (McWilliams, 2001). A similar situation was uncovered in 2003 when a security loophole within Passport allowed attackers to obtain the passwords of early .NET Passport adopters by giving only minimal personal client information, such as an e-mail address and postal code (McCormick, 2003). On top of this issue is the magnitude of usernames and passwords for each different account. Users are supposed to remember these without the use of pen and paper, as writing them down could compromise their security.

1.2 Problem Statement

1.2.1 Main Problem:

What processes must be adhered to by the client user and the website, to ensure the protection of the user's identity in the online environment?

Due to the ubiquitous nature of the Internet and computing, users are unknowingly connecting to online environments that have simple client authentication processes. The authentication process may occur on fraudulently set up spoofed websites. This exposes the user to the risk of potential identity theft, resulting in possible financial losses.

In a recent survey showing the incidents of online fraud, it was reported that the online loss of revenue due to fraud has risen from $1.5 billion in 2000 to $3 billion in 2006. (CyberSource, 2007). This statistic is further supported by another report showing that losses within the United Kingdom rose by 55%, from £14.5 million in the first half of 2005 to £22.5 million in the same period in 2006 (Young, 2006). Due to the large increase in online fraud within the last few years, it has been suggested that merchants be far more careful when deciding which orders they fulfil and which they will reject. Rejections by U.S. based merchants are up to 13% for all orders originating outside the U.S. (Sullivan, 2004).

Surprisingly, in the face of the large sums of capital lost to online fraud, a joint study between Washington University and Princeton University discovered that there was a notable lack of concern from online users about trust in the online environment, online identities and online interactions (Friedman, Nissenbaum, Hurley, Howe & Felten, 2002). This statistic is alarming due to the clear rise in online fraud and identity abuse over the past few years. It is unsurprising that unlawful acts are perpetrated against individuals online in order to gain illegal access to information and the theft of online identities.

1.2.2 Sub-Problems:

- **What are the critical success factors for identification and authentication of a user at time of sign-on?**
- **What process can be used to ensure a user is connecting to an authentic website?**
- **How can users be adequately protected from common online threats?**

The above identified sub-problems are based on the main problem previously defined. By answering each of these questions a set of processes can be defined. Each of these processes will contribute in addressing the research problem, and once all three problems have been solved, this will mean the main research problem has been addressed.

1.3 Objectives

The objective of this study is to produce a model through which users can experience a more secure online environment by making better use of existing identification and authentication procedures. These improvements should ensure that the individual with the proper security access can link to the secure environment, and guarantee that they are who they claim to be, whilst ensuring that the website attempting to be accessed is authentic. This process should be performed through the use of multiple forms of authentication and authorisation methods, protocols and controls.

1.4 Methodology

The research will be performed by means of an extensive literature review in order to gain more knowledge and to make inferences from the work of experts in the field of identity and access management within the online environment. As this research will be performed by means of a literature review, the sources of data will stem from journals, academic papers, books, case studies, news articles and examples from around the world. The research will be performed using the process of qualitative and interpretive research methods. Systems Theory will be examined through the course of this study, showing how one process change will have an impact on another.

1.5 Outline of the Treatise

The treatise provides a background to user identification at the time of sign-on to online systems. This is done by investigating the needs of the online environment, and the process by which users are verified in order to gain access to the online environment. Chapter 1 provides a background to the problem of identifying users in an online environment, the potential problems within the sign-on process due to illegal activities, and begins to look at the overall guidelines of identity management, such as identification and verification processes. The focus moves towards identity management processes and the security practices surrounding online environments to provide an overview of identity management and begins to delve into how users are identified as who they claim to be in Chapter 2. In

Chapter 3 the focus moves to authentication management and authorisation procedures, and the requirements to identify who a user of the system is. Chapter 4 investigates models that are currently used in the process of identifying users at the time of sign-on to online systems. Particular attention is given to the current business leaders in this field, with Microsoft's implementation of the Single Sign-on identity domain in .NET Passport. The implementation of the Federated User Identity Model promoted by Liberty Alliance will be examined. Finally, a look at Mozilla's TrustBar implementation of the personal service provider identity model, which incorporates the use of personal authentication devices within identity management, will be examined. A comparison and critical analysis of the models described will take place in order to show the strengths and weaknesses of these different implementations and gather some insight into how they can be improved. In Chapter 5 recommendations are made regarding the lessons learned from the critical analysis of the models in Chapter 4, specifically looking at integration of traditional user identity management models, with user-centric identity management models. A conclusion summarising the ideas expressed through this study will be in Chapter 6, providing an overview of the entire treatise by summarising the main concepts of the document.

Chapter 2

IDENTITY MANAGEMENT

In the constantly changing world of information technology and the inherent threats of new technologies to businesses, identity management and information security are of major concern for organisations. Processes are required to manage compliancy of country specific laws and effectively manage business risks. The process of putting effective controls in place to counter these business risks can be a source of confusion. This chapter will begin with a brief overview of identity management in order to fully understand why it is required and what is involved in the managing of a user identity. The overall requirements for the attributes of an identity are described to show the nature of user information that needs to be protected. The chapter then moves on to the identity management life cycle in order to understand the process that should be followed in order to successfully manage an identity. The requirements for identity management systems in both the public and private sector are then discussed. The role of an identity in the online environment is discussed within digital identities. Possible solutions are then proposed in order to determine the best way for implementation of an identity management solution within an enterprise. The business benefits of using an identity management solution will be shown by looking at previous implementations in well established companies such as Fujitsu, PriceWaterhouseCoopers and Onyx. Finally a look at the different standards initiatives will take place, focusing on Liberty Alliance and Microsoft.

2.1 Identity Management Overview

As the possible uses of the Internet continue to be realised, companies and users require more control over the identity-related information belonging to a given person. This information is often scattered in a multiple number of systems throughout the organisation, some of which may even be controlled by third party suppliers (Sarbanes Oxley, 2007). The scattered nature

in which this data is stored causes problems when attempting to create a seamless experience for users. This is because the accessing of this information for authentication purposes, takes place across multiple different systems.

Governments have enacted strict laws and regulations for different types of industries for the protection of information. Compliance with these regulations is not an option but a strict requirement. Audits need to be regularly performed to gauge an organisation's adherence to these regulations. Failure to comply can result in heavy fines and delays in moving specific products into the market. The existence of scattered storage of identity management information makes compliance and audits extremely difficult. Table 1 provides some examples of the type of laws which have been implemented for the use of identity information.

Law / Regulation	**Coverage**	**Description**
Canadian Personal Information and Electronic Documents Act	Privacy	Applies to companies operating within Canada. Defines rules for protection of personal information, collection, usage and disclosure for commercial activities.
European Data Protection Directive	Privacy	Applies to companies within the European Union (EU). Addresses identity theft, online fraud and privacy issues of consumers, employees and citizens. Designed to standardise privacy laws in EU member states.
Electronic Signatures in Global and National Commerce Act	Electronic signatures	Applies to companies operating in the U.S. Allows for use in particular circumstances for legally binding electronic signatures.

Health Information Portability and Accountability Act (HIPAA)	Privacy	Applies to health care companies within the U.S. Calls for controls to safeguard health information on patients. Establishes patients' rights to control access of their personal health information. Requires technical standards for access controls, audit, authorisation, data authentication, network authentication and security.
Food and Drug Administration Rule 21 CFR 11	Records retention, electronic signatures	Applies to pharmaceutical and other firms operating in the U.S. Defines requirements for the control of electronic records, electronic document submission, and criteria for approved electronic signatures.
Gramm-Leach-Bliley	Privacy	Applies to financial services firms in the U.S. Requires service providers to establish administrative, technical and physical safeguards to ensure the confidentiality of customer records. Prohibits firms from disclosure of customer information without the consent of the customer.
Sarbanes-Oxley Act	Accountability	Applies to public companies in the U.S. Requires annual reports to assess effectiveness of internal controls and procedures (including identity management) for financial reporting.
Securities and Exchange Commission Rule 17a-4	Records retention	Applies to securities brokers in the U.S. Requires brokers and dealers to keep original documentation of all communications received and sent by a firm relating to their direct business. All account records have to be retained for six years.
Customer Identification Program (U.S. Patriot Act)	Privacy, record retention, identity verification	Applies to financial services companies in the U.S. Requires processes for risk-based identification of new customers. Companies must collect identity information from customers, verify that information, and compare that against government lists of known/suspected terrorists.

Table 2.1 - Relevant Laws and Regulations (Lewis, 2003)

With the examples of legal requirements shown above identity management has been recognised as a means to control system access and reduce financial risks. In order to realise this, a comprehensive approach to identity management is required, which warrants interoperability within applications. These approaches should allow for the exchange of authentication, authorisation and other identity-related attributes, as well as identity-related operation requests in a standard and secure manner, thereby enabling users to get a personalised service experience, without requiring them to store personal information centrally. Identity management solutions should therefore offer scalable, secure and reliable services (BMC Software, 2006).

Overall identity management needs to be seen by businesses as a tool, which allows for them to adequately manage their systems securities. The legal requirements are often put into place to provide a code of "best practice", which can be seen in most implementations of corporate governance such as COBIT and ITIL. Ultimately the company is responsible for the way in which they use identity information and are liable should that information fall into criminal hands. In order to fully understand the concept of the form of information which companies will store, the inherent characteristics of an identity must be examined.

2.2 Elements of an Identity

An identity in respect of the online environment is an expression of individual's unique characteristics in a format that is able to be recognisable online. The type of information that may be used in both physical and online existence is that of ID numbers, banking information, and postal addresses.

De Leeuw (2004) specifies three different types of identities. The first is a biometric identity which is based on the physical attributes of the individual. These physical attributes include DNA, face recognition, and fingerprint identification. The second type is an Attributed identity. This includes all data that is attributed to the individual such as full name, date and place of birth along with other forms of physical information. The third type is the

Biographical identity. This includes information on education, criminal record, taxes, employment, and a multitude of other information normally described as private in nature.

Due to the often sensitive nature of these types of information, and the large scale of fraud in the online environment, as mentioned in the introductory chapter, it is vital that identities are managed correctly within companies, for both customer's and employee's safety, and the reputation of the business should that information be compromised. The identity management life cycle provides a strong basis for the management of customer and employee identities.

2.3 Identity Management Life Cycle

In order to successfully control identity management, an understanding of the life cycle of identities is required. The first step in the solution to a more secure user environment is the implementation of proper identity management principles by businesses. It is imperative that businesses make proper use of each step in the identity management life cycle to manage user profiles and information.

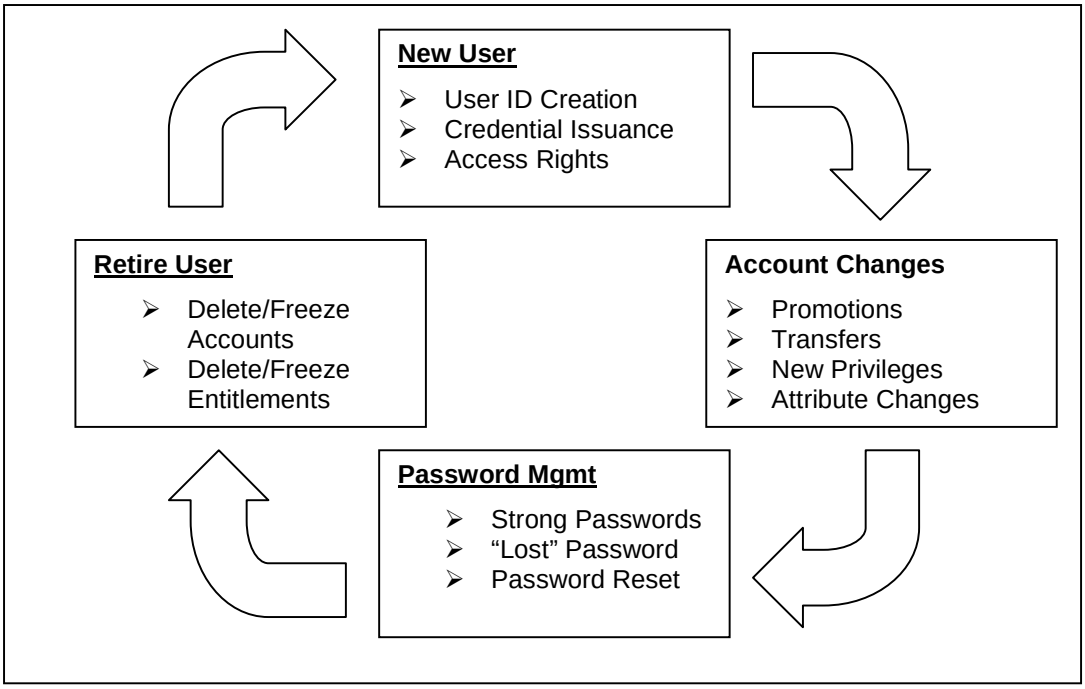

Figure 2.1 – Identity Management Process (Lukawiecki, 2006).

The process is summarised as follows:

- A **new user** is required to have access to the system
  - A user identity is created
  - Specific credentials are assigned to the user account
  - Access rights as specified are assigned to the account
- **Changes** required to account are made
  - User is promoted and requires new access rights
  - User is transferred and requires new access rights
  - User is in need of different account privileges to perform their tasks
- System **Password Management**
  - Management processes to ensure secure strong passwords
  - Reset of passwords by system manager
- **User Retirement** and removal of privileges
  - Accounts are either frozen or deleted based on requirements
  - Account entitlements are removed

This diagram provides an overview of the basic concepts of identity management and the steps that are required to successfully manage the identity of users of systems. This overall life cycle can be applied to most situations for sign-on.

A number of products have been created in order to deal with the problems involved in successfully managing the life cycle of identities within an organisation. According to Microsoft, identity life-cycle management includes the use of processes and technologies for the provisioning, de-provisioning, management and synchronisation of digital identities while remaining compliant with governance policies. The success of an implementation of identity and access management relies mostly on the efficiency with which the digital identity life cycle can be managed (Microsoft, 2004a).

Microsoft (2004a) makes mention of 5 management services which control the identity life-cycle, which must be implemented within a secure environment and have provision made for a thorough audit trail.

- Identity Integration – Links identity information within the multiple directories, databases and other identity stores. It provides a unified view of users, and can implement identity provisioning and deprovisioning across the multiple stores of information.
- Provisioning – Addition and removal of security principals in the centralised identity stores.
- Delegated Administration – Delegation of the ability to manage specific aspects of digital identity to different users.
- Self-Service – Ability for normal users to manage a section of their own identity in order to reduce the costs of management.
- Credential Management – Different authentication mechanisms have different credentials, so any platform that supports multiple authentication mechanisms should have the capability for users to manage their own multiple credentials.

In order for a business to effectively manage their user base, there is a need to put processes into place that adequately control the life cycle of the users. Should a user choose to deregister from the online service, their identity should be removed from that website as soon as possible in order to protect against any possible access violations and identity theft. The fewer identities to manage on a system and the likelihood of infiltration diminish. With the concept of how the digital "life" of an identity should be managed, the focus now shifts to the expectations of governments and businesses investing in identity management systems.

2.4 Identity Management in Public and Private Domain

Identities may be managed by either the entities themselves, in the case of the online environment, or by other parties. These parties can either be public, such as personal records offices or immigration services, or private, like employers or shops.

2.4.1 Private Sector Organisation Aims for Identity Management

The key objectives of the private sector in the creation and use of identity management systems have distinct similarities and differences to those of the public sector. A key similarity is that both public and private sectors require a system that has the ability to allow an end user to be able to perform a single sign-on. There is also a desire in both sectors to enhance Customer Relationship Management (CRM) methods and increase opportunities to uncover fraud in their systems. The private sector has additional requirements in order to remain competitive in a changing business environment. In the private sector identity management can also be required in the formulation of a basic business strategy. For example, an organisation may promote them by providing a proprietary single sign-on system to intermediate business relationships between their existing customers and other private companies. The private sector looks at the following drivers in identity management solutions:

- Organizational Efficiency – Enabling of transactions and interpersonal communication.
- Competitive Advantage – Capturing of larger market share over competitors.

- Security – Allow authorised access and prevent unauthorised access to information and services.
- Speed of Reaction to Change – Mergers, reorganisations and departmental moves.
- Fraud Prevention – Difficult to calculate but prevention will provide savings in the future.
- Consistent Treatment of the Individual – Complete management of users and customers within the identity life cycle.
- Integrated Information Infrastructure – Enable a move away from single information storage techniques (National Electronic Commerce Coordinating Council, 2002)

With the private sector looking at new business opportunities available to the online environment, it is important that they focus on the needs of the customer. The ability to provide for a seamless sign-on to a multitude of services, customization of the user's experience and consistency of the business process, and closer relationships between the business and the customer through CRM technologies, provide a strong competitive advantage. This process also makes a more comfortable, informal relationship with the customer, increasing the levels of trust through the steps taken by the online service in fraud prevention and the security of their personal information. Governments are also making use of Internet technologies in order to handle interactions with citizens easily and in a more automated fashion than the traditional paper based methods. The South African Revenue Service launched an online facility in 2006 for the submission of income tax returns via the Internet (South African Revenue Services, 2006). Similar protections to citizen information are expected by citizens when making use of a government system for submission of sensitive information.

2.4.2 Public Sector Aims for Identity Management

Within the public sector, there are however a number of similarities with the private sector. The difference is that the public/government environment is normally a follower of the implementation of the private sector, and in many cases some previous steps for the private

sector must be implemented in order to meet the goals. The goals of identity management for the public sector can be summarised as follows:

- Interactions – Allowing of filling in of government forms via online methods, for example, tax filings, license renewals and grant applications.
- Protection – Detection, tracking and apprehension of terrorists. Federal legislation has been put in place to tighten identity authentication requirements for the transportation industry, specifically civilian air travel.
- Availability – Availability of identity information when needed in authentication processes for individuals (NECCC, 2002).

Identity management within the public sector is known as National Identity Management. Following the September 11th, 2001 attacks in the USA, attempts are being made worldwide to improve the quality of National Identity Management, with specific emphasis being placed on the use of biometrics to identify individuals (De Leeuw, 2004). It can be seen as imperative that identity management fulfils the roles set out for it, in order to improve the level of trust within both the public and private sector.

Now that the aims for public and private sector identity management have been defined, the role of identity management in the online environment must be defined.

2.5 Digital Identity Management

A digital identity is the representation of a human identity used within a network interaction with other machines or individuals. The main objective of a digital identity is to reinstate the trust and ease that secure human transactions used to have, over an environment where face-to-face meetings are impractical. The attributes of a digital identity are:

1. Who one is (identity)
2. The credentials that one holds (attributes)

The credentials are the defining factor for a digital identity. A full digital identity is very intricate and possesses both legal and technical implications. The simplest form of digital identity consists of a user name and password. As systems have become more networked

and distributed, Digital Identity processes must be robust enough to build complex distributed user interactions, whilst making these interactions more user-friendly. This must occur while maintaining the required controls and security demanded by both the public and government bodies. Digital Identity can be used to facilitate the following operations:

- Authentication – Proving the identity is what it claims to be in the transaction
- Authorisation – Granting of permissions to access data or applications
- Confidentiality – Ensuring no unauthorised party can intercept the data transmitted
- Data Integrity – Ensuring that data has not been changed in transmission
- Proof of Source – Use of public and private key encryption to ensure the document originated from the source it believes it should have
- Non-Repudiation – Use of public and private key encryption to ensure the source and destination of a transaction
- Reputation – Aggregation of signed information from various sources as proven credentials based on the past transactions history (DigitalIDWorld, n.d.)

Digital Identities can therefore be seen to promote the ability of creating transactions across an environment in which people will normally never meet, while maintaining the existing identity based attributes that transactions have always had between individuals. Often in these times the transactions seldom occur between two physical individuals. With the advent of modern technology such as the web spider, making purchases on behalf of an individual, it is not even necessary for one individual to be involved in the transaction. The overriding goal of the digital identity is to release certain required identity information when required, with the permission of its owner, in order to complete a transaction.

Now that the attributes of an online identity have been defined, the solutions of how to effectively manage these entities need to be defined.

2.6 Identity Management Solutions

With digital identities identified as a facilitator for the requirements specified by government and business management, it is important to understand how the attributes of a digital identity are implemented into a viable business solution. With the existing nature of current business trends, in which budgets are being scaled back, companies are incredibly cautious when needing to invest large sums of capital into initiatives that will only provide a solution to a technical problem. The modern era demands business solutions that provide more than a technical solution, but rather enable the business to meet its objectives set out in its vision and mission. This process takes place through the use of Business Process Re-engineering (BPR) techniques to make improvements to the responsiveness to the business processes, with automated systems that promote self-service administration. Through the use of such tools, the need for support staff that would have fulfilled that business role has been reduced. Identity management delivers measurable goals for return on investment by way of reduction in costs and an increase in productivity. In order to make a successful implementation of an identity management solution, and thereby to realise the benefits of such a system, the implementation should be approached from a strategic vantage point.

2.6.1 The need for a framework

Identity management has a very wide scope, and has a role to play in a multitude of facets of the business. It needs to be emphasised that identity management has to be implemented at a corporate-wide level in order to be effective in the business. Lewis (2003) comments that most implementations of identity management infrastructures are built one application at a time, rather than designed to be implemented on an enterprise scaled framework. The result of this form of implementation is a spider-web of overlapping systems some of which perform the same functions as others with inconsistent policy frameworks. These systems tend to be error-prone, expensive to manage and due to the inconsistencies of framework implementation, tend to be prone to security attacks (Vanamali, 2004). A framework can be implemented to enforce some form of control over this situation. This framework will then become the baseline for all future identity management projects to be implemented.

2.6.2 Identity Management Framework

Identity management frameworks can help align the chosen identity management initiatives with an organisation's business objectives and security initiatives. It focuses on issues relating to:

- Business value delivery
- Confidentiality and integrity of business data
- Non-repudiation of services
- Authentication and authorisation
- Provisioning and deprovisioning of user privileges
- Auditing
- Compliance levels and monitoring (Vanamali, 2004)

The key components of a framework for identity management based on a top-down approach are shown in Figure 2.2. This approach shows each layer of the pyramid relying on the layer above it.

Figure 2.2 – Key Components of the Identity Management Framework (Vanamali, 2004)

The key points of the framework are a security vision, identity management strategy, Policies and standards, identity management architecture, identity management specifications and identity management road maps. Vanamali (2004) provides an overview of each of these levels.

2.6.3 Security Vision

Organisations must create a security strategy based on the current business and IT strategy, which must have executive support in order to be effective. Identity management initiatives need to be closely aligned with an organisation's security initiatives and should implement similar principles as the companies' information security management systems scope, security principles and values. The companies' security visions should include:

- Importance of information security within the organisation

- Need for securing of information assets
- A plan for management of information assets
- Risk management approach to control possible risks to data

2.6.4 Identity Management Strategy

An identity management strategy should align with an organisation's business and IT strategy. The strategy should be built on both the internal and external key business drivers of the organisation. The strategy identifies:

- Objectives for identity management.
- Success criteria against all initiatives will be measured. These include success factors to measure the effectiveness of objectives.
- Anticipated business benefits, like improved business processes, cost reductions, improvement in service delivery.
- Risks of the strategy, which require organisational change from the political and cultural perspective. Initiatives that require cooperation from other sources need to be evaluated. The strategy can be used to redesign business processes, workflows, show areas that could be improved through automation, correct control weaknesses and provide possible alternative solutions.

2.6.5 Policies and Standards

An identity management Framework needs to define a group of policies to be used for identity management. These policies need to be able to cover generic and specific issues. A framework defines the standards that all identity management initiatives pursued by a company must comply with, for example encryption levels, directory standards, etc. It is also essential that the framework must define set information management guidelines laying down requirement for audits and compliancy checks. This makes for a consistent process for measurement of all identity management initiatives.

2.6.6 Identity Management Architecture

Companies need to have an enterprise architecture which encompasses the security architecture. The architecture of an identity management system needs to conform to the guidelines imposed by the security architecture. With this conformity the architecture must identify the key components of identity management in order to provide effective measurements for managing security across the organisation. The main objectives of identity management architecture are:

- To act as a blueprint for current and future identity management initiatives
- To be effective, consistently applied, manageable and allow for practical implementation.

Figure 2.3 shows the key components of an identity management solution.

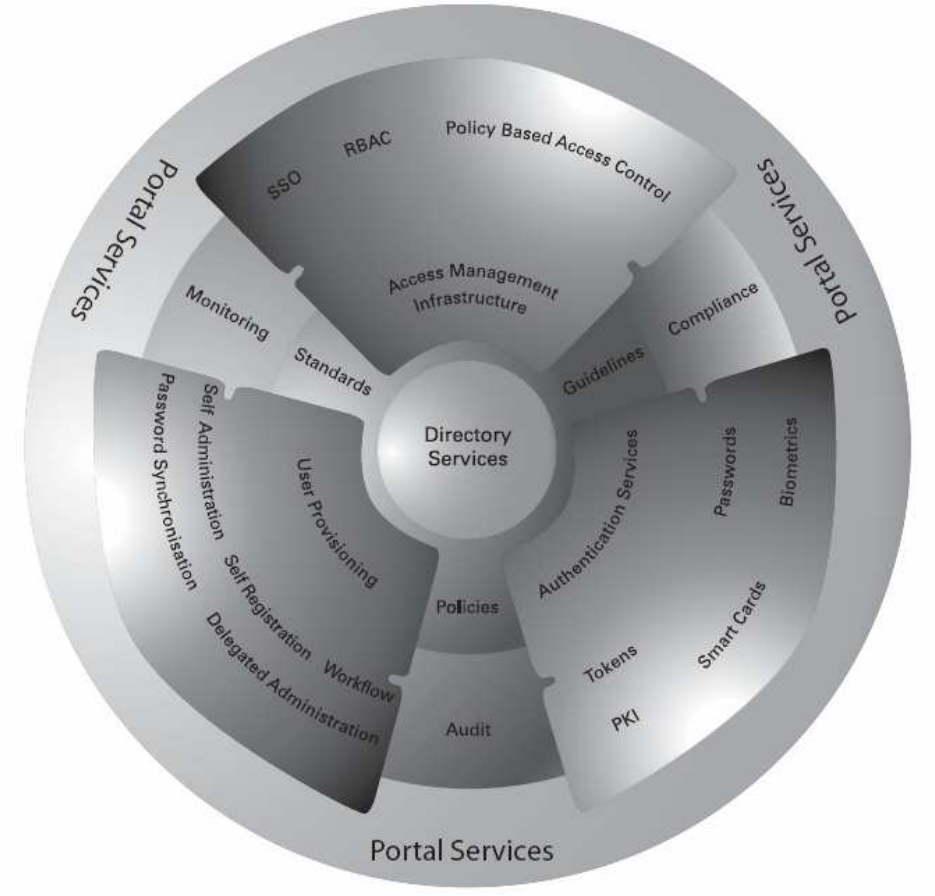

Figure 2.3 – Key Identity Management Components (Vanamali, 2004)

The control functions that are specified in the architecture need to support the design, implementation, maintenance and management of the identity management infrastructure. The core management components specified in Figure 2.3 are:

- Directory services – The most critical component of identity management. It is a repository for user ID and profile information, playing a key role in the authentication of users, and also enables on-demand service delivery.
- User provisioning – Role-based approach driven by a directory, user provisioning oversees the complete life cycle of an identity across different systems.
- Authentication services – This identifies the user through authentication methods, including digital certificates.
- Access management infrastructure – Based on a set policy, an access management infrastructure controls access to information systems and applications.
- Portal Services – Act as a presentation layer, providing a single interface for all web-enabled systems and applications personalised to the users' profile.

2.6.7 Identity Management Specifications

The detailed specifications are used to guide technology choices based on the business' required functionality. A key constraint is the understanding of how the components of the identity management architecture interact to meet the overall goals. These specifications include the evaluation criteria for the integration and implementation of identity management solutions.

2.6.8 Identity Management Road Map

The definition of a road map is a critical step in the setting up of a framework. The purpose of the road map is to identify the steps that need to be taken to deploy and integrate identity management components so that they are in line with the organisations overall identity management specifications, architecture, policies and standards, and identity management strategy. It must also specify the priorities for the short to long term strategies, based on the potential business impact and value proposition.

2.7 Benefits of Identity Management

The impact of a successfully implemented identity management system can be shown by assessing the outputs of such processes in well established companies. Sun Microsystems (n.d.) lists overall key benefits of identity management as the following:

1. Assists in planning, implementation and management of solutions through a complete lifecycle of services portfolio.
2. Reduces costs and complexity, while increasing the rate of Return-On-Investment made in identity management.
3. Ensures predictable implementation procedures and efficient business operations, thereby ensuring greater system satisfaction from both users and customers.
4. Manages all four main areas of concern for the business (people, process, practice and platform), when implementing identity management in the organisation.

These can be seen as overall key benefits of identity management implementation. Further implementations in other well known companies have produced similar results when implementing an identity management solution.

2.7.1 Fujitsu

Fujitsu has measured the benefits based on their use of their own People Data Management products:

- Improved processes for employees joining and leaving the company allowed for large numbers (roughly 15% of total corporate email and NT accounts) to be removed as the users had left the company.
- Improved security and decreased managerial overheads on mail and NT systems.
- In the implementation of a new financial system, data relating to approximately 3,000 employees was maintained manually. This task required four full-time staff members and the data input was frequently error-filled.
- A link from the People ERS was implemented in order for the finance system to have a regular and automated people data feed, which provides accurate data at less than 25% of the previous manual cost.

- Minimal cost for the addition of more people to the financial system.
- Easy access to the viewing of people data for the required manual processes such as staff management within departments and personal detail verification.
- Ten to fifteen corporate systems that were previously operating independently, are now working from the same data (Locke & McCarthy, 2002).

2.7.2 PriceWaterhouseCoopers Customer

- Deployed an Oblix NetPoint 5.1/LDAP infrastructure as an enabler for identity management. Functionality now exists for Web access security and scalable identity management infrastructure for offering a number of web based services.
- Application integration standardisation – New applications now go through application integration processes such as web single sign on, access management and identity management.
- Reduction in security development costs and lowering of costs for ongoing maintenance and help desk operations (Gordon, 2004).

2.7.3 Onyx – Microsoft Onyx Case Study

Onyx, a leader in the waste management industry in Europe, wished to synchronise the e-mail and intranet directories to build an enterprise directory for employees. In two months, Onyx improved their identity management processes in order to create a dependable identity infrastructure for all of the businesses collaborators. The company now manages the profiles of their 5,000 French employees with a greater level of precision. The benefits of the implemented system included:

- Optimisations of identity management – Directories previously separate are now integrated and accounts of former employees are now easily located and removed.
- Reliable Reference System for Employees – All identity information was moved into a consolidated directory for use by staff, which was always current and will be depended upon for the company's applications.

- Future Development Base – Through the use of the new infrastructure multiple beneficial projects were planned, including the connection of the new infrastructure to Onyx sites outside of France. (Microsoft, 2004b)

2.8 Standards Initiatives

When setting up an identity management system for use within an organisation, the task can be seen as monumental. Where does an organisation begin in setting up such a system that will meet its goals, and meet them while keeping the company secure? Because of this uncertainty with regards to what should and should not be set up for an identity management system, the Liberty Alliance was set up in order to provide a baseline for best practices.

2.8.1 History of Liberty Alliance

The Liberty Alliance was initially formed in 2001 by organisations in order to establish a set of open standards, best practices and guidelines for the usage of federated identity management. In 2002 they released Liberty Federation which became the industry standard used to address the authentication privacy and security issues inherent in online identity management. Liberty Federation allows online users to authenticate and sign on to a network or domain only a single time from any device and make use of multiple websites. The use of a federated approach usurps the problems of multiple authentications and supports privacy controls established by the user. They then further contributed their federation specification, ID-FF, to OASIS which formed the foundation for Security Assertion Mark-up Language (SAML) version 2.0, the converged federation specification that Liberty now recognises. The Liberty Alliance has directly focused on business and policy making aspects of identity management, having published business and policy guidelines in a number of forms for different market segments (Liberty Alliance, n.d.).

The overriding vision of the Liberty Alliance is the creation of a networked world based on a set of open standards, in which businesses can conduct online transactions seamlessly while

ensuring the protection of the privacy and security of an individual's identity information. The members of the Liberty Alliance are working in order to meet the following objectives:

- Build a set of open standard-based specifications for federated identity and identity-based web services.
- Drive global identity theft solutions.
- Provide interoperability testing
- Provide a certification programme for products that make use of the Liberty specifications.
- Establish best practices, rules, liabilities and business guidelines.
- Work in partnership with standards bodies.
- Address end user privacy and confidentiality issues (Liberty Alliance, n.d.)

2.9 Conclusion

Organisations are now viewing identity management as a solution to a multitude of security challenges. However organisations need to consider how they can ensure the benefits and value of an identity management system within their business. Due to the poor amount of documentation on new systems and the functionality that they may possess, often when a new system is designed it is built completely from the ground up. Frequently businesses are unaware that there are already built components which can be applied to their new systems in order to share common functionality and security concerns. This wastes both time and money in continuously re-inventing the wheel. When a framework for identity management is used correctly on new identity management systems, it provides clear goals, strategy, policies, identity management architecture, specifications and a road map of how to reach those goals. This provides a strong base for successful, business-driven and clearly understood identity management.

In this chapter the concepts of identity management were discussed. It was shown that the information that is stored within an identity is of great value and needs to be protected. The management of an identity is of equal importance. Companies should make use of the

identity management life cycle to ensure that identities are adequately protected while under their care and removed when they are no longer required. The aims for identity management within the public and private sector were discussed. From this analysis the need for fraud prevention and the integrity, confidentiality and accessibility of this information was found to be a requirement in both systems. The benefits of making use of an identity management solution were found to be vast, depending on the nature of the system and the expected outcomes.

In essence identity management should be viewed as a modern day tool for the management of customer and user transactions in the online environment. The use of identity management is stipulated as a need for compliance with government laws and best practices of the industry. Identity management can be used as a tool to manage the business and protect it from risk. Now that the elements of an identity and the importance of the management of that identity have been discussed, Chapter 3 will focus on the management of the authentication and access of users.

Chapter 3 builds on the concepts outlined in this chapter, by looking at the role of access and authentication management of identities, and how the levels of trust of customers and website vendors can be increased through adherence to compliancy standards and proper access management processes.

Chapter 3

ACCESS & AUTHENTICATION MANAGEMENT

In order to effectively manage a business environment in which multiple users are in need of accessing systems over large distributed networks, it is imperative for the security of the business to ensure that the users who connect to this environment are whom they claim to be. A 1993 edition of The New Yorker contained a cartoon by Peter Steiner in which a dog explains to another dog the advantages of the Internet. The dog specifies plainly that, "on the Internet, nobody knows you're a dog." This cartoon asks the question of how important is the knowledge of an identity to a vendor/system administrator. Would the vendor still sell a product to an entity if they were aware that the customer was a dog, lacking the ability to pay for the items or services? Due to the risks involved a vendor would not enter into an agreement if they knew the customer was an animal. The Internet has the ability to mask an identity and in doing this opens up all forms of possibilities. It can then be concluded that due to the lack of definitive online identity, every action that is performed online is subject to a certain amount of risk. A merchant may not be overly concerned about the identity of their customers if the possibility of failure of payment is small however in order to reduce the possibility of failure for payment a higher level of trust between the merchant and the user needs to be insured. A business may be more concerned with the authorisation of their customers than their authenticity. The role of trust plays a great role in the relationship between the buyer and the seller and it is important to understand the role of trust in an online environment.

This chapter will look into the concepts of managing the trust of users and website owners in the building of a strong relationship of trust between the two parties. The roles of access control and the benefits for better protecting client information are presented. Along with access control the issues of accountability and access control techniques are presented to

provide an insight into the need for compliance within access control and the benefits through this process. The chapter begins with a look into the role of trust management and the importance of ensuring high levels of trust between user and business owner.

3.1 Trust Management

The concept of trust is invaluable to both merchants and consumers. The definition of trust from the Oxford English Dictionary (1989) is "Confidence in or reliance on some quality or attribute of a person or thing". In the online environment there is a large amount of doubt from both the merchant and the customer as to the validity of both individuals. In real life business deals are negotiated via means of paper-based contracts or face to face verbal agreements. All of these means are valid as there is a means of legal recourse should the business deal go sour. On the Internet, as mentioned previously, there is no proof that an entity is who they claim to be. This lack of fundamental trust has spread into the traditionally most secure of environments, the banking sector. In a recent report by Computer Fraud and Security it was stated that 52% of respondents were unlikely to sign up to use online banking, as well as reports that 82% of respondents would not respond to any mail from financial firms (Consumers losing trust in online banking: survey, 2007).

The Internet's e-commerce is based on a virtual environment in the way in which it has very few physical attributes and offers limited social markers, which makes the customers' assessment of the trustworthiness of a vendor rather difficult. In online commerce, customers take on substantial amounts of risk when making purchases from an online vendor. This is due to all encounters taking place through the vendor's website. It is important for customers to assess the risks that can occur when purchasing online. Through previous studies it has been shown that the level of trust affects the customer's intention to purchase online. Customers on a vendor's website often leave the website when they believe they do not have sufficient trust (Chau, Hu, Lee & Au, 2006).

It is important for online vendors to build strong relationships with their customers to ensure that customers continue to return and make use of their services. In order to secure this trust, it is imperative that vendors make use of proper access control procedures to provide the minimal risk to their customers.

3.2 Access Control

Access control is defined by Lopez, Oppliger and Pernul as the, "prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner" (2004). Within the realm of computer security, based upon this definition, access control includes the authentication and authorisation processes involved in a sign-in event. Within the online environment access control makes use of biometric scans and digital signatures and certificates.

The control of access to resources and restricted functions within systems is a major component in system security. The requirements for an access control model are summarised as follows:

- Access control models must be easy to use and transparent to end users.
- The effects of access control procedures on the rest of the system need to be clearly understood.
- Access control models have to allow for complex access policies at different levels of implementation.
- Models need to be sufficiently flexible to allow for specification, delegation, revocation and overall management of access policies at runtime.
- Models need to provide strong protection in shared user environments.
- Models may grant access by considering the current context of the user (Lopez, Oppliger & Pernul, 2004).

These requirements can also be interpreted as best practices for the setup of any access control process. The implementation of an access control system is based on the policy implementation of the business. Like company policies, the reasons for implementation of access control procedures need to be fully understood by staff and users in order attain the desired level of benefit by management.

Access control is built on a set of authorisations which are given as directives through the security policy. These authorisations state that specific subjects (defined as a user or process) are allowed to perform specific functions or actions (defined as an access mode) to a specified object (defined as a resource of the system). The traditional approach of static authorisation through which a subject takes an action on an object, is best suited for basic traditional systems, but fails during implementation on more complex systems. More forms of authorisations need to be made available such as content-based authorisation, constraint based authorisation and negative authorisation (Cuppens, Cuppens-Boulahia & Ghorbel, 2007).

Access control models used in modern systems fall into one of two categories, those based on capabilities and those based on access control lists. In a capability-based model, the possession of a capability to an object provides access to the object via a secure channel. In an access control list model, the subject's access to an object is dependant on whether the identity's access is found on an approved list. These lists can be edited to provide user access to required resources.

Access control systems provide the essential services of:

- Identification and authentication – Unique identification of the user via use of a username or some other distinct identification, and authentication via verifying the claimed identity by use of a password or other forms of authentication

- Authorisation to determine what a user or subject can do on the system, such as read and write access and ability to execute applications within the context of the security policy and system rules
- Accountability to keep track of what actions a subject performed

3.2.1 Accountability

For all uses of an access control mechanism or procedure the keeping of a history of the access controls and audit logs of actions performed by users is of high importance. This information is vital for use in potential legal proceedings and in the tracking down of problems within systems determining who performed what action. A large portion of the accountability and audit trails are implemented due to legal requirements within compliancy issues.

A regulative system requires the entities that make use of it, to be able to be uniquely identified so they can be held accountable for their actions. It is not possible to ensure accountability in applications where there is no implementation of identity controls. Applications that only make use of a username for user authentication only provide a weak measure for accountability insurance. In such applications users can have multiple identities in the system at the same point in time. The user is then also able to disappear and reappear in the system with another identity without being properly restricted. Introduction of mechanisms which measure accountability are based on a scoring model. These mechanisms may provide the users with economic incentives to retain the same identity for a prolonged period of time. Implementations of enterprise applications normally require users to make use of the system under their real identities. In these cases users are requested to identify themselves by making use of public key certificates which are then matched against their legal identities (Firozabadi & Sergot, 2002).

Continuous review of access logs and storage of the access logs in a secure and consistent manner is required should any of that information be required as evidence in a legal suit. Automated alerts should be sent to system administrators in order to ensure that unauthorised user actions are logged. Examples of this would be more than three failed log in attempts in a specified period or use of a disabled user account. Alerts on these forms of unauthorised or suspect actions can allow security administrators to identify what went wrong and how best to combat it in the future, as well as watch for illegal attacks.

3.2.2 Access Control Techniques

There are a number of access control models and approaches to handling the problem. Access controls are described as either discretionary or mandatory.

3.2.2.1 Discretionary Access Control

Discretionary access control (DAC) means that each object within the system has an owner, and that owner chooses the access control policy assigned to it. A number of objects in Windows make use of this security model (Tavares, 2004).

Access controls can be discretionary within Access Control Lists, capability-based or role based access control systems.

3.2.2.2 Mandatory Access Control

Mandatory Access Control (MAC) ensures that an organisation's security policy is enforced without user compliance from an application. The assigning of security labels to information is correlated against the level of security a user has access to. Overall MAC mechanisms are more secure than DAC but contain trade-offs in performance and user convenience. A MAC model contains one or more of the attributes:

- Only administrators make changes to security labels
- All data is assigned a security level reflecting its value for protection
- Users read from a lower classification than their security level and up to their security level

- All users can write to higher classifications
- Users are given access to objects only of the same classification that they are authorised to view
- Access is based on labelling of the resource and user's credentials
- Access is based on the security of the client (Open Web Application Security Project, 2002)

Ultimately the process of access control is as strong as its weakest link. A system implemented with the strongest of authentication and access control mechanisms fails completely if the groundwork is not controlled by system administrators and support staff such as human resources.

3.2.3 Life Cycle Management and Human Resources

An alarming trend when viewing access rights that users possess is the way in which they are managed. Human Resources departments need to take a deeper look into how they control employee's roles in their course of working for a company. Currently when looking at the management of user identity, many companies are not efficient in the way in which they handle user roles.

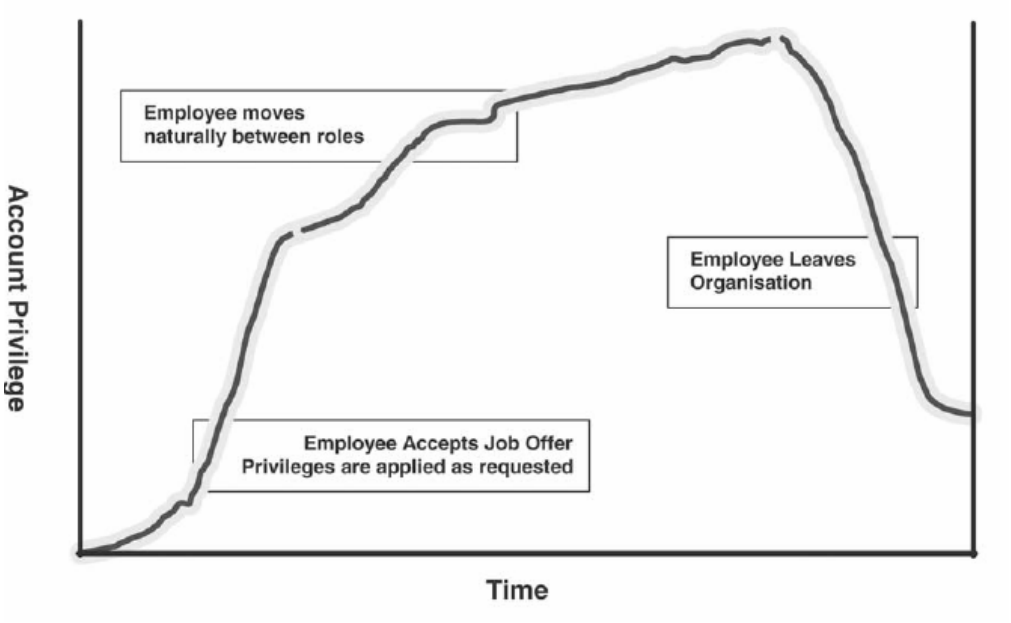

Figure 3.1 – Current Employee Life Cycle – Access to accounts (Young, 2004)

Figure 3.1 shows how when an employee is selected for a role, general access requests are granted, an example is accessing the main system's network. In some instances certain requests are granted before the user is even at the company, in order for them to be productive from their first day. Over the course of the employee's employment, certain access rights are increased in order for the employee to fulfil his/her work functions. However the graph shows that as the employee's work responsibilities increase, there are very few privileges being removed. This process ends when the employee leaves the organisation, but even after the employee leaves the organisation there are, on a number of occasions, privileges that still remain. This results in a number of potential issues, including:

- Open access to privileges that the user may no longer need to perform their job function.
- Orphaned accounts in target systems.
- Administrative overhead in system clean-ups.
- Assets not returned when user no longer needs them.
- IT roles and permissions have no relation to HR roles.

- Difficulty in determining a common provisioning policy for employees and contractors (Young, 2004).

It is clear that in order to clean up this inefficiency, account privileges that are based on user's roles are implemented. Should such an implementation take place, the graph would look as shown in Figure 3.2.

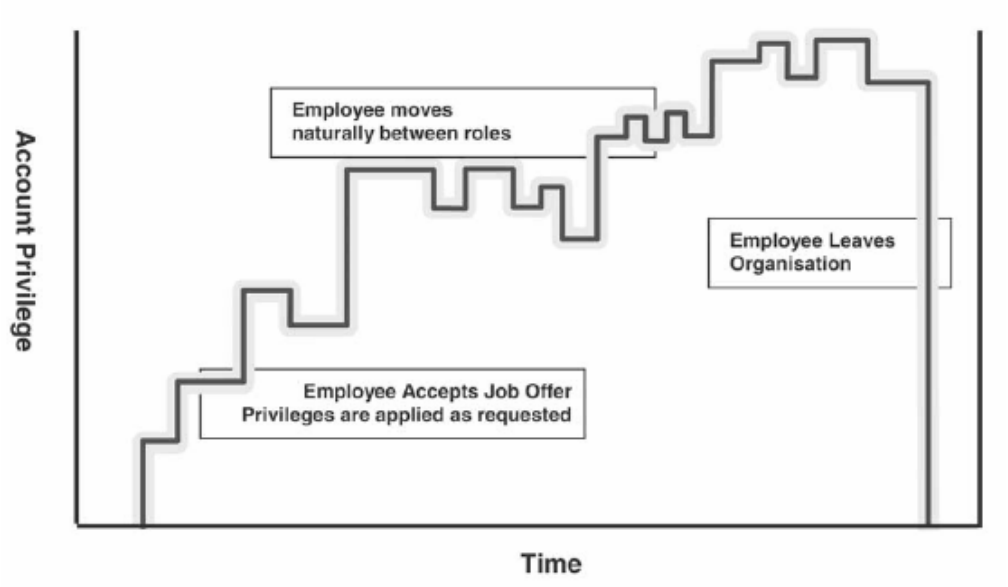

Figure 3.2 – Role Based Access Management (Young, 2004)

As users change their job roles within the organisation, their account privileges will then either be cut or expanded, but upon leaving the company all, account privileges are then completely removed. It is imperative for successful identity management on the environment for HR to comply with the process, which can significantly reduce administration overhead, streamline business process and help enforce security policy for IT systems within identity management (Young, 2004).

3.3 Compliance

With the huge boom to the world of marketing and advertising that the Internet has provided, with it has come a large number of legal issues needing to be addressed. Rights to an individual's privacy and personal information need to be protected. These areas are closely

looked at in the way companies protect their information through the use of COBIT and ITIL. The process of authentication is the point at which the identity meets the world. The challenge for identity and access management solutions is to provide authentication methods whose strength is appropriate to the inherent threats that they face.

Two core themes of compliance have however been set out in the focus areas that are addressed by identity and access management solutions. These are the need for organisations to protect the data of the individual stored on their systems, and secondly the mitigation of risk arising from unauthorised access to organisational processes and information.

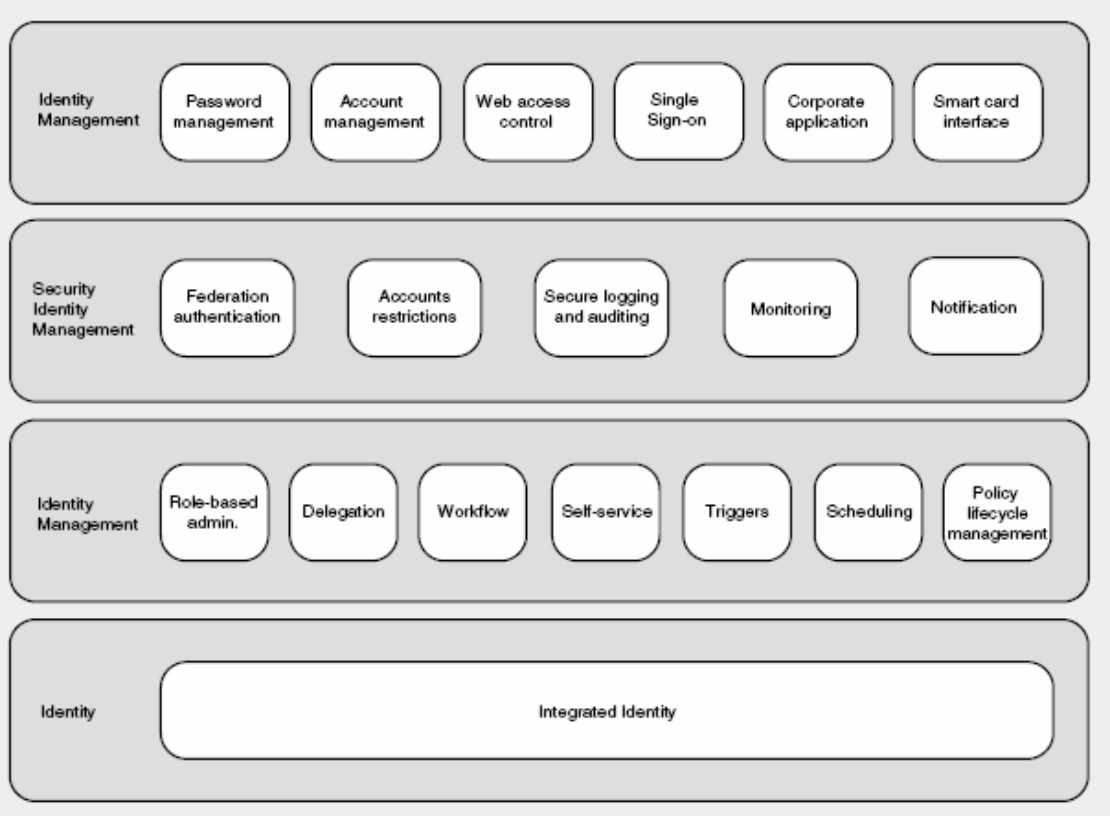

Figure 3.3 - Elements Comprising an Access Management Solution (Rodger, 2004)

Figure 3.3 shows examples of the elements that make up an identification & access management solution. The foundation of all the elements is a secure repository for the

identity information. This element is the most important as the use of identity is the basis for the protection of other resources and thereby requires that the information must be guarded safely. A common approach within a number of I&AM solutions is to allow organisations directory resources to be leveraged, as these are well protected from malicious access and provide the backbone of existing identity activities. Directories can be used as large identity repositories, whilst being suitable for compliance because of their high levels of security (Rodger, 2004).

It is now accepted that the username and password mechanism is no longer a secure authentication option. It is important for organisations to look ahead for a multi-tiered authentication strategy to protect information assets. In this approach other forms of authentication can be used as enhancements to the username and password approach, each providing a factor of the overall authentication. The adoption of a multiple factor authentication enhances the security of the assets that need to be protected, and by reducing the risk that arises from these threats a number of compliancy issues are resolved. Compliance requirements dictate that only authorised people should be able to access information (Rodger, 2004).

3.4 Conclusion

Merchants store a particularly large amount of information online. This information is used for user preferences on purchasing as well as delivery information and contact details of customers. From the merchant's perspective there is not much concern about the overall identity of the individual but more so their ability to pay for the service. However regulatory bodies have put large amounts of effort into ensuring that a user's information is kept secure and is used in the correct way. Should the security be breached it is then imperative that accurate logs exist in order to identify what actions took place under that user's identity. This would be useful in cases where prosecution is required.

Having looked into access control and authentication management and how they should be applied, the next chapter will begin to look at the overall design and implementation of three industry models for implementation of an identity management solution to the single sign on problem. These three models are the Mozilla TrustBar, the Liberty Alliances Federated Identity model and the use of Microsoft Passport .NET as solutions.

Chapter 4

COMPARISON OF IDENTITY MANAGEMENT SOLUTIONS

The ultimate dream of the computer scientist and practitioner is one in which computer systems know who their users are. This ideology is based on the concept that users should be authenticated to a computer system as simply as possible. Furthermore based on that authentication of the user, systems must authorise those users and control access to system resources accordingly. The dream is seen with many names: Single Sign-On (SSO), Single Sign-In (SSI), authentication and authorisation infrastructures (AAI), privilege management infrastructures, etc. The umbrella term that is most frequently used to cover all of these cases is identity management. This study has shown the different dangers that are inherent in the online environment. These dangers are briefly summarised as spoofing, phishing and identity theft of client details. The aim of this chapter is to look into the processes involved in the different forms of identity management solutions for the Internet. A look at Microsoft's Passport .NET is taken in order to see the approach suggested by recognised industry leaders in Microsoft. The Liberty Alliance's view is then analysed to determine best practices from the rest of the industry. Finally the chapter moves on to an investigation of identity management from the view of the user, to determine how to best protect the user from other forms of attacks in Mozilla TrustBar.

4.1 Microsoft Passport .NET

As part of Microsoft's .NET initiative, a set of Web services was introduced including a user authentication and SSI service called Microsoft .NET Passport. This service was released in 1999 and is one of the most widely used services of its kind. It is used within the Microsoft Hotmail Service, a free online email facility (Lopez, Oppliger, & Pernul, 2004).

Microsoft is well known as the market based leaders for a number of technologies. Globally they possess the possible infrastructure in order to support a large effort such as a unified single sign-on methodology.

4.1.1 Passport Model

The Passport .NET service makes use of a Single-Sign-On Identity Domain. This is an extension of the Common User Identity Model as shown in Figure 4.1. The identifier and credential indexes in the figures refer to the issuing entity. For example, an identifier and credential with an index of 1 mean that they have been issued by Service Provider (SP) 1.

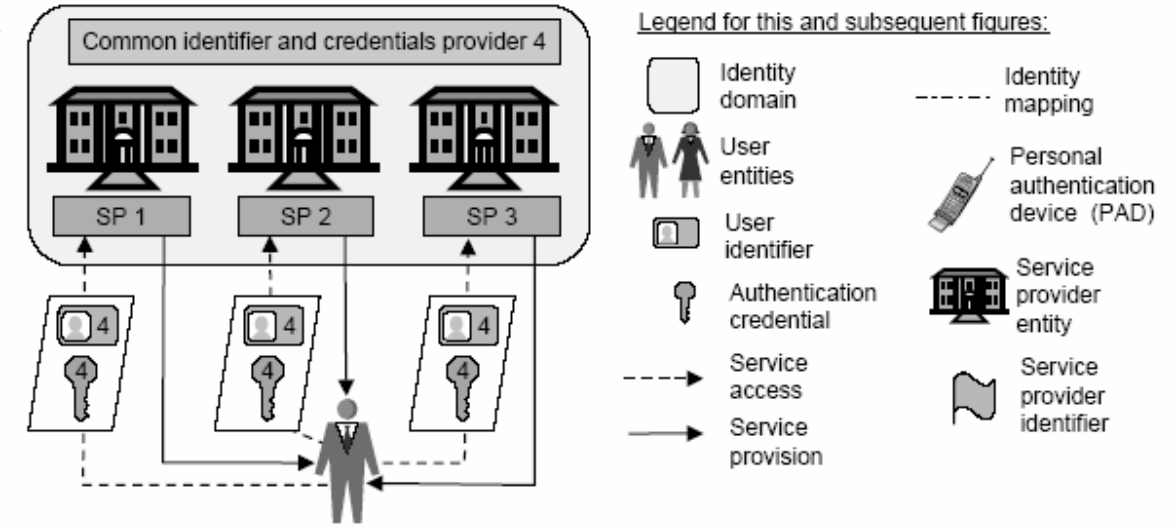

Figure 4.1 Common User Identity Model (Jøsang & Pope, 2005)

The principle of the Common User Identity Model lies in having a separate authority structure in place that acts exclusively as an identifier for users as well as providing user credentials to other service providers. Through this model a user can access all service providers by making use of just one set of user identifiers and credentials. This system may be implemented via use of a primary key identifier (PKI) in which a single Certification Authority (CA) issues certificates to all users within the domain. The identifier name can be a set of email addresses that are globally unique. Users in this case would only need a single

identifier and credential to be authenticated by all service providers within the domain of the CA. The underlying working of this model is the basis for the operation of the single sign-on Identity Domain incorporated in Microsoft Passport .NET (Jøsang & Pope, 2005).

There are inherent problems in the possible setup of such a model. The use of email addresses for the purpose of user identification is a risky proposal. Email addresses are not necessarily unique identifiers of users. Users can have multiple e-mail addresses, and the unique identifier for users can be relatively easily retrieved by potential users wishing to commit fraud. Other problems in the setup of an SSO environment is the lack of defence in the sign on procedure. With the use of multiple authentication and sign-on requirements across websites, should one set of user credentials be compromised, only that login and information contained within it can be affected. Should the user credentials of a SSO be compromised, all websites which make use of those user credentials are compromised, thereby threatening the user identity further. The .NET framework operates from the SSO identity model which allows for a user set identifier.

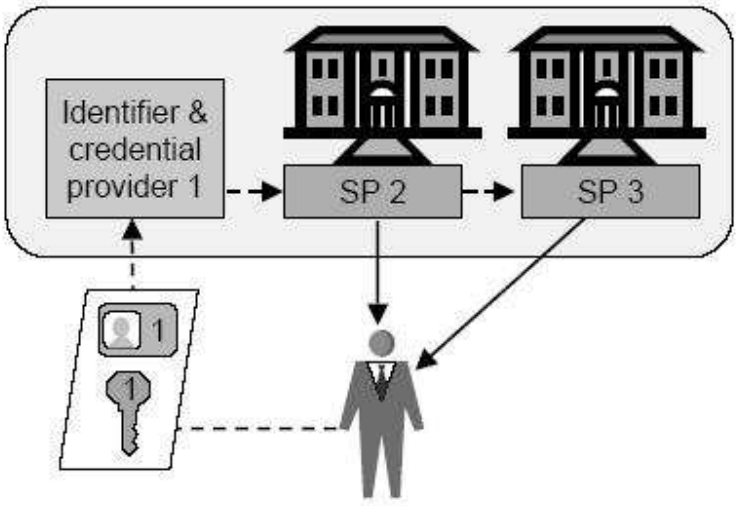

Figure 4.2 SSO Identity Domain Model (Jøsang & Pope, 2005)

The Single-Sign-On Identity Domain Model shown in Figure 4.2 shows how a user may be authenticated by making use of only one service provider. This single service provider, once

user authentication has taken place, then allows other service providers to consider that user has been authenticated. The approach to this is known as a Single Sign-On (SSO) solution as the user only needs to authenticate their identity once in order to access all services they should have authority to use. In this form of implementation, there is only one party responsible for the allocation of identifiers, issuing of user credentials and the performing of the authentication. This SSO implementation is very similar to that of the federated identifier concept used by the Liberty Alliance, however, no mapping of user identifiers is needed. This is due to the same identifier being used in every service provider. Through this process, once a user has been authenticated through the single login provider, all affiliated websites to the .NET Passport will consider the user as authenticated should they attempt to access them. This process lasts for a specified amount of time till the session times out, then a new login by the user is required (Jøsang & Pope, 2005).

Microsoft overall is ideally suited for the process of handling an SSO platform. Microsoft already provides a large number of services online for e-mail, online chatting, and searching facilities. Through the use of this already existing infrastructure Microsoft could increase their business footprint. Ultimately what would be requested from users would be a form of non-profit organisation that would be tasked with the setup and maintenance of a global SSO identity framework solution. However there would be some issues should such an implementation take place. Issues concerning user privacy and freedom of movement online could be infringed should a single entity take control of all SSO authentication and the information held therein, and be compromised either by an illegal party or from government organisations.

Now that the form of model that the .NET Passport implements has been presented, the overall implementation of the principles of this model can be better understood by looking further into how users make use of the .NET passport and the underlying methodology behind it.

4.1.2 User Registration

When a request for registration for a Passport at a specific website is made, two separate accounts are created at the same time. Through the use of a single form the user opens an account with the website owner as well as one with Passport. All information that would be recorded under the owner website is sent from the Passport service upon registration to the owner website with all the profile information normally entered at registration. An overview of the registration process is shown in figure 4.3.

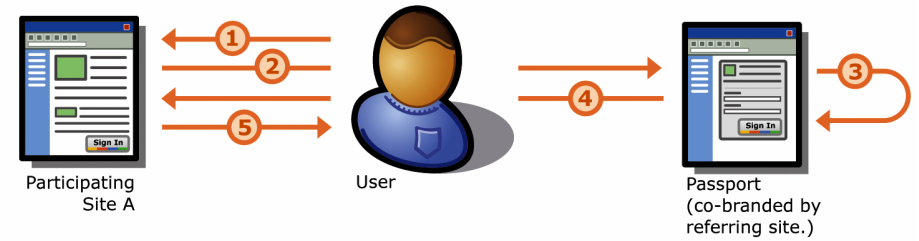

Figure 4.3 – The Registration Process (Microsoft, 2004c)

1. User browses to Site A, a participating website or service and clicks the "Sign In" button (or attempts to register).
2. The user is redirected to a registration page displaying the registration fields required by Site A. (The minimum number of fields required is two: email address and password.) The user can choose whether or not they will share their information with other Passport enabled websites that they sign into.
3. The user reads and accepts the terms of use, and submits the form.
4. The user is then redirected back to Site A with their encrypted authentication ticket and profile information attached.
5. Site A decrypts the authentication ticket and profile information and continues their registration process, or grants access to their website.

Information that is unrelated to a customer's Passport profile is only stored on Site A and is not shared with the Passport profile. Site A also does not receive any information that relates to the Passport system. Passwords, secret questions and answers, security keys and other

customer credential information are not shared in order to maintain the security of the user's authentication data. The Passport profile only makes use of information that will ease possible further registrations. Examples of this sort of information would be Country, Postal code and Time Zone (Microsoft, 2004c).

Lopez, Oppliger & Pernul (2004) further describes the information that is stored per user account, mentioning that each .NET Passport account can include the following components:

- Passport Unique Identifier (PUID) which is a 64-bit numeric value assigned by the .NET Passport Service when an account is created
- Passport user profile containing user's e-mail address or phone number, first and last names, and demographic information for the user, as well as the user password (a minimum of 6 characters)
- Optional secret questions created by the user, along with their answers, are stored to be used with a possible reset of the user password
- An additional 4 digit security key is used when users attempt to access websites that require a strong credential sign-in. This security is only created the first time a user accesses a website that requires a stronger set of user credentials

The standard listed credentials are the minimum amount of information that is required for a user to have a .NET Passport. In all cases the amount of information that is requested from the user upon registration depends on the website where they request to register, as well as any information that they would want to share with other Passport participating websites during sign in. Information that is not needed by the Passport service is only stored on the vendor's website and not by the Passport service.

4.1.3 Passport .NET Authentication

The Passport authentication messages are passed in the form of electronic "tickets" that are used to inform websites that the user has successfully signed in. A ticket which is stored in the form of a cookie contains information on the date and time of sign in, and the date and time of the last manual sign in. In order to receive this information the user has to

authenticate them through the use of the .NET Passport. The process followed is shown in Figure 4.4.

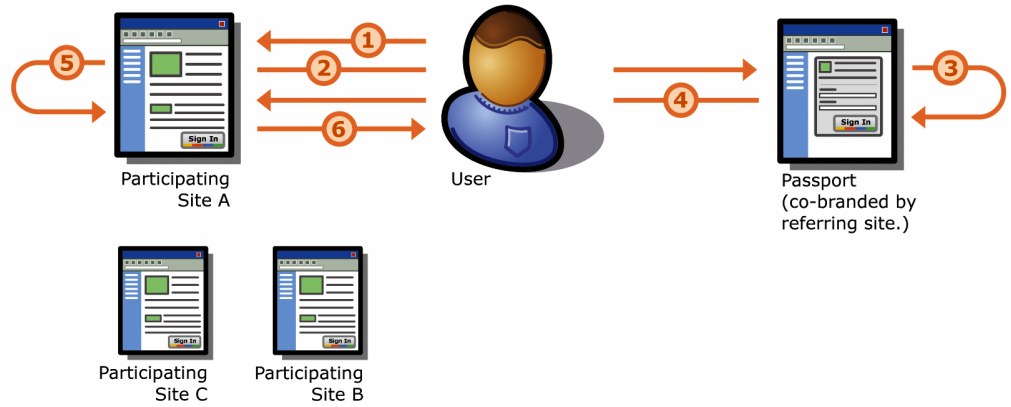

Figure 4.4 – The Passport Authentication Process (Microsoft, 2004c)

1. User browses to participating website or service (Site A in this example). User clicks "Sign In" button or link.
2. User is redirected to Passport.
3. Passport checks if the user has a "Ticket Granting Cookie" (TGC) in their browser's cookie file (one that meets the rules that Site A has set). If one is detected they skip to Step 4 and never see the Passport login UI. If the TGC does not satisfy the time since sign in rule requested by Site A, then Passport removes information that Site A passed on the query string and redirects the user to a page that asks for the currently signed in user's password. This new page has a short URL in the Passport.NET domain. If the user enters the correct information, they proceed.
4. The user is redirected back to Site A with their encrypted authentication ticket and profile information attached (if the user has chosen to share it, and if it is present).
5. Site A decrypts authentication ticket and profile information, and signs the customer into their website.
6. User accesses the page, resource or service they requested from Site A.

NOTE: Sites B and C do not receive any information in this process. No information about a user is shared with Sites B and C unless the user chooses to sign in at those websites.

In order to attain a ticket, the user clicks on the Passport sign in logo in the website. This will then redirect the user to a special page on Passport.com. This page takes information from the website that directed the user to that location, from the URL and assigns it a unique website ID. This process allows Passport to know which website referred the user, and to which website the user needs to be returned. Once the login details have been processed, Passport redirects the user to a page on Passport.net.

There are 2 reasons for this internal redirection within Passport. Firstly, through this process the URL is shortened in order for the user to verify that the page address is owned by Passport. The second reason is in order to separate the user interface from the domain in which the authentication cookies were originally written. This process helps to prevent unauthorised access to these cookies, as browsers only allow for the reading of cookies which have been written in the same website currently being accessed. The whole process of the redirection takes place in a matter of seconds, and once completed returns to the requesting website.

Upon return to the requesting website, the user has attached two encrypted packets of information within the returning query string. Website owners making use of the Passport service would need to install Passport Manager. This application reads the packets that have returned with the user and writes them as encrypted cookies in the owner's website domain. The first of these cookies contains the authentication ticket information. The second contains profile information that the user selected, as well as operational information and unique identifiers that need to be passed. These packets are encrypted with a unique secret key which is shared between Passport and the owner website. The owner website then takes the information and uses it to issue its own cookies.

When the user navigates to another Passport participating website, the new website has multiple options on how to authenticate the new user. When a user clicks the sign in button, they are once again directed to the Passport sign in page. The difference now is that there is a ticket-granting cookie saved on the web browser that Passport can read. Because the cookie ticket contains the time that it was issued, it allows the referring website to decide the timeframe that the website needs to consider the cookie as safe enough to use. If the cookie ticket is too old the user is then prompted to re-enter their credentials.

Each website may choose how old the ticket-granting cookie is before they will reject it. They also have the option of forcing users to re-enter their password. This eliminates the ability of someone who does not know the user's password to access the user's information. Through this process there is variance in the protocols for ensuring the user's ticket cookie is valid, and potential security holes are opened for user information to be compromised.

A potentially hazardous feature to the user of .NET Passport, reported by both the Microsoft (2004c) and discussed by Kormann & Rubin (2000) is that of the automatic sign in of Passport. If this option is selected the username and password of the individual user are stored locally on the individual's client machine. With an automatic sign in selected the user will be signed on to the .NET Passport service without their intervention whenever they make use of the machine. Even disconnecting from the Internet or turning the machine off has no effect to the user remaining connected to the service.

Although a user may use their .NET Passport account at multiple websites, the password is only stored in the .NET Passport database, and is only shared with the .NET Passport servers that need to make use of it for authentication. The .NET Passport service possesses a facility which, should a user make an error in attempting to sign in, .NET Passport then automatically blocks access to the user account for a few minutes in order to stop attempts for password cracking software being used to gain unlawful access to the account.

When the user wishes to sign out, the .NET Passport server checks the websites that the user has visited through the visited websites cookie. .NET Passport then redirects the client's browser to each visited website and requests each website to execute a script deleting the cookies that those websites created at sign-in. Unless a user makes use of the option for automatically connecting to the Passport service, all .NET Passport cookies are session based and are deleted when that session is closed. If a user makes use of the automatic sign in option, the cookies are persistent and are not deleted if the browser is closed. Through the user of the expiration of user authentication related cookies, Passport ensures that user information is not stored indefinitely on the client machine.

Overall the .NET Passport solution provides a relatively simple solution to the problems experienced by users within SSO. Websites affiliated with the .NET Passport program can opt to have the service manage their user base, shifting responsibility for this process from the individual website to Microsoft. The major disadvantage of the .NET Passport solution is the problem of having a single entity being responsible for all identity authentication tasks. Should a government request information from the entity, it opens up the user to privacy issues.

The Liberty Alliance's Federated User Identity is a concept which is a form of competition to Microsoft's .NET Passport.

4.2 Liberty Alliance Federated User Identity

The Liberty Alliance is a body that is defining specifications for networked identity management. The Alliance is an undertaking by a group of organisations and government agencies, in order to provide open technical specifications for a federated identity. When the Liberty Alliance began their operations, the first phase of development involved the setting up of specifications which enabled simplified single sign-on for end users. This process became Liberty's Identity Federation Framework (Madsen 2004).

The use of multiple respected organisations and government agencies allows for a well-rounded set of specifications for the identity management. The problem with an implementation such as that of Microsoft's .NET Passport is that all the specifications have been set up by Microsoft. Although they are the industry leader, one corporation's view on a topic is not necessarily the best for a solution. Hence, the underlying concept for the Liberty Alliance is a consortium made up of leading industry companies, such as Sun Microsystems, to discuss and decide on a best practice to become the industry standard.

4.2.1 Federated User Identity Model

The identity federation concept can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognise the user identifiers and entitlements from other service providers within a federated domain. Through the use of a federated identity domain, service providers establish agreements with other service providers in order that identities from different service provider specific identity domains are recognised across all domains. The agreements set up by these service providers include policy and technology standards to be used by the parties. A mapping is established between the different identifiers owned by the same client in their different domains in order to link the identities (Jøsang & Pope, 2005).

The result of this process is a single virtual identity domain as shown in the figure below:

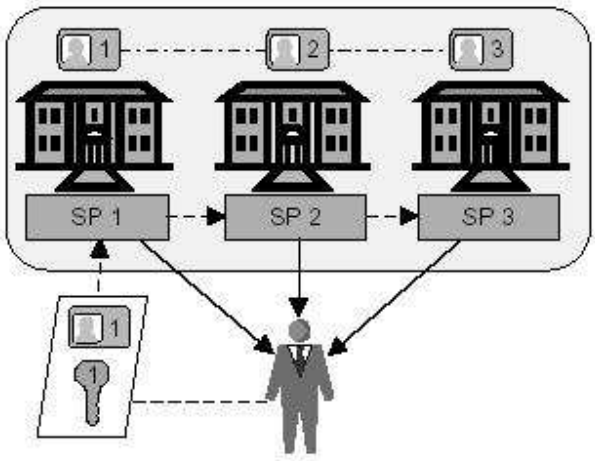

Figure 4.5 Federated User Identity Model (Jøsang & Pope, 2005)

The federation of an isolated user identifier provides the client signing in to the service, the view that there is only a single identifier domain. The client user can possess their own separate identifiers for each of the respective service providers, although the client does not need to possess all of the identifiers for sign in. The reason is because the user possesses a known credential which is sufficient for him to receive access to all services within the federated domain. The inherent problem with this form of model is that users still have to manage multiple identities and credentials, even though the user is not actively using all of those identities. Therefore, the process of identity federation will be most successful when the user wants to manage only one set of identifiers and credentials.

The core differences between the Federated User Identity Model in Figure 4.5 and the SSO Identity Domain Model in Figure 4.2, is the user identity and credential evaluator. In Figure 4.2 there is a single entity responsible for the identification and authentication of all users within the system. In figure 4.5 multiple user identity and credential evaluators may exist. Once a user is authenticated by one system within this federated domain, all other websites within that federated domain can verify the user as being authentic.

Having reviewed the concept behind the model for the Liberty Alliance implementation of a SSO solution for users, a review of the process involved for the successful sign-on of a user needs to be identified.

4.2.2 Liberty Alliance Single Sign-On procedure

The Liberty specifications for Single Sign-on are an enabler to provide single sign-on functionality across different enterprise domains and websites. The use of a browser only authentication method is considered essential for acceptance by users within the market as users frequently switch browsers.

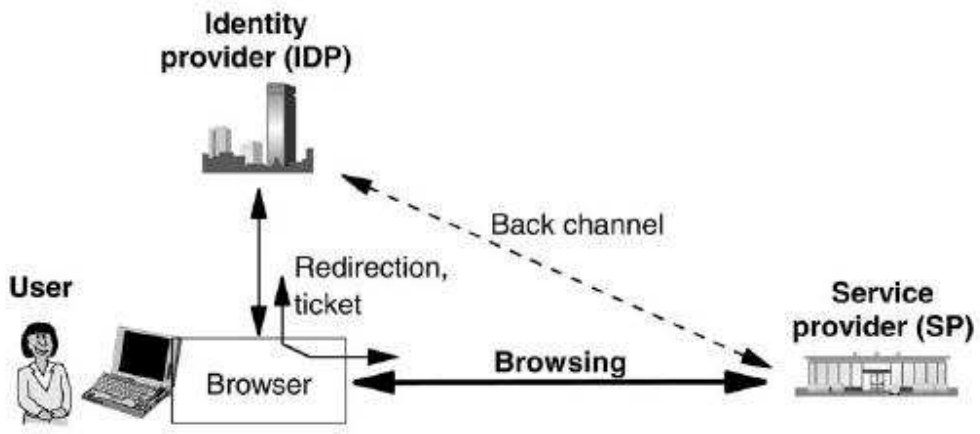

Figure 4.6 - Browser based single sign on (Pfitzmann, 2004)

Pfitzmann (2004) describes the process of Liberty's Single Sign-On as follows:
A user accesses the service provider via browsing online. When submitting a log in request, the service provider redirects the user's browser to the identity provider of the user. The user then logs in through use of a typical user ID and password. The browser and identity provider may, under certain circumstances, reuse a secure session from a recent login. The identity provider then redirects the browser back to the service provider with an additional ticket, to handle other services such as data transfer logistics on other channels. The term of single sign on is only used if a login name or other private user details are transferred.

The benefit to the user shown in this form of implementation is that the user does not have to be redirected to a separate login page for the purpose of authenticating the user. When the user is then authenticated from one service within the circle of trust, all other websites within that trust domain can verify that the user has been authenticated on a sister website and eliminate the need for sign in.

The Liberty Alliance provides a viable alternative to the solution to the .NET Passport. By having a consortium of companies involved in the setting of standards, a broader level of consensus is achieved and the best solution is implemented. Within the realm of SSO the issue with Liberty Alliance is the lack of ability to provide a scalable solution for a user to connect to a multitude of websites. This is due to each setup of the Federated identity solution existing within separate circles of trust. If a user moves between 2 different circles, he or she would be required to reconnect and sign-in with different credentials. From the analysis of two solutions tasked with the identification and authentication of the user credentials, the responsibility is now moved onto the identification and authentication of the accessed website by the user. This is done through an investigation of the Mozilla TrustBar.

4.3 Mozilla TrustBar

The Mozilla TrustBar is a current implementation of the Personal Service Provider Identity model. The TrustBar is a plug-in toolbar used within the Mozilla and Firefox browsers, through which a user can store images mapped to server certificates. Whenever a server certificate is verified, the toolbar checks that a mapping exists, and displays the mapped image on the toolbar while the corresponding page is still being loaded (Jøsang & Pope, 2005). The analysis of the Mozilla TrustBar is from a different perspective than that of the service provider authentication methodology. A large focus is placed on how to secure user authentication processes. This endeavour only solves the risks inherent in the sign-on process of the user, and does not cater for the potential user problems of phishing or website spoofing. The underlying objective of the TrustBar implementation is to make users more

aware of the security behind the pages that they view. TrustBar allows users a quick and easy way to visually authenticate the website they are viewing.

4.3.1 Personal Service Provider Identity Model

Through the use of a form of Personal Authentication Device (PAD), in the case of the TrustBar the PAD is the client browser, users can generate private identifiers service providers by mapping the domain name of the website and other unique identifiers to personally chosen identifiers for the same website. The identifier can be anything that can be recognised, such as text, pictures and sound. This concept is illustrated in Figure 4.7 below:

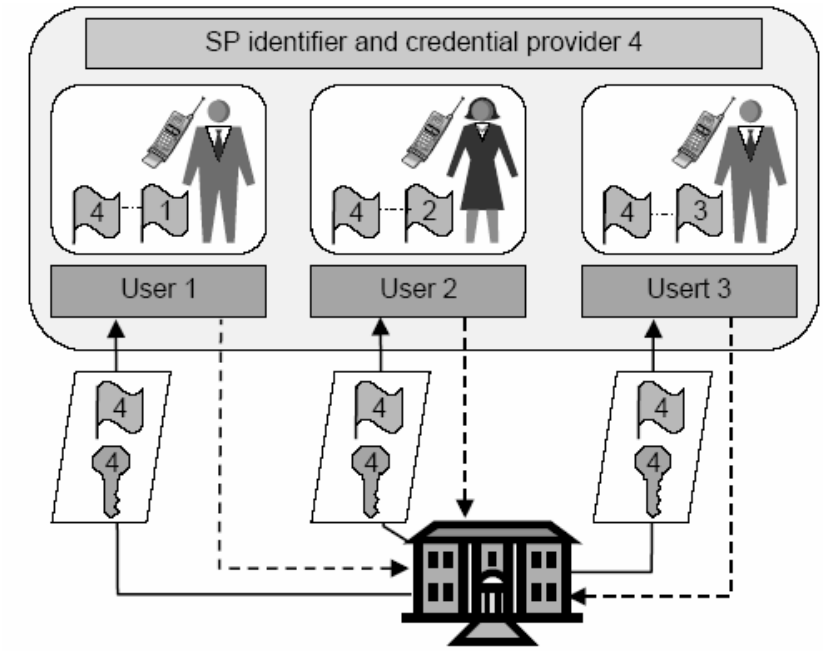

Figure 4.7 Personal Service Provider Identity Model (Jøsang & Pope, 2005).

The index "4" of the identifier and the credential contained in the messages of Figure 4.7 indicates that they were assigned by the centralised identifier and credentials provider with the same index, which when used in practice can be a Certificate Authority or a Primary Key Identifier index. The PKI indexes are shown at "1", "2" and "3" of the SP identifiers depicted within the personal domain of each of the users, indicating that they have been individually assigned by the respective users. The mapping between the global SP identifier and the personal SP identifier of the user, takes place in the user domain. In order for this to

be practical, the user's PAD needs to be directly involved in the authentication protocol (Jøsang & Pope, 2005).

The design of TrustBar allows for users to set up their own identifier for each domain. In the setup for this process they can map pictures or text to these visual identifiers. When a browser then accesses the requested website, the user can then expect to see the visual identifier for the website that they set up. This allows for an easy method of confirming that a website is authentic. In order to fully understand the possible benefits behind the use of the TrustBar implementation, the authentication process of the retrieved websites must be analysed.

4.3.2 TrustBar Authentication

The overall process of the client user authentication on the server attempts to protect the user from potential eavesdropping and modification by Man in the Middle (MITM) adversaries. Large portions of financial and other websites make use of Secure Socket Layer (SSL) and Transport Layer Security (TLS) to authenticate the user. A number of those websites only make use of the SSL or TLS protocols only after the user has typed in a username and password, and clicked 'submit' (Herzberg, 2005).

This form of implementation provides the potential for a MITM to redirect the user to a modified version of the same page. Should this occur, the user can unknowingly release username and password information to a third party through this page. However, the modified page has been changed in order to send the user information back to the MITM. It is clear that the traditional approach to a sign-on methodology does not protect the user from these forms of attacks to their information, and that the user requires an easier way to confirm they are at the website they intended to be.

Herzberg (2005) mentions the ways in which TrustBar provides a solution to the client user problem:

- TrustBar periodically downloads a list of the unprotected login websites that is maintained on the Mozilla TrustBar servers. This list contains all the unprotected login websites which Mozilla track, and any alternate login pages for those websites that are protected. This can be used to redirect the client should an unsafe link be found. There is a trend amongst these websites that when a user accesses one of the unprotected pages, they are automatically redirected to an alternate login page that is protected.
- TrustBar makes allowance for users to assign a name or logo to websites of their own choosing to visually identify the website. TrustBar computes a hash of all unprotected websites for which the user has assigned a name or a logo. TrustBar compares this hash on subsequent access to the same website. Should the website not have been modified in five consequent accesses, TrustBar begins to display a "Same since" and a date value. When the website eventually changes a warning is then displayed when the page is again accessed. As most login pages are structured to just perform the login function, they are not prone to constant change. This can be helpful to users as they can then immediately notice any change to these generally static pages.

Herzberg and Gbara (2007) provide further uses of TrustBar for solving the user problem through the following items:

- In SSL and TLS protected websites, TrustBar shows, by default, the name of the organization that owns the website through the identification from the digital certificate. TrustBar also displays a representation of the logo or the name of the certificate authority who issued the certificate.
- With unprotected websites, TrustBar presents the domain name.
- TrustBar displays a padlock for all protected websites, with the same icon but with a "No Entry" sign over the padlock for unprotected websites.

Mozilla TrustBar solution to the user's web usage condition is novel. The service provides the client with a free facility that can make the user feel far more secure in their online service usage. By providing a visual aid to the user of the current status of the website they are visiting, it gives the user the ability to visibly identify the security available on the website. This will improve the user's overall experience and provide them with a measure of self protection from potential spoofing attacks.

4.4 Comparison

The three models reviewed thus far in this chapter have different perspectives in their approach to the handling of identity management. All the examples chosen have their limitations, since they are not easily comparable. It is not possible to provide a valid comparison of the .NET Passport system which was implemented with a singular methodology, to the Liberty Alliance framework. The reason for this is that the latter is not so much a system, but rather a set of open technical standards that any network of organisations can implement. Every single sign-on implementation based on the Liberty Alliance framework can be scrutinised, but the efficiency of these systems is only as strong as the level to which the specifications are applied. Further complicating this analysis is the Mozilla TrustBar. The TrustBar looks at the identity management paradigm from a completely alternate perspective, that of the user. TrustBar implements similar steps when authenticating, but instead of the authentication of the user, authentication of the website being accessed is performed. The consolidated comparisons, where they can be drawn, are shown in Table 4.1 below:

	.NET Passport (Lopez, Oppliger & Pernul, 2004)	Liberty Alliance (Olsen & Mahler, 2007)	Mozilla TrustBar (Herzberg, 2005)
System	Singular System implemented by Microsoft	Open Specifications with various forms of implementation on multiple different systems.	Single System implemented by Mozilla to handle classification of web addresses
Single Sign-On	Previously multi-organisation single sign-on. Since 2003 single-organisation sign-on	Implementation dependant, supporting multi-organisation SSO	Single verification of websites accessed by user
Choice of Identity Providers	Microsoft was the only identity provider	Allows several identity providers if they are accepted by the service provider	Mozilla serves as identity provider for authentication of websites
Identifiers	Personal Unique Identifier per user	Unique handle per user per federated pair of website	Unique identifiers per participating website
Responsible controller	Microsoft and service providers were single data controllers	Service providers within a circle of trust are controllers at the time users visit their websites	Mozilla and service providers as single data controllers
Contractual Framework	Contract between Microsoft and service provider	Implementation dependant -Contract between every website in a circle of trust -Depending on implementation other models may exist, such as every participating service provider having a contract with one party which organises and administrates the circle of trust	No contract required, makes use of open source community

Table 4.1 – Comparison of .NET Passport, Liberty Alliance and Mozilla TrustBar

Table 4.1 attempts to compartmentalise the three models into specific sections for comparison. The .NET Passport is implanted as a single entity which is maintained and managed by Microsoft. All usage of the .NET Passport requires adherence to Microsoft standards by website vendors as stipulated within contracts between Microsoft and these parties. The Liberty Alliance makes use of a set of open specifications that can be implemented by parties in various ways to allow for an SSO environment to be created for users. The SSO facility will however only apply between websites within the same circle of

trust between the vendors, and should a user move out of this circle they will need to resubmit their login criteria. The responsibility for the validity of the user at time of SSO is placed under the controller of the website. The TrustBar system is very different, looking at user issues from the perspective of the user. TrustBar currently works off a single system which is implemented by Mozilla, handling the classification and analysing the security quality of the websites to create a central repository for determining website validity. TrustBar relies on the open source community for its survival. It provides an easy to use system for the authentication of websites for the user.

Overall the three models analysed provide a significant step towards meeting the overall goal of an integrated system for protection of the user in the online environment when looking at each of their components. The .NET Passport provides a facility for the identification and authentication of the user within a secure and reliable environment. With the immense reach of the Microsoft solution, the .NET Passport provides the ability for users to span their SSO experience across multiple websites, a feat unable to be achieved with the current setup of the Liberty Alliance Framework. The Liberty Alliance does however provide a far more flexible solution to the dominance of Microsoft, allowing a flexible framework of best practices for companies to adhere to in order to set up their own. On comparison of the Single Sign-On technology, .NET Passport is a single platform, providing a single sign-on facility for websites associated with its service. Depending on the form of implementation of the Liberty Alliance frameworks, the setup can support multi-organisations SSO. The TrustBar however is responsible for a single verification of user accessed websites. To place each model into a specific category for the issues they resolve the models can be summarised as follows:

- Microsoft .NET Passport – Provides a solution for a broad scale implementation of identification and verification of users within an SSO environment. It also provides a relatively simple integration between vendors, due to a single user identification provider.

- Liberty Alliance – Provides a more flexible implementation solution for the website vendor through the circles of trust, although a limited solution for identification and verification of the user within an SSO is provided due to potentially limited sizes of the circle of trust. With each website within the circle of trust providing their own login forms for the user, and with a greater level of trust between the websites involved, the ability to audit users' movements within the system is greatly increased.
- Mozilla TrustBar – Provides a way of identification and verification of the website from the user perspective. Through the implementation of an easy to use identification and verification process to immediately alert the user to potential threats within the website they are attempting to access, the user is provided with a greater sense of security and control.

4.5 Conclusion

The underlying question the user of a system will always need to ask is the concept of trust. In this chapter three concepts of identity management were investigated. The first two are Microsoft Passport.NET and the Liberty Alliance Federated Identity. Subtle differences arose between the two forms that provide a single sign-on for the user. Finally, the chapter delved into the perspective of identity management from a more external point of view through the possibilities available under Mozilla TrustBar. The overview of these three models provide the basis for Chapter 5 in which the user experience is fully analysed and a model is drawn up based on the experiences of the models analysed in this chapter.

Chapter 5

A USER CENTRIC ONLINE IDENTITY & AUTHENTICATION MANAGEMENT MODEL

5.1 Introduction

Chapter 4 reviewed three existing identity management systems, which are implemented internationally. The overriding theme of all the model implementations is the ultimate protection of the user's experience. The .NET Passport and Liberty Alliance framework were reviewed to provide an insight as to how a user is identified in a single sign-on environment. A view from the user perspective was then taken by looking at other potential benefits that the Mozilla TrustBar possesses over that of a traditional SSO approach. A comparison of the attributes generic to the models was performed to show the strengths and weaknesses of the relative models.

Chapter 5 proposes a hybrid model which can be used to provide a less experienced Internet user with better protection and security when making use of the online environment. The chapter begins by looking at the pitfalls of the previously discussed models in Chapter 4 and the processes required for both user and IT system authentication to occur. The chapter then looks at the authentication of IT systems and users. Within this process the roles of the user for the authentication of the IT system, and the role of the IT system in the authentication of the user, are defined. Having defined the requirements from each of these two processes, a hybrid model for the protection of the user is proposed. Through this model, the requirements for an effective hybrid authentication system can be deduced. These requirements can then be put to use to ensure that a naive user is adequately protected from the potential threats that dominate the online environment. The emergent model is then discussed. Finally the model is put into context in the terms of general systems theory.

5.2 Inherent Issues from Existing models

Although all three models discussed in Chapter 4 do provide a valued service, none of the three cover the overall experience of the user. This is due to each model focusing exclusively on either the sign-on or website identification issues. None focus on the broader issues of the user and the total protection of the user within the online environment. The overall state that needs to be adhered to for the protection of users in the online environment can be summarised as follows:

- Scam Protection – Users need to be aware of the potential scams that exist in the worldwide web. Education is the best form of prevention from such incidents. Included in these forms of attacks are requests via email for client banking information and general usernames and passwords (Bradley, 2007).
- Website Spoofing – Possibilities exist for users to be automatically redirected to, or directly logon to websites which appear identical to the expected website. The only notable difference is that of the domain name being slightly different from the expected domain. Such websites will have login credentials shown as expected, but will be sending the user login information to a malicious third party. Users need to be aware of fraudulent websites and the potential risks that can occur should their information be entered into such websites mistakenly (Herzberg, 2005).
- Multiple Verification – When making use of multiple website services, each with individual login criteria, a facility exists to improve the user experience through the use of a single sign-on methodology. One sign in will reduce the possibility of interception of client login criteria, and will promote ease of use online. Although this format promotes significant ease of use for the user, the convenience comes at a price. By removing the need for multiple authentications, should the user's identification information be compromised, the security of the user information on a multitude of websites will be jeopardised. Should each website possess their own login criteria and security protocols, the security of the user information overall is better protected (Lopez, Oppliger & Pernul, 2004).

- Credential Security – The credentials of the user need to be securely stored and transmitted when authenticating for single sign-on environments. Losses of this form of information could be devastating to the clients' online identity, either by financial means, or personal status loss.

Each of the models assessed has attributes that cover these user requirements but overall they do not cover the entire online user experience. As shown in Table 4.1 of Chapter 4, the methodologies of each model differ significantly in the way in which they deal with the identification and authentication of the user and websites accessed. By assessing the shortfalls of the described models, the required elements for a successful model can be deduced.

5.2.1 Liberty Alliance Federated Identity

The Liberty Alliance Federated Identity Framework provides a setup for a strategic partnership amongst individual businesses. The overall process of user single sign-on is secure to the user. The inherent problem within the Federated Identity proposal is the size of the domain. Domains are set up by like-minded websites who choose to be within the same domain. The potential is still great for the user to have to endure having multiple user profiles across multiple domains that may or may not be federated into one identity domain or circle of trust.

The concept of a circle of trust (CoT) refers to the business, legal and privacy considerations that govern federated identity management between organisations. Through the use of a CoT within the network of companies wishing to form such a partnership, the standards for interoperability are defined. By making use of the Liberty Alliance Frameworks, the standards for communication and security in the transmission, identification and authentication of user details is defined to promote ease of interoperability amongst all participants within the CoT (Liberty Alliance, 2007).

The use of the Liberty Alliance Federated Identity Framework has two major disadvantages. First is the use of the CoT principles inherent in the framework. The framework calls for the use of protocols and controls between all parties within the CoT. The setup of all companies is different, thereby making the change of company protocols to the Liberty standard an expensive and time consuming process. Furthermore, the scope of the single sign-on of a user is limited to only the websites that are engaged in the CoT relationship. Therefore, even with a CoT firmly in place, there is no assurance that the user will make use of the SSO opportunities, as they may never interact with another website within that particular circle.

Secondly, should the user make use of the SSO facility within websites of the CoT, the user is then risking their personal information via a lack of "defence in depth". The "defence in depth" concept is an information assurance strategy on which multiple layers of defence are placed within an IT system. The principle behind the "defence in depth" approach is ensuring that any potential attacker must compromise multiple defensive procedures, in order to successfully gain access to the system (IATF, 2002). By providing a single criterion for identification of a user, the multiple levels of security for the identification and authentication of a user per website are removed. Through this process, the user is then exposed to potential risks, in which once their login credentials are compromised, and an attacker can gain access to user information stored on all other partner websites in the CoT.

The Liberty Alliance framework can be a very successful and viable solution to provide a client with a seamless online experience should a global implementation of trust and an overall domain of trust prevail.

5.2.2 .NET Passport

Microsoft's .NET Passport implementation provides a global potential solution to the single sign-on identity problem. From a user perspective Microsoft is viewed as the industry leader. Over the years Microsoft has cemented its dominance over the computer industry with its

operating systems. This overall dominance instils a form of user recognition and reliance. Microsoft also possesses the capability of setting up the massive infrastructure required to undertake a global identity domain.

The .NET Passport has some major disadvantages. Similarly to the Liberty Alliance Federated Identity Framework, it also suffers from a lack of "defence in depth". Users need only sign in once to gain access to all websites making use of the .NET Passport SSO methodology. This will similarly expose the user to potential risks. If their .NET login credentials are compromised, an attacker can gain access to all websites that are affiliated with the .NET Passport program. Secondly, users should be made more aware of the perils of making use of the automatic sign in to .NET Passport. Use of this facility should be removed as cookies are permanently activated and the user is never signed out of the system. This can lead to potential security breaches under the user's identity. Along with these problems within the .NET Passport framework is the problem of a developing monopoly situation. Having a single company, such as Microsoft, dictating terms on how technologies should be implemented, can become problematic within the industry, as consensus will not necessarily be followed in the setting up of the best practices for SSO environments. Furthermore, with one company maintaining full control of user information, the civil liberties of the service users could be compromised should the company be forced to disclose this information to government.

5.2.3 Mozilla TrustBar

The Mozilla TrustBar implementation provides a unique view, focusing on the protection of the user. Implementations of identity management solutions primarily focus on the protection of the client data within the process of identity authentication. TrustBar takes a wider view of the identification issue, and promotes a format through which a user can themselves ensure they connect to the website that they intended to. By giving the user the ability to verify the website they are attempting to access, the user plays an active role in the security process and their actions determine the course of action on the website. It ensures

that the user is not potentially exposing their login credentials via a spoofed website. The disadvantage of the TrustBar is the displaying of the verification information for the website that the user is accessing. A naïve user may simply choose to ignore the warnings that are presented to them. What is ultimately needed is more user interaction in determining that they are in the correct domain.

The major disadvantage of the Mozilla TrustBar framework is the lack of provision of an overall solution for the protection of the user. The TrustBar is simply an add-on to a browser and does not provide any facilities for SSO opportunities for users. For this solution only protects the user from spoofed and less secure versions of the intended website, and plays no role in the protection of user credentials within an SSO online implementation.

In order to adequately develop a model to ensure the users' protection, an understanding of the attributes required for authentication of a person by an information technology system, and the requirements for a user to authenticate a system, need to be identified.

5.3 Authentication of IT Systems and Users

A principal cause in the increase in identity related crimes in the online world is due to authentication procedures in the online world being far less secure than those in the offline world. A bank may have thick walls, security guards, and a secure vault to protect the customer investments, for example. This proposes a significant obstacle to any criminal wishing to break in. Within the online environment the point of entry can be as simple as a username and password. Through the use of a brute force attack and the computing power of modern day computers, the security controls can be compromised. The process of social engineering to acquire client information can make an attempt to access client information even simpler. Through the process of making a system online from its offline predecessor, the technical authentication procedures are adapted to the online capabilities, frequently without adapting the security measures (FIDIS, 2006). The offline procedure allows for

security checks to take place far easier than the online procedure that it replaces. The authentication of the actual website may be adequate, but if users are incapable of establishing the trustworthiness of the website they are lured to, this does not help.

The traditional movement of existing company security infrastructures to the online equivalent can be a complex task. This is due to controls existing in the real world, such as high walls or fences, not necessarily having an equivalent in the online environment. By making use of more controls and checks and by having dual authentication performed by both users and systems, a more secure environment for the online user will be developed.

5.3.1 Authentication of users by IT Systems

The process of user authentication is principally linked to the verification of the user identity in order to control user access to restricted resources and areas. Authentication is based on something an individual possesses, such as an identity card or passport, something an individual knows, such as a password or PIN, or something an individual is, being their human characteristics. The core advantages of using the processes of possession and user knowledge are the ease through which such systems can be configured and set up, the low cost involved in the implementation, and the ease of use of the system for the user. However the inherent problem in these two authentication forms is the ease with which passwords or smartcards can be shared or lost, thereby compromising the user security. From a technical viewpoint, an identity is nothing more than a digital pseudonym that represents a person. Because of this, measures are needed to prove that the digital pseudonym belongs to the person who claims it as their own. (FIDIS, 2006)

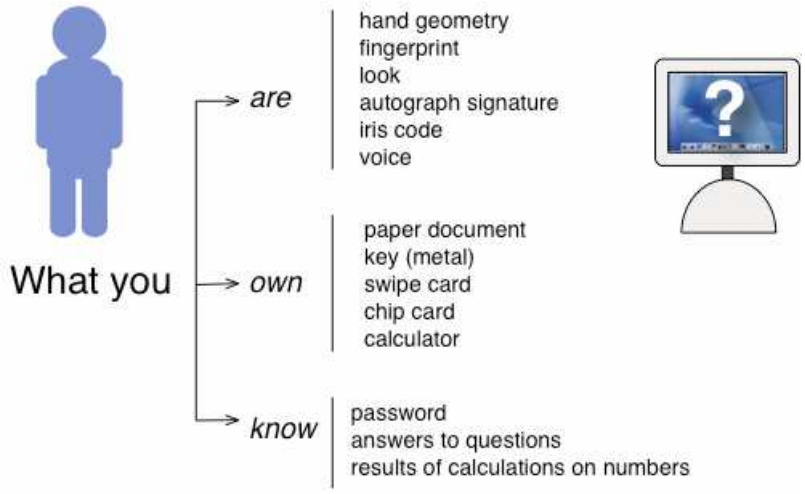

Figure 5.1 - Authentication by an IT System (FIDIS, 2006)

Figure 5.1 depicts how an IT system can determine the authenticity of an individual. When an identity is used, it must always be in connection with proof that it was used by the person to whom it belongs. This process is known as dual authentication which is stronger than a single form of authentication. This is due to the increase in criteria that is required in order to identify the user. By increasing the number of unique identifiers required to be met by the user, the "defence in depth" strategy applies by providing more comprehensive protection of the user identity. Based on these, IT systems are able to recognise a human by:

- what he is through the use of biometric techniques
- what he possesses
- what he knows

The more controls that can be implemented via the use of identification criteria in an authentication process cause an increase in the level of certainty that the authorised identity is accessing the system. Through this process of making use of more criteria for the authentication process, higher levels of trust by both the user and the system are created. This translates to a strong security environment existing within the system.

5.3.2 Authentication of an IT System by a Person

Thefts of user identification information, such as usernames and passwords, are performed by deceiving a user into believing that an IT system is what it claims to be. Via this spoofed website, the user enters their login information and attempts to connect, inadvertently sending their identity data to the hoax website perpetrator. A user authenticates an IT system through three points as shown in figure 5.2.

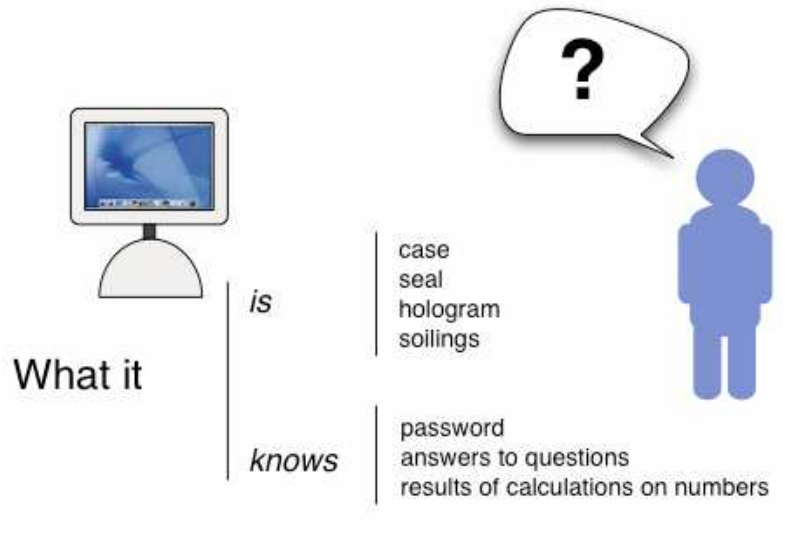

Figure 5.2 - Authentication of an IT System by a Human (FIDIS, 2006)

These points as described by the Future of Identity in the Information Society (FIDIS) are:

- What the IT system is – By looking at the information coming through on the displayed website, the user can determine the validity of the visited website. The immediate method of identifying a website is through the assessing of the website's URL. If the URL corresponds to the website the users expected, they continue the assessment by determining the validity of the website's digital certificates. In checking the digital certificates the user can determine the validity of the website through the scrutiny of the digital certificate, particularly looking into the issuer of the digital certificate and the dates for which the certificate is valid. This process can be automated through the use of a system such as Mozilla TrustBar.

- What the IT system knows – Through the registration process the user will setup their initial profile consisting of a username and password. Additional to this process, some websites may make requests for other personal information relating to the client, such as a mother's maiden name. Through display of this information through user interaction, the user is ensured they are on the correct website.

Through the use of both user authentication and system authentication, a user can ensure they are making use of a valid Internet website. Thereby a generic model for the promotion of an overall solution to the problem of encompassing the entire user experience is required to adequately protect the user from the possible threats of online identity theft.

5.4 A Model for Securing the User Online experience

In order to protect the user from the number of threats to their online identity, an approach is needed in which both the authentication of the user criteria and the authentication of the website visited online are made possible. In Figure 5.3 a model is proposed which promotes a dual pronged approach to the protection of user information within the online environment. This model addresses user protection from two angles. Firstly the validity of the website is checked and reported back to the user. This is done to ensure that the user is attempting to access and authenticate on the correct version of the website. After this process, the process of SSO authentication takes place to allow the user to make use of the benefits within the SSO environment.

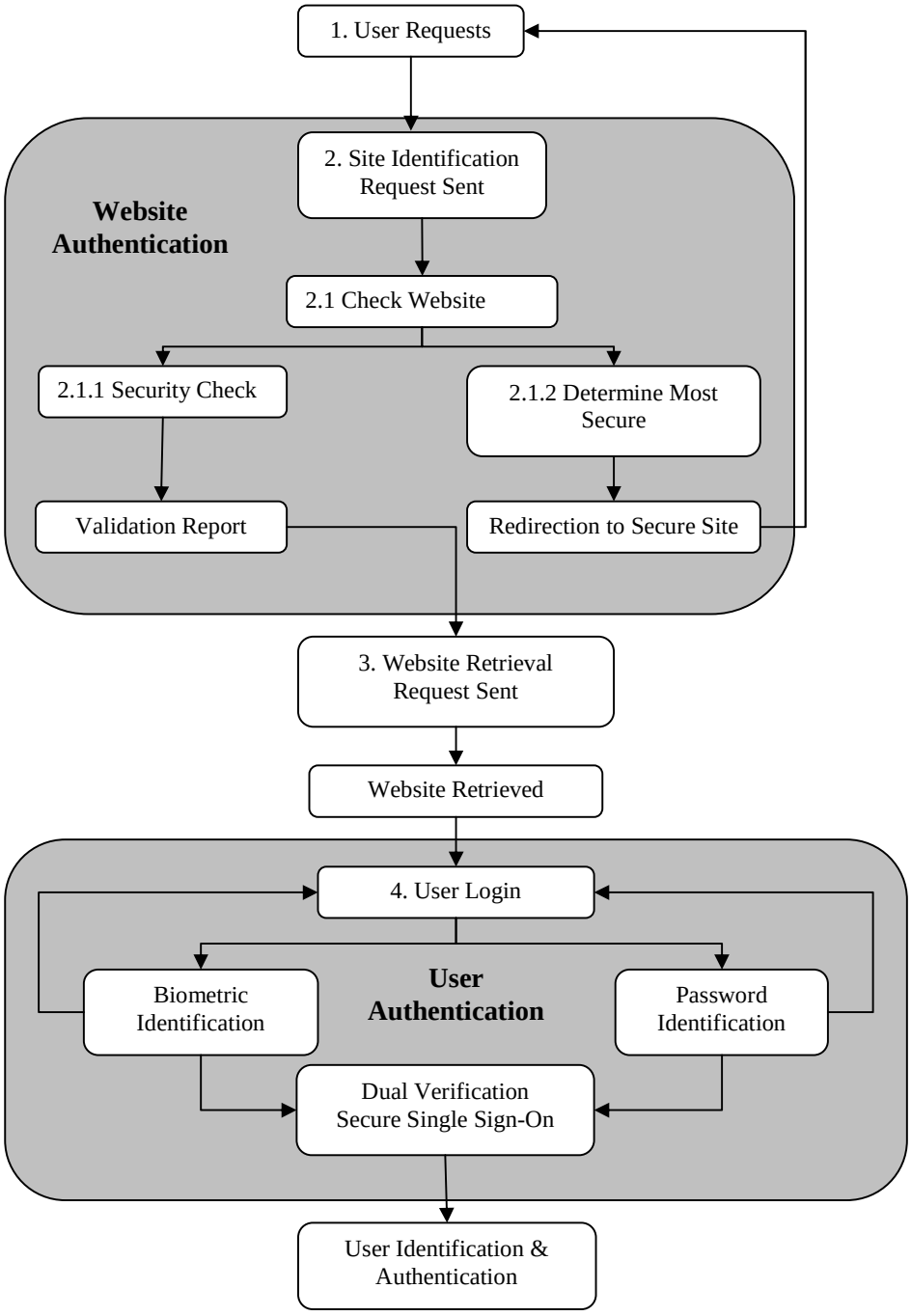

Figure 5.3 – Model for User Centric Online Protection

5.4.1 Description of Model

The process described in the model is expanded as follows:

1. User Requests Website – The user makes use of their browser and enters the URL of the website they intend to visit. From selection of this website the process then moves into the process responsible for the authentication of the website.

2. Website Identification Request – On the user performing a request of the intended website, a request is sent to a central repository for the validation of websites, such as the repository used by Mozilla TrustBar. The information in this repository will provide information to the user in order for them to validate the security of the website.

2.1 Check Website URL – With the information stored in the repository, a number of checks take place in order to determine the security built within the requested website.

2.1.1 Determine Most Secure Website - A number of websites potentially have more secure web pages, which are not necessarily set as the default login page. In these cases the repository will determine which website is the most secure. If a more secure inner link for the same domain is found, the repository sends back a response to the user browser in order to redirect to the more secure website. Should this occur, then the entire process begins again.

2.1.2 Website Security Check – This process involves checking the requested URL. Based on the URL the repository then searches in order to determine the validity of the digital certificates, the authority of the certificate issuers, for example Verisign, and also if the website is flagged as a spoofed website. The result of this is a URL validation report, which is then sent back to the user browser, in order to display the results and allow the user the opportunity to validate the website themselves, from these results.

3. Website Retrieval Request Sent – When the user requests the website, the physical request to retrieve the website is sent and the website is retrieved as per normal HTTP protocols.

4. User Login – Once the page has been loaded with the information required for the validation report, the user then attempts to login to the single sign-on website. In this process

to promote more secure sign-on a biometric form of input, such as user fingerprint identification, is sent along with the traditional password identification. Should either of these validation properties fail to achieve a positive identification, the user is sent back to the initial login page. Should both criteria match, the user is then verified and authenticated within the single sign-on environment. This process will then ultimately lead to secure user identification.

5.4.2 Relation of proposed model to General Systems Theory

The concept of General Systems Theory proposes that systems work individually within their own environments and achieve their sub-goals. When the overall system is analysed and each subsystem is assessed as part of the whole environment, an emerging property becomes evident, through which each sub-system adds a benefit which contributes to the overall functioning of the whole system (Heylighen & Joslyn, 1992).

When a user makes a website request, there is uncertainty on the part of the user, on the security of the environment through which the user is attempting to access. This process involves a large level of trust on the part of the user, that their information is not being intercepted by a third party. By creating a dual pronged approach to protect the user, a secure environment is created in which the user can have confidence in their online environment's security.

The process of identification and validation of a website which a user is attempting to access provides an intermediate step in the overall protection of the user. With the implementation of controls with the user in the form of visual markers to easily identify the website they are attempting to connect to, the user plays an active role in their own protection. This website identification and authentication process for the user can be kept as an individual subsystem, and work individually just within this role. As a single component of the system however it does not provide the full functionality to protect the user from all potential online threats.

In the process of user identification and authentication at time of sign-in, the verification process of the user is built upon by the dual forms of authentication of both biometric and password verification. Each of these processes can be seen as subsystems in the overall protection of the user. The authentication of the user by means of the username and password validation would run as a separate process to that of the biometric authentication. All subsystems work together to provide an improved level of authentication for the user. By making use of a dual authentication process for the process of identifying and authenticating the user, the website then has a higher level of certainty that the user is who he or she claims to be.

Based on the above mentioned subsystems, similar parallels can be seen between the proposed model and general systems theory. The identification of the user is broken down into two parts. The first is responsible for the validation of the user through the traditional means of username and password. The second is responsible for the validation of the user through biometric forms of identification. Each of these processes or subsystems is responsible for a portion of the whole solution. Without both processes the identification and authentication of the user will be flawed, as each system individually will not adequately identify the user. Similar to this is the incorporation of the system authentication by the user. With only user identification the website could be fraudulent, and without the user identification, the user could not be identified. By making use of each of the smaller processes for authentication the check within both the website authentication process, and the user verification process, each process builds on to the other and creates an emergent property which can be defined as a system for the greater protection of a user within the online environment.

5.4.3 Conclusion

This chapter provides an insight into the requirements to protect a user from the threats within an online environment. Through the use of a username, password and biometric

forms of identification, the accuracy of user identification is increased. In addition to this the ability for the user to identify the website attempting to be accessed, and verify its authenticity, protects the user from potential online threats such as spoofing. By the combination of these to forms of authentication, from the user and from the system side, an enhanced level of security is created for the user. This protects the user from potential threats from website spoofing and identity theft. Through the use of a dual pronged approach to user and system authentication, a higher level of trust is produced between the two parties.

Chapter 6

CONCLUSION

6.1 Summary of Chapters

The adoption of the Internet and the numerous opportunities available within it has made an indelible impact upon modern society; unfortunately with its adoption within the mainstream population cyber crime has increased. The reason for this is the major difference between the real world and the online environment. In the real world trust between the customer and the business retailer is gained far more easily. The real world has tangible attributes, such as guards and locked doors which the user can immediately recognise and builds a sense of trust. In the online environment the propagation of trust between user and website is far more difficult to establish. In addition to this issue is the increase in the number of new users to the online marketplace. With these new users there are high levels of susceptibility for naïve users being targeted through social engineering techniques to retrieve their user credentials. It is important for users to have their information adequately protected through all stages of their online experience, in order to shield users from such threats.

Chapter 1 provides a background to the problems faced by users in the online environment. The research area and the research problem were introduced to provide the processes that should be adhered to by client users and websites to ensure that a user's identity information is adequately protected online. The intended objectives, and research methodology to be used, were presented. Chapter 1 concludes with a high level overview of the research project.

Chapter 2 provides an overview of the identity management process. By showing the laws stipulated by governments for the protection of an individual's online identity, the emphasis

placed on the protection of user information is shown. The types of identity that exist, and the attributes associated with them are presented, along with the generic process for the identity management life cycle to provide a background to the topic and the processes that should be performed for effective management of an identity. The aims for identity management within the public and private domain are presented, to define what is expected by both domains for the management of an identity. The concepts underlying an identity management framework are presented in order to show the process for the implementation of an identity management solution in an organisation, and the benefits of such a process. Finally an enquiry is made into the setting up of standards initiatives for the management of identities, and how they came to exist.

Chapter 3 performs an investigation into the access and authentication management process. With the significant difference between the environments of the real world and that of the online environment the management of user levels of trust within the systems is an important issue to consider. Statistics are presented relating to the usage of online systems and effect a lack of trust can have on a business. Based on this premise, the role of access control is presented. Within access control the accountability aspects are discussed to show the benefits of access control logging. Techniques for access control are mentioned to give insight into how website should be managed. The life cycle of access rights are presented and provides an insight into trends of how user access rights tend to increase regardless of their system roles, until they are removed. This is in contrast of the best practice of access control and assigning only the necessary access rights to users to perform their function. The chapter concludes with an investigation into the role of access management in terms of the compliance within the best practices of corporate governance in ITIL and COBIT.

Chapter 4 performs a comparison of three existing implementations of identity management solutions. An analysis of the Microsoft .NET Passport solution for SSO of users is presented, by first looking at the common user identity model, to provide an overview of the identity

model verification process common across all forms of identity models implemented in the three selected models. The .NET Passport model is analysed paying particular attention to the SSO Identity domain model. The processes are analysed with a focus placed on the registration and authentication process for users within an SSO environment. The Liberty Alliance's Federated User Identity framework is assessed to give a different perspective to the SSO solution supplied by Microsoft. The federated user identity is proposed by a number of companies to promote interoperability within setup circles of trust between businesses for the purposes of SSO. The Mozilla TrustBar is analysed to look at the identification and verification from the perspective of the user. Finally a comparison of the models takes place through the use of a table to easily show the core differences between the three models.

Chapter 5 provides a proposal for the implementation of a dual pronged approach to the identification and authentication of both users and websites. By making use of a dual authentication approach to ensure that both the website and the user are valid, a higher level of protection to the user's identity is achieved. The chapter begins by looking into the issues affecting the existing three models for identity management, and the expectations of the user for an overall solution for protection from online threats. The process for the authentication of users by IT systems, and the authentication of IT systems by users is presented in order to determine the requirements for performing a dual form of authentication within a single system for authentication and SSO. The model for a dual pronged approach to the identification and authentication of both user and website is presented and described. The model is then described in terms of its contribution to general systems theory.

6.2 Solving the Research Problems

The main research problem set out in Chapter 1 was, **"What processes must be adhered to by the client user and the website, to ensure the protection of the user's identity in the online environment?"** In order to effectively answer these questions, a set of sub-problems

were defined, that needed to be answered in order to solve the overall problem. These sub-problems were:

- **What are the critical success factors for identification and authentication of a user at time of sign-on?**

  Chapter 2 discussed the laws and regulations stipulated by governments for the protection of an individual's online identity. Based on these laws the standards for identification and authentication for the protection of user information is defined through the use of COBIT and ITIL. Further in Chapter 2, the aims for identity management within the public and private domain were discussed, in order to determine the requirements that would best suit both domains to manage an identity. Core to the process of identification and authentication is the guarantee that the expected user is connecting to the system. By making use of the traditional username and password criteria, and a biometric identifier in order to validate the user, the certainty level in the user validation is that much greater. The concept of an identity management framework was presented in Chapter 2 to determine the best process for the implementation of an identity management solution within an organisation, and the resulting benefits to making use of such a process. Chapter 3 provided some further background on the importance of levels of trust for users' and businesses mutual benefit. The importance of access control was discussed to provide insight into the techniques used to successfully control user access, and effectively protect their system from threats by making use of concepts such as the life cycle of access rights for users. The concept of SSO was presented throughout the research project, and the requirements for user reconnection to the SSO environment were mentioned in Chapter 4. In adhering to practices of securing the user login area and the controls in monitoring this area for potential threats, increasing the user identification criteria by insisting on alternate biometric forms of identifiers, the owner of the website is ensured of a higher level of confidence that the expected user is connected to the system.

Based on the findings from this sub-problem, the following processes should be in place to solve the overall research problem:

- Users need to be identified and authenticated within an environment that is as secure as possible, making use of the strongest forms of security protocols available on the Internet.
- Users need to be identified through the use of as many identifiers as possible. By making use of a username, password, and form of biometric authentication, the chance that the incorrect user is attempting to access the website is greatly reduced.

Therefore, this sub-problem has been met by determining the critical success factors for user identification and authentication are a secure sign-on environment and an increased number of user credentials.

- Second sub-problem: **What process can be used to ensure a user is connecting to an authentic website?**

  Chapter 4 provides an analysis of three common identity management models. The Mozilla TrustBar was analysed to provide an insight into how a user can be involved and provide their own website authentication. By providing the users with a process for adequate and easy to use identification of the website based on website authentication criteria, the user plays an active role in the determination of the validity of the website. By making use of a facility similar to the Mozilla TrustBar a simple process of identification and validation of the website and the security criteria built within the website is provided. Through the introduction of a centralised repository for listing the security of websites and the most secure website within a specified URL to reroute users away from possible security threats within a website, extra value is added to this process.

Based on the findings from this sub-problem, the following process should be in place to solve the overall research problem:

- The security criteria of a website, and its validity should be presented to the user in an easy to understand format, for the user to immediately identify any potential risks to their online identity by signing in to a potentially compromised website. Through this the user plays an active role in the identification and authentication process.

Thus, this research project has adequately addressed this sub-problem by identifying the need for user involvement in the process of validating the website they are attempting to access. This sub-problem helped contribute by showing the benefits of having user involvement in the authentication process.

- Third sub-problem: **How can users be adequately protected from common online threats?**

  In the analysis of the three identity models set out in Chapter 4, the processes involved in the use of an SSO environment were discussed in the use of Microsoft's .NET Passport and the Liberty Alliances Federated Identity. By making use of similar technology for the identification and authentication of users during the sign-on process, but making use of a further biometric component, the user's information is made more secure. Further controls that should be considered are the locking of user accounts when the identification criteria are not met, and possible use of login timers to ensure that users reconnect when they have been inactive for a prolonged period of time. Chapter 5 proposes a model which makes use of a dual pronged approach for the authentication and identification of both the user and the website. This model is based on the best practices defined from the industry leaders in SSO (Liberty Alliance and Microsoft) and the expectations of the user for an overall solution for protecting themselves from online threats. The model proposes a solution which handles both forms of identification. Through this process the website

is identified and authenticated by the user's browser, and the user goes through a process of identification and authentication during the process of sign-in to the website. By making use of such a system with two forms of authentication to protect both the user and the website, cases of potential fraud situations and identity theft are avoided. Through such a solution which handles both these authentications in a simple to identify and easy to use framework, the security of the naïve user is ensured.

Based on the findings from this sub-problem, the following process should be in place to solve the overall research problem:

- Login counters should be implemented to lock users out of their accounts should they fail to authenticate within a designated number of attempts.
- Login timers should be implemented to ensure the user has not been compromised through the interception of their session information. If the user's session becomes inactive for a prolonged period of time, the user must be forced to sign back into the SSO.
- Users and websites should play an active role in performing a process of dual authentication, each by the other party, to ensure that a greater level of trust is built between them.

The processes for controlling the identification and authentication of both the user and the website need to be enforced to create a secure online environment.

Hence this sub-problem has been addressed by providing suggestions to protect the user from potential online threats. Together the three sub-problems have addressed the research problem as stated in the problem statement.

6.3 Future Research

As a continuation of the research presented within this research project, empirical data should be collected to determine the specific requirements of both Internet users and the websites wishing to incorporate SSO methodologies within their customer service, what they consider acceptable levels of performance and the priority they attached to this type of initiative. An analysis of the user study, including a background of users and will ensure that the needs of all users and service providers are considered in the scoping and development of the system and will ensure that the focus of the system remains true.

Chapters 4 and 5 provide a number of issues for potential further research which fall outside the scope of this project. The privacy rights of the users in making use of a system which will be responsible for the protection of their online identity information and having their online history of websites visited being recorded, can be researched. Should this information fall into criminal hands or be requested by a government, the privacy rights of the individual will be compromised. A further avenue of research is the cost implications and how such a system will be adequately governed. The setting up of an organisation tasked with validating users and websites will need to be investigated to determine which organisation will be best suited to handle this information, and the challenges surrounding securing the information on such a critical system for user protection. Further research is also required in the determining of how the proposed model could be best implemented to provide an easy to use solution for the protection of the user and the website from user fraud and identity theft. These areas need to be researched in depth to ensure the release of such a system is viable within the current Internet market.

6.4 Summary

A comprehensive framework for the protection of the user within the online environment does not yet exist. This may well be due to the chaotic nature of the Internet, through which each website and user browser would need to require a unique blend of technologies in order

to make such a solution work. However, this research project contributed by providing a model for the integration of user and website validation procedures along with sign-on processes into one combined process. The next step in this research area could be the conducting of further research into how the model proposed within Chapter 5 can be implemented to provide an easy to use solution for the protection of users.

References

Absa (2006) Absa introduces more Internet Banking security measures.
Retrieved May 2007, from
http://www.absa.co.za

BMC Software (2006) Supporting the identity management lifecycle with BMC Identity Management, Suite 5.5, Technical White Paper.
Retrieved July 2007 from
http://www.bmc.com

Bradley, T. (2007) Gone Phishing.
Retrieved October 2007, from
http://netsecurity.about.com/od/secureyouremail/a/aa061404.htm

Caslon Analytics (n.d.). *Identity crime.*
Retrieved May 2007, from
http://www.caslon.com.au

Chau, P.Y.K. Hu, P.J. Lee, B.L.P. & Au, A.K.K. (2007) Examining customer's trust in online vendors and their dropout decisions: An empirical study. *Electronic Commerce Research and Applications*, Vol 6(2), pp 171-182

Consumers losing trust in online banking: survey (2007). *Computer Fraud & Security* Vol 2007(2) pp 4

Cuppens, F. Cuppens-Boulahia, N. & Ghorbel, M.B. (2007) High level conflict management strategies in advanced access control models. *Electronic Notes in Theoretical Computer Science* Vol 186, pp 3- 26

Cybersource 8th Annual online fraud report, 2007 Edition.
Retrieved May 2007, from http://www.cybersource.com

De Leeuw, E. (2004) Risks and threats attached to the application of Biometric technology in national identity management.
Retrieved May 2007, from
http://secure.gvib.nl/afy_info_ID_1322.htm-ThesisMSIT.zip

DigitalIDWorld (n.d.) What is Digital Identity?
Retrieved June 2007, from
http://www.digitalidworld.com

Duke University (n.d) *Authentication vs. Authorisation.*
Retrieved May 2007, from
http://www.duke.edu

Emigh, A. (2005) *Online Identity Theft: Phishing technology, Chokepoints and Countermeasures.*
Retrieved June 2007, from http://www.antiphishing.org

FIDIS (2006) D5.2b: ID-related crime: Towards a common ground for interdisciplinary research.
Retrieved September 2007, from http://www.fidis.net

Firozabadi, B.S. & Sergot, M. (2002) Contractual access control. *Proceedings of 10th International Workshop on Security Protocols, Cambridge UK, 2002*

Friedman, B. Nissenbaum, H. Hurley, D. Howe, DC. Felten, E. (2002) Users' Conceptions of risk and harms on the web: A comparative study. *CHI2002: changing the world, changing ourselves.*
Minneapolis, Minnesota, USA, 2002, pp. 614 -615

Gordon, T. (2004) Quantifiable benefits of implementing identity management systems
Retrieved July 2007, from http://www.isd.salford.ac.uk

Granova, A. & Eloff J.H.P. (2005) A legal overview of phishing, *Computer Fraud and Security,*
Vol 2005(7) pp. 6 – 11

Herzberg, A. (2005) Defending users of unprotected login pages with TrustBar 0.4.9.93.
Retrieved September 2007 from http://osdir.com/

Herzberg, A. & Gbara, A. (2007) TrustBar: Protecting (even naïve) Web users from spoofing and phishing attacks. Retrieved June 2007, from http://www.cs.biu.ac.il

Heylighen, F. & Joslyn, C. (1992) Systems Theory.
Retrieved November 2007, from
http://pespmc1.vub.ac.be/SYSTHEOR.html

IATF (2002) Defense in Depth – Release 3.1 September 2002.
Retrieved August 2007, from http://www.iatf.net

Jøsang, A. & Pope, S (2005) User Centric Identity Management, *Australian Computer Emergency Response Team Asia Pacific Information Technology Security Conference,* Royal Pines Resort – Gold Coast, Australia 22nd-26th May, 2005

Kormann, D.P. & Rubin, A.D (2000) Risks of the Passport single signon protocol
Computer Networks, Vol 33(1-6), pp. 51-58

Lewis, J. (2003) "Enterprise Identity Management: It's About the Business,"
vol.1, 2 July 2003, Burton Group Directory and Security Strategies
Directory and Security Strategies Research Overview
Retrieved November 2007, from www.burtongroup.com

Liberty Alliance (n.d.) History.
Retrieved July 2007, from
http://www.projectliberty.org/liberty/about/history

Liberty Alliance (2007) Contractual framework outline for circles of trust.
Retrieved July 2007, from http://www.projectliberty.org

Locke, M. & McCarthy, M.(2002) Realising the business benefits of Identity Management.
Retrieved July 2007 from http://uk.fujitsu.com/web/global/whitepapers/identity_management.pdf

Lopez, J., Oppliger, R. & Pernul, G. (2004) Authentication and authorisation infrastructures (AAIs): a comparative survey, *Computers & Security*, Vol 23(7) pp 578 - 590

Lukawiecki, R. (2006) *Identity lifecycle management.*
Retrieved June 2007, from https://msdb.ru/Downloads/TechNet/IdentityLifecycleManagement.ppt

Madsen, P. (2004) Federated identity and web services. *Information Security Technical Report,* Vol 9(3), pp.56-65

McCormick, J. (2003) *More .NET Passport security doubts raised.*
Retrieved June 2007, from http://articles.techrepublic.com.com/5100-1035_11-5054996.html

McWilliams, B. (2001) *Stealing MS Passport's wallet.*
Retrieved May 2007, from http://www.wired.com/science/discoveries/news/2001/11/48105

Microsoft (2004a) *Identity life-cycle management.*
Retrieved 25 June 2007, from http://www.microsoft.com

Microsoft (2004b) *Onyx – waste management group improves productivity with identity information solution.*
Retrieved 5 July 2007 from http://www.microsoft.com

Microsoft (2004c) *.NET Passport Review Guide.*
Retrieved August 2007, from http://www.microsoft.com

Microsoft (2005) *Authentication vs. Authorisation.*
Retrieved 27 May 2007, from http://www.microsoft.com

National Electronic Commerce Coordinating Council (NECCC) (2002) *Identity Management: A White Paper.* NECCC Annual Conference, New York, December 4-6, 2002.

Ollman, G. (2004) The Phishing guide: Understanding & preventing phishing attacks.
Retrieved 2 June 2007, from http://www.ngssoftware.com/research/papers/.

Olsen, T. & Mahler, T. (2007) Risk, responsibility and compliance in 'Circles of Trust' – Part I. *Computer Law & Security Report*, Vol 23(5), pp. 342 - 351

Open Web Application Security Project (2002) A Guide to building secure web applications. Retrieved August 2007, from http://www.cgisecurity.com/owasp/html/index.html

Oxford English Dictionary – *Trust* (1989).
Retrieved May 2007, from http://www.oed.com

Oxford English Dictionary – *Phishing* (2006).
Retrieved May 2007, from http://www.oed.com

Pfitzmann, B. (2004) Privacy in enterprise identity federation – policies for Liberty 2 single sign on *Information Security Technical Report*, Vol 9(1), pp. 45 – 58

Phishing increases as users get wise. (2007). *Network Security*, Vol 2007(1) pp. 2

Rodger, A. (2004) Access Management the key to compliance. *Card Technology Today*, Vol 16(4), pp. 11-12

Sarbanes Oxley (2007) *Open initiative to help organisations govern identity information across enterprise applications.*
Retrieved 27 June 2007, from http://www.s-ox.com/News/detail.cfm?articleID=2233

SearchVOIP (2006). *Identity management*
Retrieved 6 May 2007, from http://searchvoip.techtarget.com

South African Revenue Services (2006). *eFiling for individuals goes live*
Retrieved August 2007, from http://www.sars.gov.za

Standard Bank (n.d) *Internet banking security.*
Retrieved May 2007, from http://www.standardbank.co.za

Sullivan, B (2004) *MSNBC – Online fraud costs $2.6Billion.*
Retrieved May 2007, from http://www.msnbc.msn.com

Sun Microsystems (n.d) *Identity management services framework.*
Retrieved July 2007, from http://www.sun.com/service/identity/

Tavares, C. (2004) What is Discretionary Access control?
Retrieved July 2007, from
http://www.pluralsight.com/wiki/default.aspx/Keith.GuideBook/WhatIsDiscretionaryAccessControl.html

Vanamali S. (2004) Identity management framework: Delivering Value for Business, *Information Systems Control Journal*,Volume 4, 2004

Wikipedia (2007) *Online Identity.*
Retrieved May 2007, from http://en.wikipedia.org/wiki/Online_identity

Young, D. (2004) Human resources have a vital role to play within employee identity management. *Network Security*, Vol 2004(11),pp 5-7

Young, T. (2006) *Computing Magazine : Online fraud losses increase 55 percent.* Retrieved May 2007, from http://www.computing.co.uk

Appendix A

A USER CENTRIC MODEL FOR ONLINE IDENTITY AND ACCESS MANAGEMENT

M. Deas & S. Flowerday

Nelson Mandela Metropolitan University

University of Fort Hare

ABSTRACT

The problem today is that users are expected to remember multiple user names and passwords for different domains when accessing the Internet. Identity management solutions seek to solve this problem through creating a digital identity that is exchangeable across organisational boundaries. This is done through the setup of collaboration agreements between multiple domains, thus users can easily switch across domains without being required to repeatedly sign-on. However, this technology is accompanied by the threat of user identity and personal information being 'stolen'. Criminals make use of fake or 'spoofed' websites and social engineering techniques to gain illegal access to this information on the user. This has been catapulted to the fore by the statement that phishing has increased by 8000% over the period of January 2005 to September 2006 (APACS, 2007). Due to this, the need for users to be protected from online threats has drastically increased. This paper examines two processes in order to protect the user login information. Firstly, user's information must be protected at the time of sign-on, and secondly, a simple method for the identification of the website is required by the user. This paper looks at these processes of identifying and verifying user information followed by how the user can verify the website at sign-on. The roles of identity and access management are defined within the context of single sign-on. Three different models for identity management are analysed, namely the Microsoft .NET Passport, Liberty Alliance Federated Identity for Single Sign-on and the Mozilla TrustBar for website authentication. A new model for the definitive protection of the user in the online environment is proposed based on the evaluation of these three existing models.

KEY WORDS

Identity Management, Authentication Management, Mozilla TrustBar, Liberty Alliance, .NET Passport

A USER CENTRIC MODEL FOR ONLINE IDENTITY AND ACCESS MANAGEMENT

1 INTRODUCTION

The Internet has played a major role in the way people do business and interact socially. Websites are used to sell goods and provide services online whilst storing sensitive customer information such as credit card details and identity numbers. This information is stored using simplistic user sign-on tools. The use of this technology creates the challenge of how to ensure that the correct user is connecting to the correct system online.

To ensure users are who they claim to be at the time of sign-on an authentication tool, other than that of single key authentication password, is required. The use of dual key authentication, over that of single key passwords, produces higher levels of trust between the user and website provider. A number of users are still naïve as to the dangers of the Internet and are connecting to websites with simple security measures for client authentication. The authentication process may occur on fraudulently set up spoofed websites. This exposes the user to the risk of potential identity theft. Although organisations have been set up to standardise the processes of online identity management, the risk exists that a user's account information can be illegally accessed. It is therefore important that adequate identity management controls are put into place to secure the online user.

The remainder of this paper is organized as follows: Section 2 presents the role of identity management for businesses as a tool to meet legal requirements for client protection and the benefits of identity management to the business. Section 3 investigates the role of access and authentication management, focusing on user issues and trends relating to online systems usage. Section 4 provides an overview of the identity management solutions implemented by Microsoft Passport .NET, Liberty Alliance Federated User Identity and the Mozilla TrustBar. Section 5 provides a critical comparison of the models. The discovery is made that none of the investigated models focus on the issues of the user and the protection of the user within the online environment. Each model focuses exclusively on the sign-on or website identification processes and lacks a wholesome environment for the user to interact within. Section 6 attempts to create a model for user centric online protection. This model is based on the use of dual authentication techniques in the form of user authentication by the system, and system authentication by the user.

2 ROLE OF IDENTITY MANAGEMENT

Through the use of identity management, businesses benefit as they draw from best practices and ensure compliance to regulations. Legal requirements for client protection are implemented to provide a code of "best practice" as noted in COBIT and ITIL (Lewis, 2003). The company is ultimately responsible for the use of identity information and is held accountable should that information be used fraudulently. In making use of the identity management life-cycle the user's account is managed from the time of creation, to the time of the user permanently leaves the system. This process includes the removal and addition of

system rights (De Leeuw, 2004). Through efficient use of an identity management solution companies realise the following benefits:

1. Better planning, implementation and management of solutions through a complete user based life-cycle of services.
2. Reduction in costs and complexity, while increasing the rate of return on investment made in Identity management.
3. Predictable implementation procedures and efficient business operations, thereby ensuring greater system satisfaction for both users and customers.
4. Manages all four main areas of concern for the business (people, process, practice and platform), when implementing identity management in the organisation (Sun Microsystems, n.d.) (Gordon, 2004)

Organisations now view identity management solutions as the answer to a number of security challenges. It is also imperative for organisations to consider how they can take full advantage of the benefits and the value of an identity management system within their business (BMC Software, 2006). Furthermore, the use of effective identity management controls will provide the system user with a secure environment within which they can function. The effectiveness of such a process, however, is only as strong as the level to which access and authentication management controls are applied.

3 ACCESS AND AUTHENTICATION MANAGEMENT

To manage a business environment in which multiple users require access to systems over large and distributed networks, it is essential that the business ensures the users connecting to this environment are whom they claim to be. The Internet has the ability to mask an identity, and this process can be used to perpetrate fraud. Due to this ability, every action performed online is subject to a degree of risk. This lack of trust has spread into the banking sector. In a recent report by the journal, Computer Fraud and Security it was stated that 52% of respondents were unlikely to sign up to online banking facilities and that 82% of respondents would not respond to any emails from financial firms (Consumers losing trust in online banking: survey, 2007).

In online commerce customers take on substantial levels of risk when making purchases from an online vendor. This is because all encounters take place through the vendor website. This has created the need for customers to be able to assess the risk when purchasing online.

Customers often leave a website when they do not gain a sufficient sense of trust (Chau, Hu, Lee & Au, 2006). Due to online merchants storing large amounts of customer data it is critical for vendors to build strong trusting relationships with their customers. This can be ensured by making use of proper access control procedures to provide minimal risk to the customer. From the perspective of the merchant, there is little concern over the identity of the individual customer, but more concern over their ability to pay for services or goods. If security is breached on the vendor website, it is imperative that accurate logs exist for the auditing of user actions.

The dangers to users in the online environment are summarised as spoofing, phishing and identity theft. By implementing strong controls to ensure that an authorised user is accessing the system, the business risk is diminished (Rodger, 2004). In order to identify the best methods to protect an online identity from online threats, it is essential to look at international systems for single sign-on (SSO) protection of the user.

4 COMPARISON OF IDENTITY MANAGEMENT SOLUTIONS

The ideal environment for the computer scientist is one in which computer systems know who their users are. The ideology behind this is based on the concept that users should be authenticated as simply as possible. An investigation is performed in order to determine the approaches to implement this idea, specifically looking at Microsoft's Passport .NET, Liberty Alliance and Mozilla TrustBar.

4.1 Microsoft Passport .NET

The Passport .NET service makes use of a SSO Identity Domain. Microsoft is suited for the process of handling an SSO platform as it already provides a large variety of services online for e-mail, online messaging and search facilities. Issues regarding user privacy and freedom of movement online could be infringed should a single entity take control of all SSO authentications and the information held therein. The process followed for user authentication through the Passport service is shown in Figure 1.

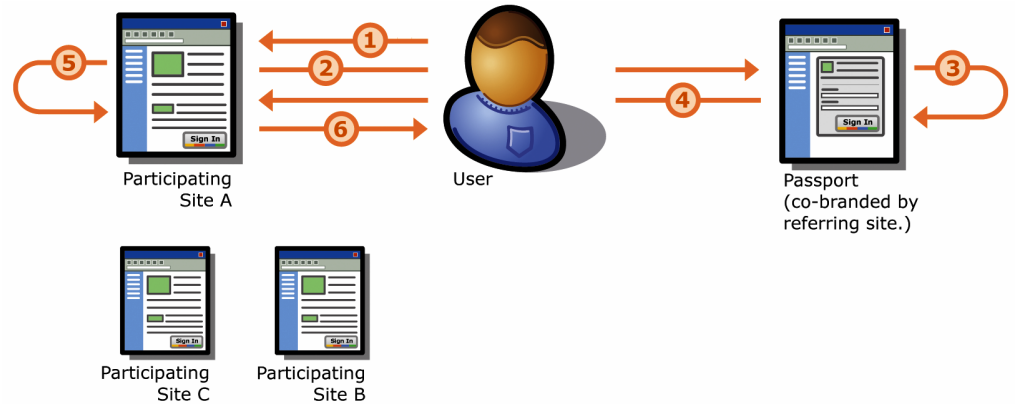

Figure 1 – The Passport Authentication Process (Microsoft, 2004)

1. User browses to participating site or service (Site A in this example) and clicks "Sign In" button or link
2. User is redirected to Passport
3. Passport checks if the user has a "Ticket Granting Cookie" (TGC) in their browser's cookie file meeting the rules of Site A. If one is detected, they skip to step 4 and do not go through the login process. If the TGC has lapsed based on Site A's time requirements, then the user is redirected to a page asking for their login credentials to be entered correctly in order to proceed

4. The user is redirected back to Site A with their encrypted authentication ticket and profile information attached.
5. Site A decrypts the authentication ticket and profile information and signs the customer into the website.
6. The user accesses the page, resource or service they requested from Site A.

NOTE: No information about a user is shared with Sites B and C unless the user chooses to sign-on to those sites.

A potentially hazardous feature to the user of .NET Passport reported by both Microsoft (2004) and discussed by Kormann and Rubin (2000) is that of the automatic sign-on to Passport. If this option is selected the username and password of the individual user are stored locally on the individual client's machine. When an automatic sign-on is selected the user will be signed on to the .NET Passport service without intervention. Disconnecting from the Internet or turning the machine off has no effect on the connection of the user to the service. This option creates the possibility for a user's account to be infiltrated potentially exposing sensitive information.

Although a user may use their .NET Passport account at multiple sites, the password is only stored in the .NET Passport database and is only shared with the .NET Passport servers that need to make use of it for authentication. The .NET Passport service contains a feature in which should the user in making an error in attempting to sign-on, the system automatically blocks access to the user account for a few minutes. This process stops attempts using password cracking software to gain unlawful access to the account.

Overall the .NET Passport solution provides a relatively simple solution to the problems experienced by users within SSO. Websites affiliated with the .NET Passport program can opt to have the service manage their user base, shifting the responsibility for this process from the individual website on to Microsoft. As stated previously the main drawback to the .NET Passport solution is the problem of having a single entity responsible for all identity authentication tasks, as it can be exposed to security and privacy issues.

4.2 Liberty Alliance Federated User Identity

The Liberty Alliance is an undertaking by a group of organisations and government agencies to provide a set of open technical specifications for the creation of a federated identity solution. When the Liberty Alliance began their operations the first phase of development involved the setting up of specifications which enabled simplified SSO for end users. This process became Liberty's Identity Federation Framework (Madsen, 2004).

The Liberty specifications for SSO are an enabler which provides SSO functionality across different enterprise domains and websites.

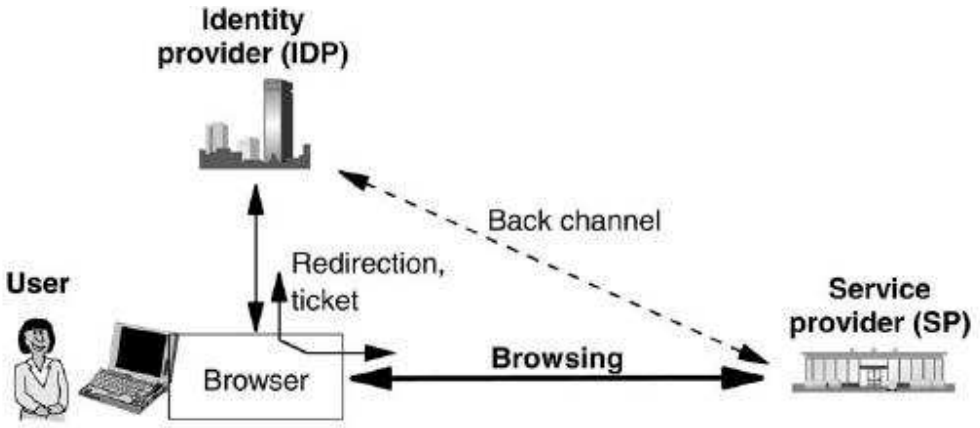

Figure 2 – Browser based SSO (Pfitzmann, 2004)

Pfitzmann (2004) describes the process of Liberty's SSO as follows:

A user is accessing the service provider whilst browsing online. When submitting a sign-on request, the service provider redirects the browser to the user's identity provider. The user then log's in, through the use of a typical username and password. The identity provider redirects the browser back to the service provider with an additional ticket, to handle other services, such as data transfer logistics on other channels

The benefit of using this form of implementation is that the user does not have to be redirected to a separate login page for authentication purposes. Once the user is authenticated by one service within the "circle of trust" all other websites within that trust domain can verify the user as having been authenticated, eliminating the need for multiple SSO (Liberty Alliance, 2007).

The Liberty Alliance provides a viable alternative to the solution from the .NET Passport. By having a consortium of companies involved in the setting of standards, a broader level of consensus is achieved and the best solution implemented. Within the realm of SSO the problem with Liberty Alliance's solution is the lack of ability to provide a scalable solution for a user to connect to a multitude of websites. This is due to each setup of the federated identity solution existing within separate circles of trust. If a user moves between two different trust circles, they will be required to sign-on with different credentials.

4.3 Mozilla TrustBar

A potential solution for a user to identify the websites they are connecting to is the use of a plug-in toolbar supplied within Mozilla Firefox browsers. Through the use of this plug-in a user can store images mapped to server certificates. Whenever a server certificate is verified, the mapped image is displayed on the toolbar, while the corresponding page is still being loaded (Jøsang & Pope, 2005). Mozilla TrustBar focuses on how to secure the user in the authentication of websites. Through the use of this, the user is protected from the threats

of phishing and website spoofing. The TrustBar attempts to make users more aware of the security behind the web pages they view.

The overall process of the client user authentication on the server attempts to protect against potential eavesdropping and modification by Man in the Middle (MITM) adversaries. Large numbers of financial and other websites make use of Secure Socket Layer (SSL) to authenticate the user. A number of those sites however only make use of SSL protocols once the user has typed in a username and password and clicked 'submit' (Herzberg, 2005).

This form of implementation provides the potential for a MITM to redirect the user towards a modified version of the web page. Should this occur the user may unknowingly provide login information to a third party. Through the modified page, if the user attempts to login, the user information is sent back to the MITM. Clearly the traditional approach of signing on does not protect the user from these forms of attack, and the user requires an easier way to verify that he or she is on the intended website.

Herzberg (2005) mentions the ways in which TrustBar provides a solution to the client user problem as follows:

- TrustBar periodically downloads a list of the unprotected websites that are maintained on the Mozilla TrustBar servers. This list stores the unprotected login sites which Mozilla tracks, as well as any alternate login pages for those websites that are protected. This information can be used to redirect the client if an unsafe link is found.
- TrustBar makes allowance for users to assign a logo to websites of their own choosing to visually identify the website. TrustBar tracks changes to websites and displays information in the form of a "Same since" and a date value. After the website changes a warning is displayed when the page is accessed.

Herzberg and Gbara (2007) provide further uses of TrustBar for solving the user problem in the following situations:

- In SSL websites, TrustBar shows, by default, the name of the organisation that owns the website through the identification of the digital certificate. TrustBar also displays a representation of the logo or the name of the certification authority which issued the certificate.
- TrustBar displays a padlock for all protected websites, and a "No Entry" signs for unprotected websites.

The Mozilla TrustBar's solution to the user's web usage condition is novel. The service provides the client with a free-to-use facility that can make the user feel more secure online. By providing a visual aid to the user showing the current status of the website being accessed, the users overall experience is improved.

5 COMPARISON OF MODELS

The three models reviewed have different approaches to the handling of identity management. It is not possible to provide a valid comparison of the .NET Passport system,

which was implemented with a singular methodology, to the Liberty Alliance framework. The reason for this is that the latter is not a system, but a set of open technical standards which an organisation can implement. The efficiency of a Liberty Alliance framework implementation is only as strong as the level to which the specifications are applied. Further complicating this analysis is the Mozilla TrustBar. The TrustBar looks at the identity management paradigm from that of the user. TrustBar implements similar steps when performing authentication, but instead of the authentication of the user, the website being accessed is authenticated. The consolidated comparisons, where they can be drawn are shown in Table 1.

	.NET Passport (Lopez, Oppliger & Pernul, 2004)	**Liberty Alliance** (Olsen & Mahler, 2007)	**Mozilla TrustBar** (Herzberg, 2005)
System	Singular System implemented by Microsoft	Open Specifications. Can be implemented in various ways within multiple different systems	Single System implemented by Mozilla to handle classification of web addresses
SSO	Previously multi-organisation SSO. Since 2003 single-organisation sign-on	Depends on implementation, supports multi-organisation SSO	Single verification of websites accessed by user
Choice of Identity Providers	Microsoft was the only identity provider	Allows for several identity providers so far as they are accepted by the service provider	Mozilla serves as identity provider for authentication of websites
Identifiers	Personal Unique Identifier per user	Unique handle per user per federated pair of website	Unique identifiers per participating website
Responsible controller	Microsoft and service providers are single data controllers	Controllers or processors? -Service providers within a circle of trust become data controllers "at the time users visit their websites" -However according to the Liberty Alliance, it is possible that some service providers may act as processors	Mozilla and service providers as single data controllers
Contractual Framework	Contract between Microsoft and service provider	Implementation dependant -Contract between every website in a circle of trust -Depending on the type of implementation other models may be possible, such as every participating service provider has a contract with one party which organises and administrates the circle of trust	No contract required, makes use of open source community

Table 1 – Comparison of .NET Passport, Liberty Alliance and Mozilla TrustBar

Table 1 attempts to compartmentalise the three models into specific sections for comparison. The .NET Passport is rooted as a singular entity, which is maintained by Microsoft. All usage of the .NET Passport requires adherence to Microsoft standards by website vendors, stipulated in contracts between Microsoft and these parties. The Liberty

Alliance makes use of a set of open specifications that can be implemented in various ways to allow for an SSO environment to be created for users. The SSO facility, however, only applies between websites within the same circle of trust, and should a user move out of the circle they must resubmit their login credentials. TrustBar takes a different perspective looking at the issue from the user point of view. TrustBar currently works off a single system, which is implemented by Mozilla, handling the classification and analysing the security of the websites, to create a central repository for determining website validity.

The three models analysed provide a significant step towards meeting the overall goal of an integrated system for the protection of the user in the online environment. To place each model into a specific category for the issues they address the models can be summarised as follows:

- Microsoft .NET Passport – provides a solution for broad implementation of identification and verification of users within an SSO environment. It also provides simple integration between vendors, due to a single user identification provider.
- Liberty Alliance – provides a flexible solution for the website vendor through the use of circles of trust. This is limited to providing SSO on a smaller scale because of the limited sizes of the circle of trust. Each website within the circle of trust provides its own login forms for the user. With a greater level of trust between the websites involved, the ability to audit user movements within the system is increased.
- Mozilla TrustBar – provides a way to identify the website from the user perspective. Through the implementation of an easy to use identification and verification process, the user is alerted to potential threats within the website they are seeking to access.

6 USER CENTRIC ONLINE IDENTITY & AUTHENTICATION MANAGEMENT MODEL

Although all three models discussed do provide a useful service, none cover all the needs of the user. This is due to each model focusing on the sign-on or website identification issues. None focus on the issues of the user and protection of the user within the online environment. The issues that need to be addressed for the protection of users in the online environment can be summarised as follows:

- Scam Protection – Users must be aware of potential scams online. Education is the best prevention of these incidences (Bradley, 2007).
- Spoofing – Users must be aware of fraudulent sites and the risks that can occur should their information be compromised (Herzberg, 2005).
- Multiple Verification – When making use of multiple websites, each with individual login criteria, a facility to improve the user experience through the use of SSO methodology is required. SSO reduces the potential for interception

of client login data, and promotes ease of use online (Lopez, Oppliger & Pernul, 2007).

- Credential Security – User credentials must be securely transmitted when authenticating SSO environments.

Each of the models possesses attributes that address some of these user requirements but they themselves are insufficient.

6.1 Authentication of IT Systems and Users

Authentication procedures in the online world are more complex than there real world counterparts. Through the use of brute force attacks, security controls can be compromised in a short period of time. The use of social engineering techniques can make the process even simpler. When performing the process of converting an offline system to an online version, technical authentication procedures are adapted to the online capabilities, frequently without adopting the security measures (FIDIS, 2006). The authentication of the actual website may be adequate, but if users are unable to establish the trustworthiness of the website they are lured to, this authentication is in vain. If more controls and checks are enforced along with dual authentication by users and systems, a more secure environment for the online user will be insured.

6.1.1 Authentication of users by IT Systems

From a technical viewpoint, an identity is nothing more than a digital pseudonym representing an individual. Because of this, measures are required to prove the digital pseudonym belongs to the person whom claims to possess it (FIDIS, 2006).

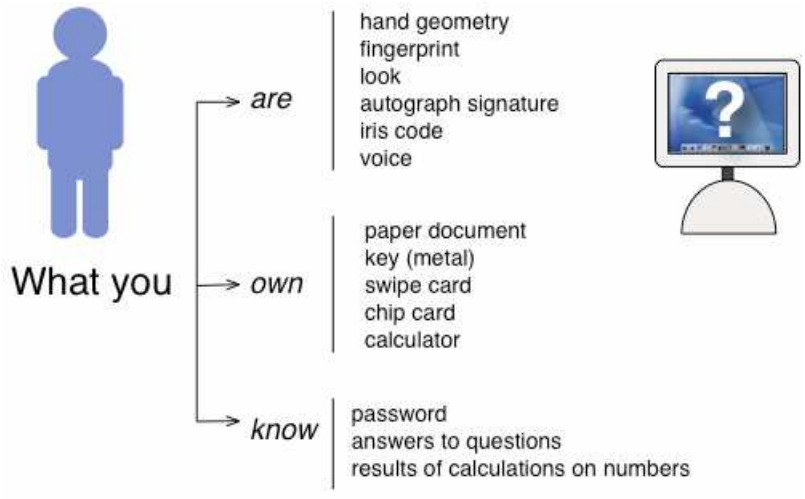

Figure 3 - Authentication by an IT System (FIDIS, 2006)

Figure 3 depicts the ways in which an IT system can determine the authenticity of a user. An increase in the number of criteria provides for a more comprehensive verification of the user to be enforced. Based on these, IT systems can recognize a user by what he is

through the use of biometric techniques, what they possess, and what they know. The higher the number of controls that can be implemented using these identification criteria, the higher the level of certainty will be that the user accessing the system is authorised to do so. Consequently the more criteria used for the authentication process, the higher the levels of trust created between the user and the system.

6.1.2 Authentication of an IT System by a person

User identity theft is performed through deceiving the user on a spoofed website. A user enters their login information and attempts to connect, thereby sending their identity data to the perpetrator. To curb this problem, users should authenticate an IT system using the criteria described by the Future of Identity in the Information Society (FIDIS, 2006) are:

- What the IT system is – By looking at the information contained on the website the user can determine its validity. The immediate method of identifying a website is through the assessment of the website URL. If the URL corresponds to that of the users expected website, they should continue by determining the validity of the website's digital certificates. In checking the digital certificates the user can determine the validity of the website. This process can be automated through the use of a system such as the Mozilla TrustBar.
- What the IT system knows – Through the registration process the user will setup their initial profile. Some websites may request other personal information relating to the client. In seeing this information the user is ensured they are on the correct website.

Through the use of both user and system authentication in a dual pronged approach a user can ensure they are making use of a valid Internet website.

6.2 A model for securing the user's online experience

In order to protect the use from the threats to their online identity, an approach is required that satisfies both user authentication and website authentication. In Figure 4, a model is proposed which promotes a two-pronged solution to the protection of user information in the online environment. The model addresses user protection from two angles. The validity of the website is checked and reported to the user. This is performed to ensure that the user is attempting to access and authenticate the correct version of the website. After this, the process of SSO authentication takes place to allow the user to make use of the benefits of the SSO environment.

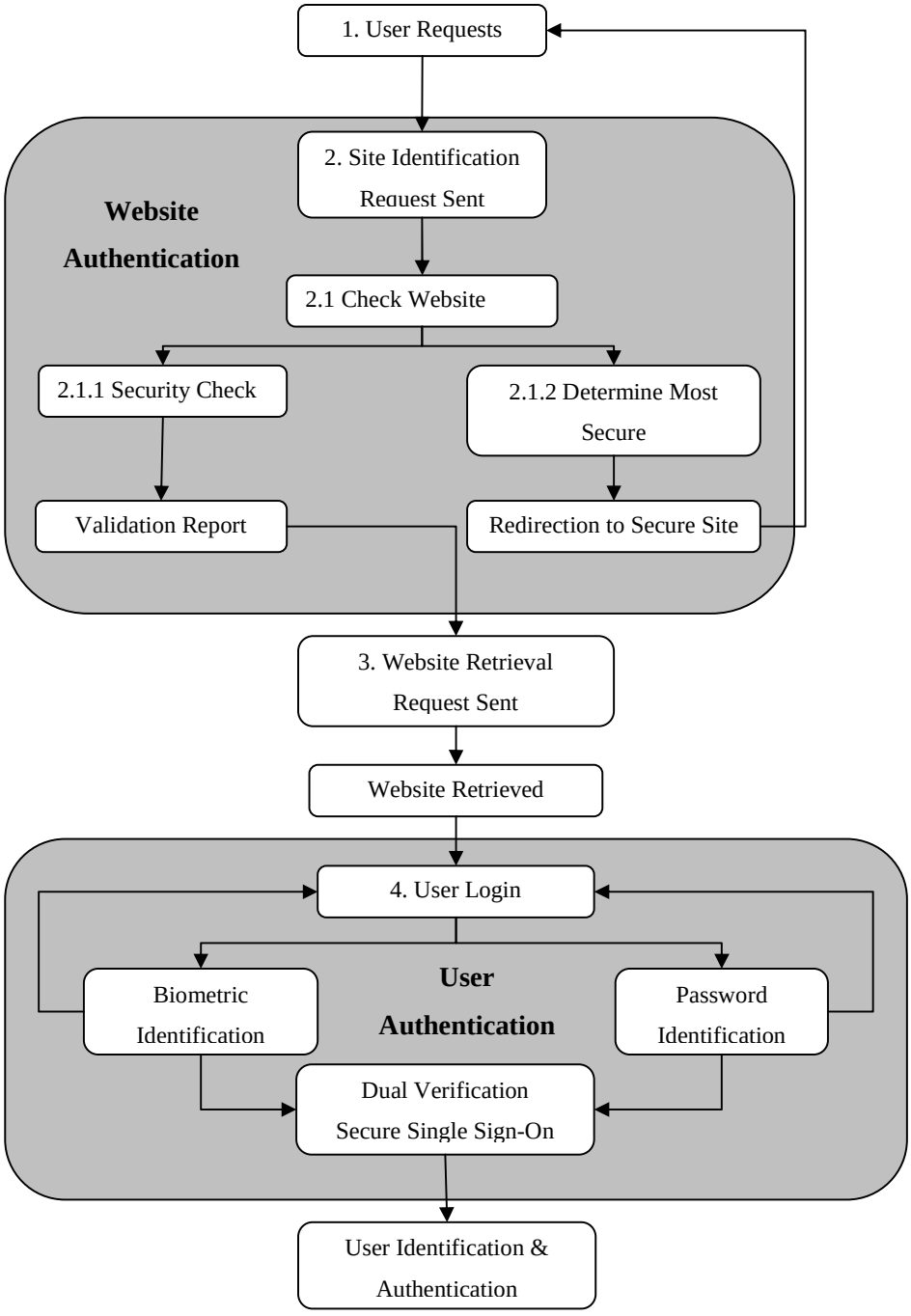

Figure 4 – Model for User Centric Online Protection

The process followed in the model is expanded as follows:

1. User Requests Website – The user makes use of their browser and enters the URL of the website they intend to visit. From selection of this website the process moves into the process responsible for the authentication of the website.

2. Site Identification Request – When the user performs a request for the website, a request is sent to a repository responsible for the validation of websites. The information in this repository provides information to the user in order for them to validate the security of the website.

2.1 Check Website URL – Using the information stored in the repository checks are undertaken in order to determine the security built in the requested website.

2.1.1 Determine Most Secure Site – A number of websites potentially have web pages, which are often more secure but are not set as the default login page. In these cases the repository determines the most secure website. If a more secure inner link for the same domain is found, the repository sends a redirect response to the browser to redirect t the more secure website. Should this occur, then the process from Step 1 occurs.

2.1.2 Site Security Check – Based on the URL the repository performs a search determining the validity of the digital certificates, authority of the certificate issuers, and if the site is flagged by the repository as a spoofed website. The result of this is a URL validation report, which is then sent back to the user's browser to display the results and allow the user the opportunity to validate the website themselves.

3. Website Retrieval Request Sent – When a user's request for a website is sent, the website is retrieved via HTTP protocols.

4. User Login – Once the page has been loaded with information required for the validation report, the user attempts to login to the SSO website. Incorporated within this process is the use of a biometric input, in the form of user fingerprint identification, along with password identification, which is used to provide a more secure environment. If either of these validation procedures fails, the user is redirected to the initial login page. If the sign-on is successful, then the user is verified and authenticated within the SSO environment. This process ultimately leads to secure user identification.

7 CONCLUSION

This paper has discussed the need for a comprehensive model for the protection of users within the online environment. The roles of identity management and the benefits to the business were discussed to define the benefits of identity management solutions to businesses. The role of access and authentication management provided an insight into online user habits with regards to security. The three models of .NET Passport, Liberty Alliance Federated Identity and Mozilla TrustBar were examined to determine the processes followed by industry leading identity management solutions. A critical comparison of these models was made which found that none cover all the needs of the user to create a comprehensive environment for the protection of the user. A model was then proposed based

on the best practices of the industry to promote the use of dual levels of authentication. This involves the user website authentication, and website identification by the user to create a secure environment. In using a username and password along with other identification methods, the accuracy of user identification is increased. In addition to this, the ability for the user to identify the website and verify its authenticity protects the user from the threats of spoofing. This will protect the user from identity theft. An alternative benefit of this process is higher levels of trust produced between the users and the vendors.

8 REFERENCES

APACS (2007) New research reveals that people are still unaware of basic security measures when banking online. Retrieved December 2007 from http://www.apacs.org.uk

BMC Software (2006) Supporting the identity management lifecycle with BMC Identity Management, Suite 5.5, Technical White Paper. Retrieved July 2007 from http://www.bmc.com

Bradley, T. (2007) Gone Phishing. Retrieved October 2007, from http:/netsecurity.about.com/od/secureyouremail/a/aa061404.htm

Chau, P.Y.K. Hu, P.J. Lee, B.L.P. & Au, A.K.K. (2007) Examining customer's trust in online vendors and their dropout decisions: An empirical study. Electronic Commerce Research and Applications, Vol 6(2), pp 171 – 182

Consumers losing trust in online banking: survey (2007). Computer Fraud & Security, Vol 2007(2) pp 4

De Leeuw, E. (2004) Risks and threats attached to the application of Biometric technology in National identity management. Retrieved May 2007, from http://secure.gvib.nl/afy_info_ID_1322.htm-ThesisMSIT.zip

Gordon, T. (2004) Quantifiable benefits of implementing identity management systems Retrieved July 2007, from http://www.isd.salford.ac.uk

Herzberg, A. (2005) Defending users of unprotected login pages with TrustBar 0.4.9.93. Retrieved September 2007 from http://osdir.com/

Herzberg, A. & Gbara, A. (2007) TrustBar: Protecting (even naïve) Web users from spoofing and phishing attacks. Retrieved June 2007, from http://www.cs.biu.ac.il

Jøsang, A. & Pope, S (2005) User Centric Identity Management, Australian Computer Emergency Response Team Asia Pacific Information Technology Security Conference, Royal Pines Resort – Gold Coast, Australia 22nd-26th May, 2005

Kormann, D.P. & Rubin, A.D (2000) Risks of the Passport single signon protocol Computer Networks, Vol 33(1-6) pp 51-58

Lewis, J. (2003) "Enterprise Identity Management: It's About the Business," *vol.1, 2 July 2003, Burton Group Directory and Security Strategies Directory and Security Strategies Research Overview* Retrieved November 2007, from www.burtongroup.com

Liberty Alliance (2007) Contractual framework outline for circles of trust. Retrieved July 2007, from http://www.projectliberty.org
Lopez, J., Oppliger, R. & Pernul, G. (2004) Authentication and authorisation infrastructures (AAIs): a comparative survey, Computers & Security, Vol 23(7) pp 578 – 590

Madsen, P. (2004) Federated identity and web services. Information Security Technical Report, Vol 9(3), pp.56-65

Microsoft (2004) .NET Passport Review Guide (2004) Retrieved August 2007, from http://www.microsoft.com

Olsen, T. & Mahler, T. (2007) Risk, responsibility and compliance in 'Circles of Trust' – Part I Computer Law & Security Report, Vol 23(5), pp. 342 – 351

Pfitzmann, B. (2004) Privacy in enterprise identity federation – policies for Liberty 2 single sign on Information Security Technical Report, Vol 9(1), pp. 45 – 58

Rodger, A. (2004) Access Management the key to compliance. *Card Technology Today*, Vol 16(4), pp. 11-12

Sun Microsystems (n.d) Identity management services framework. Retrieved July 2007, from http://www.sun.com/service/identity/