Global Information Assurance Certification Paper

Louis Tapper
May 2004
GIAC Security Essentials Certification (GSEC) version 1.4b option1

BARRIERS TO IMPLEMENTING IDENTITY MANAGEMENT

Abstract

How does and organisation accurately identify who is accessing their data and what is being accessed? How can manage this process be managed within an organisation or between organisations? These questions, illustrate fundamental concerns in an increasingly interconnected and complex digital world. Much has been written about the benefits of Identity Management, but in many cases organisations have failed to implement it. This paper is an introduction to Identity Management and how its implementation depends on understanding and overcoming a number of barriers. Recommendations on how to overcome some of the barriers to implementing Identity Management will also be presented. Identifying the business drivers, obtaining management buy in and identifying pain points are keys to the successful implementation of Identity Management.

Introduction

So you have just been audited and are now told your organisation needs Identity Management (IM), to make it more secure more efficient, save money or comply with regulations. What then is digital identity, IM and why the fuss? IM is the term used by the IT industry to describe a collection of issues surrounding managing digital identities. The purpose of digital identity is to restore the ease of human transactions that took place back when transactions were done face to face. In a machine environment, transactions are often being made for the first time with people we have never met and in different locations.
An on going question facing organisations is who gets access to data, for how long and for what purpose. Increasingly, there are multiple ways to store and access data, which in turn has increased the complexity of managing access to that data. Accurately identifying staff, customers, partners and suppliers is critical to growth of organisations and commerce, on the Internet.
IM addresses each stage of the identity lifecycle, account set-up, account maintenance and account removal. In practice some of the questions IM addresses are how you authorize or permit access to data that is spread across multiple applications or databases? How then, do you authenticate and control access? How do you provision access so that employees, customers and partners can be added and deleted easily?
One fundamental problem is identity information has traditionally been stored in isolated and independent directories that do not interact or trust each other. For example, a typical organisation might have a Human Resources database, Remote Access database, Active Directory and Customer Relations Management database. Each database requires separate maintenance and different methods to describe the identities they contain. As a result, management of user accounts becomes unwieldy and users are burdened with remembering multiple passwords. Considerable time and money is therefore being spent setting up, maintaining and removing accounts through the lifecycle of maintaining a digital identity.

There is currently no single piece of technology that solves all the problems in a truly scalable way for the Internet. A number of vendors provide products that manage various parts of the IM puzzle [1]. This is a piecemeal approach and has led to pain and increased cost to integrate existing applications. There is an increasingly trend for vendors to provide suites of products which provide most of what is required to integrate IM internally into an organisation [1].
New standards are being developed to resolve the issues of scalability and interoperability, faced by organisations that want to integrate IM outside of their organisational boundaries. One of the biggest problems to overcome is the lack of standardised security architecture that enables trust relationships among organisations in a standardised and automated way. Federated Identity (FI) the current industry buzzword that addresses these concerns and can be thought of as an extension to IM and the pinnacle of what is trying to be achieved. FI will be discussed later in the paper.

Components of an IM solution

It is beyond the scope of this paper to provide an in depth description of the components of IM as other authors have already described this in more detail [2,]. The following summary will be provided to aid discussion of barriers latter in this paper.
One of the easiest ways to conceptualise IM is to think of the components required in relation to managing the lifecycle of a digital identity [3]. These include account set-up, account maintenance and account teardown. Account set-up typically provides appropriate access to resources based on their role. Account maintenance involves managing account permissions and details while active. Account teardown involves revoking the account when it is no longer needed. For consistencies sake the following components will be used as the standard for discussing various components of IM [4].

Provisioning
Provisioning tools deal with giving people access to resources (provisioning) and then revoking that access once it is no longer needed (de-provisioning). Steps in provisioning accounts logically include requesting an account, validating user details, approving the request and creating the account. The goal is to reduce the time, effort and cost required to manage this process. Research indicates that many large companies take longer than 2 days to create and revoke access to all their systems and resources. There are some cases of companies taking years to realise that former employees continue to have remote access to their systems [3].
The way provisioning systems operate can be divided into either centrally managed or distributed agents. Distributed agents reside on each application server being managed. This makes them potentially more challenging to implement and maintain as well as being susceptible to operational problems with new software releases. Centrally managed agents reside on a provisioning server and are consequently simpler to manage and maintain. Communications with the application servers however can be limited to unidirectional communications. For instance passwords cannot be synchronised in both directions.

Access Management
Access management tools control who has access to what and provides authentication and authorization services. Authentication can range from a simple login based on usernames and passwords, to stronger authentication such as using tokens, public-key certificates and biometrics. The ultimate goal of providing simplified sign-on or reduced sign on is to ease the management burden. Role based access across an organisations systems can become possible with access management. For example, users are grouped into job functions (HR, Sales, and Support) and can be given appropriate privileges.

Identity Unification
Identity unification components allow various data stores to be combined into a central repository. Identity unification can be thought of as an overarching infrastructure other components such as provisioning, access management and FI tap into. Identity databases are increasingly being developed around LDAP databases, due to their flexible nature and ability to communicate over HTTP and SSL.

Federated Identity
FI refers to products and standards that extend an authentication context to external parties [6]. FI is the holy grail for IM, and allows separate organisations to share identity information. The challenge is to allow interoperability between organisations with differing infrastructures e.g. Public Key Infrastructure verses Kerberos authentication mechanisms.
The Liberty Alliance has been developing open standards based around SMAL to achieve FI. The SMAL standard allows individual applications to share login credentials for a given user. Liberty Alliance is also the way for non-Microsoft companies to counter the threat from Microsofts' propriety Passport platform, which was based around the WS-Security standards [6]. Passport has failed to gain true market acceptance for a number of reasons discussed later in this paper.
Both WS-Security and SMAL standards will play a part in determining how FI will be implemented now and in the future. These standards address the interoperability and scalability issues but do not however solve any of the other problems related to manageability of identity.

Business drivers for implementing Identity Management

You might say, “I am a security professional, what place do business drivers have in a presentation about security?” Security often has intangible benefits that are not easily measured or understood. To achieve security benefits from IM, business drivers must be understood to gain an organisations support. Gartner identified the following five basic business drivers for implementing IM [7].

1. *Business Facilitation*
Organisations are increasingly opening up internal data to customers’ partners and employees via the Internet. To manage access to this data, an identity infrastructure must be in place to facilitate data access. Ways in which business facilitation can occur are; allowing customer self registration, ability to personalise web portals, ability to outsource IT operations, facilitating customer retention by making it easy to do business with an organisation.

A good example of this is an IT service company who wants to allow customers to access any current call that they have open, via the web. Benefits to the customer are a better service by allowing customers to directly check the status of their calls without calling the helpdesk or engineer involved.
From a sales perspective, finding and retaining customers are core functions for most businesses. IM systems enable businesses to link sales and prospect analysis applications, market development analysis, affiliate marketing campaigns, direct sales campaigns, and sales force automation systems. Linking these systems allows business to increase revenue while reducing the cost of sales. Knowing that your customer and supplier lists will not be stolen is also central to staying in business.

2. *Cost Containment*
Reducing costs and providing return on investment is one of the leading business drivers for IM [8]. Management of accounts and permissions for helpdesk are becoming an increasing burden and cost for the helpdesk. Studies have shown that helpdesks can spend an average of 30% of their time managing accounts and passwords [4]. Direct savings can be achieved by reducing the number of staff required to manage access requests and password resets.
Costs associated with application development can be further reduced by providing a common interface for authenticating rather than having to make separate calls for each application. Non-IT services and resources (e.g. cell phones, pagers) can also be integrated and managed more cost effectively with provisioning products.

3. *Operational Efficiency*
Seamless integration of identity information allows a better flow of information, eliminating duplicated tasks and reducing the risk of error. It should enable staff to focus on core functions and service an increasing number of users. Minimizing the productivity time lag incurred when new employees join an organisation is often cited as an efficiency gain by implementing IM provisioning tools [3]. Providing seamless intranet and extranet access to applications is also touted as allowing operational efficiency gains.

4. *Regulatory compliance*
Many organisations are required to comply with regulations that are either generic or specific to an industry. For example in the United States, the Health Insurance Portability and Accountability Act (HIPPA), makes health organisations liable for the integrity and privacy of their data. Restrictions of health information only to those that need it are one of the mandates required by this act.

5. *IT risk management*
The future of web related commerce is based around assuring the public and business that transactions on the web are secure and can be trusted. The current trend is for access to data by more users from more devices and more locations. Eliminating or reducing the possibility of a major breach of security, due to insufficient user access controls is one of the major risk management objectives for most organisations.
The argument most often given from a risk management perspective is that users have to remember multiple passwords and end up choosing weak passwords or write them down. Minimising the accounts a user has to remember and performing

strength testing on the passwords can reduce the risk of a security breach. It must be pointed out that an identity if compromised will have a greater impact with single sign-on or reduced sign on products.
Access management and identity unification allows reuse of identity roles and access rights. As a result security can be applied more consistently across an organisation and revoked quickly if necessary.
Online authentication is viewed as having the greatest potential for reducing the risk of identity fraud. The ability to provide a clear audit trail of user logons and transactions is thus central to managing the risk. IM systems provide the foundation for authentication, integrity, non-repudiation and confidentiality of the data contained on a system. Authentication ensures that person is who they say they are. Integrity provides certainty that the data has not been modified in any way. Non-repudiation ensures that the person cannot later deny that a transaction took place. Confidentiality ensures only people authorised to view the data actually see it.
Figures published in the United States by the Federal Trade Commission indicate that 1 in 8 Americans are the victim of identity theft and that it is a growing problem [9]. Reluctance of companies to report identity theft has contributed to scarce publicly available figures on this issue. According to a report by Australian Office of Strategic Crime Assessments [10], the reluctance of companies to report the problems have been due to;

- Fear of adverse publicity
- Lack of awareness that there is actually a problem
- No confidence that reporting the problem will result in an appropriate punishment
- Preference to take corrective action and recover losses without criminal charges.

The report also highlights a general acceptance that a significant problem exists and warns that criminals are increasingly turning to electronic methods as source of traditional fraud. The same crimes that have always existed are now being exploited in new ways via electronic means such as the Internet. Customer surveys have contradicted the level of paranoia that some consumers have about identity theft and point out that people are four times more likely to fall victim to identity theft from loss of a wallet than through making an online transaction [11].

Barriers/ Risks

Given that IM and FIM have a long list of reported benefits, why has it not been more widely adopted in the marketplace [12, 3]? One of the fundamental issues is lack of support, understanding and executive mandates [3]. Many organisations struggle with the basics of how access rights should be assigned and provisioned [3]. Most of the identity management efforts to date have been focused on integrating the organisation internally.
With FI, many organisations do not have the fundamental infrastructure in place to effectively manage digital identity. Before organisations can take advantage of FI they must sort their own internal environment first.
In the consumer identity market Microsofts' failed attempt at implementing Passport offers some insight as to why single sign-on has not been achieved. The reasons hinge around politics, trust and demand. Although Microsoft has managed to sign up over 200 million customers to Passport, the actual real demand was much less than expected [13]. Only 2% of the customers signed up to avoid multiple logons. Most

(84%) were automatically signed up when registering Windows XP and Hotmail. Ultimately businesses have chosen to retain autonomy over their data and have shunned Microsofts' proprietary approach, which centralised identity information. Microsofts' much-criticised failings in security related issues and intense regulatory scrutiny have also prevented business buy in [13].
The failure of Microsofts' centrally managed proprietary approach to IM has lead to a surge in interest in federated models of identity that have been promoted by the Liberty Alliance. While consumer identity projects are languishing business-to-business identity projects are the most likely benefactors of identity management in the short term.

Legal issues
Legal issues regarding liability for transactions are a key inhibitor of identity management solutions [14]. Put simply, who is responsible if someone's digital identity is misused or stolen? Who is responsible for the cost if a digital identification system is compromised? For companies wanting to integrate internally, this does not pose a significant problem because the business is already trusted.
In the case of online purchases via credit card, the transaction is not made secure by any technology. It is the credit card companies taking liability for the transaction that truly protects consumers. Until liability issues across borders can be resolved, FIM will struggle to gain widespread acceptance [14].

Weaknesses in the underlying Internet infrastructure
Inherent weakness, underlying the Internet, is making the job of FI more difficult. How companies implement identity standards to mitigate the risks will play a large part in increasing security and privacy [15].
Implementing the new standards is unlikely to be a panacea however. From a security perspective, it is not the technology that is the issue but rather human behaviour. For example in an online banking situation, compromises are happen due to users not taking basic precautions to secure their PCs. Users are also fooled into revealing usernames and passwords by visiting banking sites that they think are legitimate (Phishing) [16]. More secure methods of authentication are available to banks to overcome the inherent weaknesses but they continue to use standard usernames and passwords. Basic two-factor authentication (something you know and something you have) such as onetime tokens and smartcards are not utilised because of their cost and inconvenience [16].

Cost and Complexity
Integration costs can be 2 to 6 times the cost of the licence fee, according to Gartner [1]. The more customisation an application needs, to integrate with IM products, the higher the cost is going to be. In a lot of cases Application Programming Interfaces (APIs) do not exist for custom applications and they have to be programmed from scratch. Custom applications are often not well understood in an organisation as a result of staff turnover and thus become uneconomic to integrate. The promise of a single sign on in some cases will not be realised due the cost involved in conversion. The language used by vendors has recently shifted from "Single Sign-On" to "Reduced Sign" on as a result of the failure to provide true Single Sign-On in most organisations. A real world description of the complexity involved with implementation, can be found in the paper "Web Single Sign-On Meets Business Reality" by Tim Mather [21].

Most of the research done to date [8], focuses on organisations with more than 10,000 users, where the return on investment is much clearer than it is for smaller organisations who are scared off by the costs and complexity involved [3].

Standards
Security architecture that enables administration of trust relationships between organisations, in a more standardised and automated way, is required before commerce on the Internet will really take off. No single vendor can provide identity integration for all products. Standards for integrating Identity infrastructures are still being developed and are not ready for widespread use in Internet facing environments [5]. Many security professionals are hesitant against using new standards or technologies until they have been out in public and scrutinized over a long period of time.
The interoperability and programming convenience offered by SMAL and WS-Security could make the job of hackers easier should vulnerabilities be found. It appears to be inevitable that web services standards will however become the dominant way identity information will be shared in the future. [18].

Politics
Identity databases usually have owners who can sometimes perceive removal of control and ownership as a threat to their authority [20]. Thus territorial battles can get in the way of implementing a co-ordinated solution. Organisations that have process related issues, in some instances, are reluctant to have them changed or highlighted because that identifies inadequacies of the business owners.

Privacy and Trust Concerns
Issues surrounding trust are the willingness of one organisation to rely upon a second to share information or execute a set of actions [22]. Liberty Alliance is trying to bridge this gap by creating circles of trust. In essence, companies must trust their partners to vouch for their users. This may not be a problem for organisations with well-defined security processes and safeguards but for the majority, it provides a weaker security model.
The following quote from a Meta white paper [19] sums up the trust issue from a different angle.

> *The ability of businesses to trust such technology (WSSM standard) will not be based on the generic technology alone. To bootstrap into trusting technology for delegating trust, business must first trust strategic vendors and partners to apply such technology to specific business relationships. Such vendors will be trusted only when they have earned that trust by repeatedly delivering successful business solutions.*

The implication of what Meta is saying, is that personal relationships will need to be formed with strategic vendors and businesses before automated web of trust will become widespread. Mastery of the diverse security technologies will also be a deciding factor in how trust is gained according to Meta.
How identity infrastructure complies with Privacy laws, issues and concerns is impacting on the uptake [14]. Fear of big brother watching and companies gaining information on your browsing habits are often in the mind of users when they are

considering IM. Building privacy safeguards into the system however can often be a lengthy and expensive process.

Lack of understanding
Many organisations are struggling to understand how access rights should be assigned and provisioned and thus find the concept IM and FIM a complex and daunting prospect [3]. Lack of awareness amongst business, that there is even a security problem contributes to undervaluing the security benefits of IM. Common denials that are used to reduce the level of risk in many organisations are, “It always happens to someone else”, “I have nothing of value” or “I am too small to worry about security”.
The general public perceives the Internet to be a risky place to do business. They are not however, aware or do not care about the underlying authentication mechanism that can secure their identity. To most users, a simple username and password is sufficient. The little padlock indicating a Secure Sockets Layer (SSL) in the bottom of their screens when making purchases give users an added level of comfort. In most cases users are unlikely to go to the effort to securing their identity, until the technology is imbedded by default, as is the case with SSL.

Overcoming Barriers

Overcoming barriers is critical to successfully implementing IM. The majority of the issues are people and process related and if these barriers can be overcome, then identity management will have a greater chance of being successfully integrated into an organisation. The following recommendations in most cases are common sense and business focused.

Defining current practice and policies
Examining and clearly defining current practice and policies in place is critical for managing identity. If you have not examined your current practices and policies are, effectively defining where you move to will be a difficult task. Many organisations do not even have an IM policy that specifies who has access to what and how that access is granted and removed.
The following questions all have implications when considering IM and whether a particular system is appropriate for the organisations needs. These questions will also help determine what ROI is most appropriate for an organisations needs.

- How many different classes of users are there in your environment? E.g. employees, remote employees, customers, partners, sensitive and classified information users?
- How users are currently provisioned and how long does this take?
- How are job changes managed?
- How does de-provisioning of users occur and how long does this take?
- What level of assurance is required for security identity? e.g. passwords, biometrics, tokens and smartcards.
- What is the application work flow?
- How many different applications require a separate username and password?
- How are changes managed throughout the lifecycle of the account?

A good document to identify if IM is appropriate for your organisation can be found at the Sun website. http://wwws.sun.com/software/sunone/wp-readiness.pdf [23]

Additionally, the following link can provide a quick and approximate calculation of ROI for an organisation.
http://www.waveset.com/Solutions/Resources/roi_calculator/index.html [24]

Appropriate selection of an IM suite for current and future needs
Select a IM suite that is appropriate for an organisations current and future needs. Avoid getting tied into products that are propriety focused and do not allow adaptation to emerging standards. Off the shelf products that integrate the majority of the applications will help lower implementation and consulting costs by reducing the amount of customisation required.

Obtain Management buy in
Obtaining management buy in is critical to the success of implementing IM. The implementation of IM is often a long process requiring significant amounts of money, time and organisational change so it is important to align IM objectives to business strategy. Understanding what management perceives are the main business drivers, will help in pitching the benefits and securing their support. Separating out tangible and intangible benefits will also aid in pitching the benefits. Tangible benefits include reduced cost in employing staff and less time provisioning users. Intangible benefits are hard to quantify and include factors such as enhanced customer satisfaction and increased security.

Understand business drivers
Security benefits alone in most cases will not drive IM and it needs to be considered in the context of what others in the organization perceive to be priorities. For instance the helpdesk and security management are most likely to appreciate provisioning and password management due to the reduction in administration time to do their job. Chief Financial Officers will want to know what the likely costs and ROI that can be expected. Giving tangible benefits such as how IM will affect the bottom line will generally be better understood. Business units are likely to appreciate the ability to facilitate faster and easier access to information. The ability to personalize portals and facilitate customer retention is an example of the benefits that could appeal. The CEO will generally be more concerned with the bigger picture as it relates to the organization. Regulatory compliance and how it relates to the CEOs' liability will often be of interest. How IM will help shape future direction also may be another selling point. How IM resolves day-to-day technical issues such as complying with the latest technical standards will probably not factor high on a CEOs' list of priorities.
Security professionals are concerned with integrity, availability and confidentiality of data contained on a system. Risk management and regulatory compliance are also examples of things that directly affect our work. Providing a framework for strong authentication, audit management and account terminations provides the base framework required for making a network secure.
The above examples about what will appeal to who, will vary depending on the organisation and should not be taken as a blueprint for all organisations. It should, however, leave the impression that different views of identity need to be considered.

Don't oversell the benefits
Failure in adopting IM can be traced back to project benefits being over sold in the early stages. This can lead to bitterness and recriminations later on if promises made

are not delivered upon. IM is part of a bigger picture that management must consider. It is not a panacea to all security and management problems. From a security perspective IM must be treated as one part of a defence in depth approach to secure a network. Defence in Depth implies that no one single process or technology can secure an environment and that layers of protection need to be implemented. From a business and management perspective, IM will not magically resolve flawed logic in processes or poor management.

Examine where the greatest amount of pain is and prioritise the project
Identifying where the greatest amount of pain involved in managing Identity will allow an organization to target areas that provide the most return on investment. Prioritizing manageable projects will ensure visible achievement is observed before the project is complete. Implementing areas of IM that involve greatest pain will facilitate buy in for harder to implement stages in the deployment. While smaller organisations may not be able to afford a full-blown IM solution implementing one component such as password resets may be an achievable goal.
Radiant Logic has produced a good matrix to identify low hanging fruit that enables IDM deployments to get off the ground quickly [4]. The following are 4 quick wins they have identified. The difficulty level of each component is identified on a 1 through 10 scale, where 10 is maximum difficulty. Difficulty level is based on the number or organisations that must co-operate for success, dependency risk (number of preceding activities that need to occur for success), source code invasiveness (amount of source code needs to be modified), user training requirement and overall number of moving parts (complexity of backend delivery).

Deliverable – Cleanse Orphan Accounts, Identity Virtualisation
Difficulty - 2
Goal – Remove security holes exposed by incomplete account deactivation
Activities – Perform inventory analysis of Identity data sources, map Virtual Directory to backend end profiles, execute “diff report” and deactivation scripts against mapped Virtual Directory

Deliverable – Comprehensive Account Revocation
Difficulty - 5
Goal – Ensure a revoked account is disabled in real time within all back-end systems to protect valuable enterprise resources (i.e. pay role)
Action – Integrate mapped Virtual Directory established in step 1 with existing account management software via LDAP

Deliverable – Self Service Password Reset
Difficulty - 5
Goal – Reduce help desk costs by 70% (by some estimates)
Action – Extend virtual directory user profile established in step 1 to include secret questions and answers, install LDAP enabled off the shelf Password Management product, instruct call centre to begin directing users to web to reset their own passwords

Deliverable – Extended Sign-On: allows web authentication by any of a user’s many sets of credentials
Difficulty - 4

Goal – A quick win for user convenience prior to a full scale SSO implementation
Action – Enable LDAP based web server authentication through Virtual Directory established in step 1 to enable referral based authentication for all of a user's valid accounts [4]

Set clear goals
Set clear goals about what needs to be achieved to allow the effort to be focused in the right direction. It will also aid in the appropriate product selection for the organisation.

Identify capability
Does your organisation have the ability to develop an in house solution or are you going to need to rely on the vendor for the entire engagement? What are your funding limitations? What is the timeframe? If these questions are answered it makes the choice of selecting the right vendor and assistance needed easier task [20].

Hide the complexity from users to gain greater acceptance.
No matter how clever the idea is it will be little or no use if it is not useable. If the system is not usable users will either bypass or ignore the processes that have been put in place.

Identify performance expectations i.e. outages and SLA
If the majority of you organisation operations are dependant on a single identity management repository and this is not available then it is going to have obvious political and business consequences [21]. Define what expectations the organisation has for keeping the IM solution up and available.

Set a test plan
Have an accurate test plan to allow the benefits of the IM system to be evaluated [20]. Does the system actually do what is supposed to is a question that management will ask. If previous advice about breaking the project up into manageable pieces is followed, it will be easier to justify harder to-implement components, with a test plan that sets achievable goals.

Conclusion
There is a growing demand for IM, to help reduce costs, increase efficiency, increase interoperability and provide a more secure infrastructure. Many IM projects will have little or no chance of being implemented if certain barriers are not addressed. Security professionals need to be aware of an organisations needs, based on risk analysis and business requirements. Fundamentally IM is about people and processes, not the technology. Many barriers to implementing IM have been presented in this paper but identifying the business drivers, obtaining management buy in and identifying the pain points are the keys to the successful implementation of IM.

.

References

1. Witty, R.J. The Identity and Access Management Market Landscape. 07 November 2003. http://mediaproducts.gartner.com/reprints/ca/118352.html (19 May 2004)
2. Tan, S.S. Establishing Enterprise Identity Management; March 30, 2003; http://www.giac.org/practical/GSEC/Soon_Sian_Tan_GSEC.pdf (19 May 2004).
3. Novell Worldwide Services. Exploring Secure Identity Management in Global Enterprises. March 2003. http://www.novell.com/solutions/nsure/sim_stanford.pdf (19 May 2004).
4. Trends, L. Four Quick Wins that Accelerate Identity Management Deployment. 2004. http://www.radiantlogic.com/FourQuickWinsthatAccelerateIDMDeployment.pdf (19 May 2004)
5. Bhimani, A. Web Services- Not So Fast; October 2002. http://infosecuritymag.techtarget.com/2002/oct/webservices.shtml (19 May 2004).
6. Mahrt, R. In Pursuit of Liberty? An exploration of the Liberty Alliance Project. January 2003. http://www.sans.org/rr/papers/6/851.pdf (19 May 2004).
7. Witty, R. Five Business Drivers of Identity and Access Management. 31 October 2003. http://www.waveset.com/Insights/analyst.html#Gartner (19 May 2004).
8. Gartner. Gartner Consulting Study: Automated Identity and Access Management Solutions Can Yield 300 Percent ROI. November 21, 2002. http://www4.gartner.com/5_about/press_releases/2002_11/pr20021121a.jsp (19 May 2004)
9. Legon, J. FTC: Identity theft strikes 1 in 8 adults. 29 October 2003. http://www.cnn.com/2003/TECH/ptech/09/04/id.crime/ (19 May 2004).
10. Office of Strategic Crime Assessments. The Changing Nature of Fraud in Australia; 2000. http://law.gov.au/agd/Department/Publications/publications/Fraud.htm (19 May 2004).
11. E-Marketer. Steely-Eyed about Identity Theft. May 04, 2004. http://www.emarketer.com/news/article.php?1002776 (19 May 2004).
12. Greenfield, D. Digital Identity's Hidden Maestro. 3 May 2003. http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703524 (19 May 2004)
13. Becker, D. Passport to nowhere?. 23 March 2004. http://news.com.com/2100-7345-5177192.html?tag=alert (19 May 2004).
14. Lessig et al. Digital Identity in Cyberspace; 10 December 1998; http://www.swiss.ai.mit.edu/6095/student-papers/fall98-papers/identity/white-paper.html (19 May 2004)
15. Gary Ellison, J.H. Susan Landau. Security and Privacy Concerns of Internet Single Sign-On. 6 Sep 2002. http://research.sun.com/liberty/SaPCISSO/index.html (19 May 2004).
16. Wood, R. Password security for online banking queried. 3 September 2002. http://www.nzherald.co.nz/storydisplay.cfm?storyID=2352456 (19 May 2004).

17. News.Com. Get Up To speed: Web services. 30 March 2004 http://news.com.com/2001-7345_3-0.html?tag=nefd_guts#behind (19 May 2004).
18. Desk, W.N. Market for Web Services-Based Professional Services Heats Up, Says Study; 13 May 2004. http://www.sys-con.com/story/?storyid=44807&DE=1 (19 May 2004).
19. Group, M. The Intersection of Web Services and Security Management: A Service-Oriented Security Architecture. July 2003. http://www3.ca.com/Files/IndustryAnalystReports/SOA.pdf (19 May 2004)
20. Hobbs, R. Considerations For Implementing Single Sign-On Within The Enterprise. 1 September 2003. http://www.giac.org/practical/GSEC/Russell_Hobbs_GSEC.pdf (19 May 2004).
21. Mather, T. Web Single Sign-On Meets Business Reality. Feb 2002. www.sans.org/rr/papers/6/130.pdf (19 May 2004).
22. Waters, Nigel R.C. Authentication for e-government: Privacy Impact Assessment report. December 2003. http://www.e.govt.nz/docs/authent-pia-200312/ (19 May 2004).
23 Microsystems, S. Network Identity Capability Assessment 2002. http://wwws.sun.com/software/sunone/wp-readiness.pdf (19 May 2004).
24 Waveset. Return on Investment (ROI) Calculator. 2004. http://www.waveset.com/Solutions/Resources/roi_calculator/index.html (19 May 2004)