

Authentication Monopoly in the Making?

The Question of Privacy

1 Introduction

There is a battle brewing over the future landscape of the next generation of the Pervasive Net.¹ [Langa, 2001 #58; Allan, 2001 #15; Berlind, 2002 #76; Clark, 2001 #6; Coursey, 2001 #9; Coursey, 2001 #52; Houston, 2001 #8; Kehoe, 2001 #7; Langa, 2001 #31; Manjoo, 2001 #28; Papadopoulos, 2001 #18; Parr, 2001 #62; Schoenfeld, 2001 #3; Schwartz, 2001 #37; Shirky, 2001 #17; Stross, 2001 #39; Walker, 2001 #4] Certain commercial interests are hard at work trying to create software-based bottlenecks over which they can exercise monopoly power: digital identity storehouses which not only authenticate and verify users for Internet dealings, but can also keep track of purchasing habits and preferences, time and “clickstream” of transactions, entertainment preferences, stock portfolios, education and medical histories, driver record and social security numbers, travel profiles, and more. The prevailing theory is that the Internet will make a quantum leap forward in efficiency and utility when it can recognize individual users, instead of just recognizing browsers, IP addresses, and MAC addresses. [Papadopoulos, 2001 #18][Joy, 2000 #36][Langa, 2001 #31] The potential benefits of such a single sign-on service are immense, but so are the privacy concerns. Will the convenience invariably lend itself toward a monopoly provider? And if so, is there a need for some kind of regulatory relief from a failed market?

I will examine here under what conditions the control of digital identities might lend itself toward a single provider, and subsequently address the question of whether there needs to be

¹ “Pervasive Net” is my own term, and by which I mean an Internet that becomes so essential to daily transactions it cannot be avoided. Nearly every value chain will be computerized. I borrow the future-casting from Bill Joy. []

some change or accommodation in our legal structures to correct for potential market failures, or to protect the public interest. We will be examining this issue from an interdisciplinary perspective.

Starting with the technical, are there any indicators in the architecture of identity management systems that might tip the market? For instance, is there bundled functionality that is contingent on certain mechanical, electromechanical, or software-based dependencies? We will look closely at the question of open or proprietary standards, and how they may be manipulated to tip network industry markets toward a de facto winner. We will also look at existing laws to see what protections we may have against monopoly. I will question the role of policy: are free market-based solutions or regulatory protection better for the consumer in the matter of protecting privacy. I will explain the business drivers that are pushing for digital identity from the providers and from the consumers. Are the different interests in this marketplace behaving rationally? What can economic theory lend to the analysis? In the end, I hope to demonstrate how this market will likely play out, and what the implications are for the question of regulatory relief.

2 What is at Stake?

2.1. Identity vs. Digital Identity

We need to ask what are the differences between real-world identity and digital identity, and why does the difference matter? To avoid any messy existential arguments, we'll only be considering identity as defined by some external institution or entity, such as the U.S. Government or a retail or services corporation. We can say that a personal identity constitutes a set of characteristics or attributes that collectively create a uniquely identifiable profile.

Table 1: Components of "Identity"

Things you have	Things you are	Things you like	Things you use
------------------------	-----------------------	------------------------	-----------------------

Name	Fingerprints	Entertainment preferences	Calendar
Address	Retinal scan	Dining preferences	Affinity programs
SSN	DNA	Friends and associates	Club Memberships
Driver's License	Education history		Address book
Email address	Medical history		Credit cards
Financial assets	Genealogy		Phone number
Birth certificate			

“Digital identity” is the codification and archiving of this set, or a subset, of information. Any company that sells products or services would like to “own the customer.” Access to a directory containing massive numbers of users and their digitized identities would help them provide more targeted services. Higher degrees of personalization ostensibly lead to greater levels of loyalty and trust. A company that owns this directory and can charge for access to it would certainly have control over a very desirable database of commodified information. Alan Westin and Erik Larson have both warned against “improper commercial” use of private information in discussions of the “view of information as a commodity”:

The commodification of information brings some interesting effects. One is Larson’s phenomena of ‘recombinant data’ where automated software systems scan one database after another or meld from different sources and create whole new strains of information. [Schoechle, 1995 #50]

From the commercial point of view, leveraging the information in digital identity storehouses to facilitate communication, commerce, and community provides potentially lucrative new channels of income.

The type of leveraging that would enable more targeted advertising or more innovative services can already be seen in use, for instance, at Amazon. By tracking your purchasing history and storing your credit card number, shipping addresses, and billing addresses, they can provide recommended reading or listening lists, links to consumer reviews, and “One-click” convenience in facilitating transactions. Imagine the additional synergies if Amazon were to entrust your digital identity to a “trust broker” company that had relationships with numerous

other goods and services companies? Just finish reading *Memoirs of a Geisha*? Did you know that United is offering \$600 flights from LAX to Osaka in the month of October? Just bought a new John Scofield CD? Click here to purchase tickets to the Great American Jazz Fest in your town next week at 20% off for our Internet customers. Looking for books on Java programming? You can sign up for an online course at uNext.com for a discounted rate since you are one of our affinity partners and a member of Developer Central.

2.2. Definitions

There are three main capabilities that these “trust brokers” are attempting to provide: identity access and management, authentication, and authorization.

Identity, as we have said, is a representation of a set of characteristics or attributes that collectively create a uniquely identifiable profile. Authentication is the process of guaranteeing or validating this set of attributes and associating it with a person. Authorization is a set of policy rules that define the capabilities and limitations in access rights for an authenticated identity. These capabilities can all be considered under the subset of integrated security systems, one of the two requirements for massively distributed computing. The other is integrated directory services.

The new paradigm for offering services over the Internet will be a driver for adoption of digital identity management systems, whether proprietary or open. Access to these services will be dependent on an authenticated user identity. This is demonstrated in Figure 1.

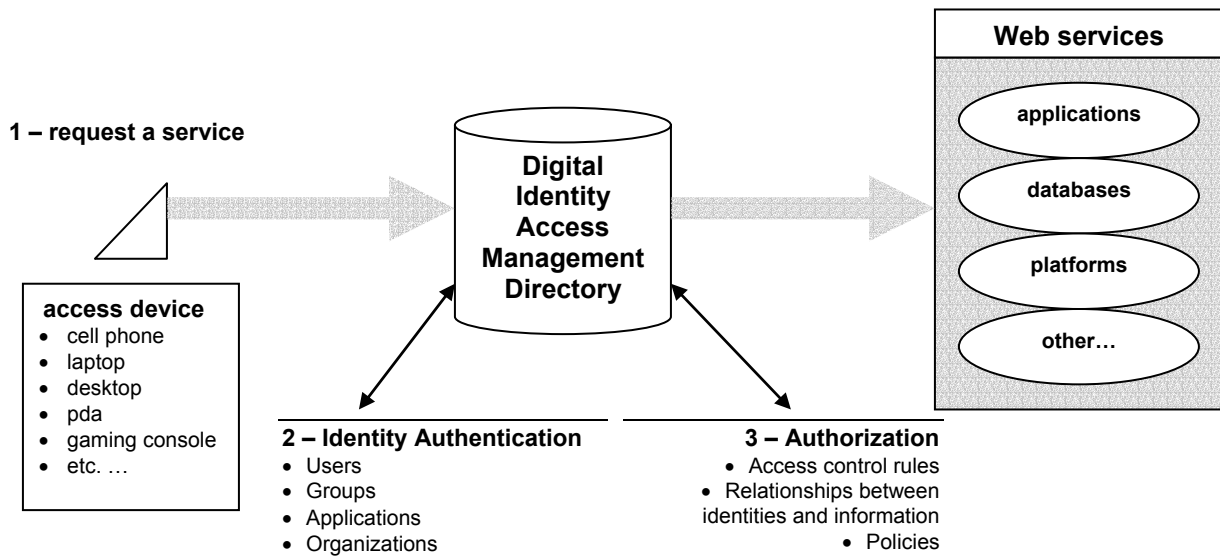


Figure 1: Access to Web services: Identity - Authentication - Authorization Procedure

2.3. Question of Monopoly

A classic definition of monopoly is a firm that has the ability to restrict output while raising price. Generally, monopolies occur when there is some element of scarcity, or in more general terms, when there is a failed market condition. The deregulation of the “natural monopoly” telephone industry in the 1996 Telecommunications Act remains an experiment in some markets, though there have been successes in others. This example alone should prove the assertion that it is easier to prevent a monopoly than it is to break one up. Although laissez-faire free-market advocates favor restraint, especially in nascent industries and infant markets, the economic models of competition in network industries have proven over and over that attempted monopolization is perfectly rational behavior. Therefore, it is certainly important to examine potential failures before they occur, and though I do not advocate proactive regulation, there are certain forms of regulation that have proven to protect innovation in the past. Certainly it is in the best interest of the public good and welfare to at least anticipate these inefficiencies and develop a game plan of scenarios. The importance of examining the appropriability of

regulatory intervention is even more poignant post-Enron, as Hal Varian metaphorically described in a *New York Times* editorial on March 14.[Varian, 2002 #71] So while it is not yet possible to say that there is indeed a definable market for identity access and management, there are enough alarms raised from privacy considerations alone that the topic of identity provision and management warrants a closer examination.

3 Technical

3.1. Architecture Considerations

There are many companies, protocols, and services that can provide intra-domain² authentication and authorization. The challenge has been to implement cross-domain, trusted authentication that is interoperable. For the type of distributed computing environment required for Web services, these authentication and authorization functions will be tied closely to integrated and distributed directory services. If authentication is to be shared across domains and across companies – across the Internet – then the authenticating entities need to be able to negotiate and agree on the various details of authentication. For example, message format, encryption methods, identification of entities, and so on. Phil Schacter, a Burton Group researcher, has said that this problem may be “the most difficult interoperability problem facing the network industry.”[Schacter, 1999 #54]

A recommendation for the framework of interoperable authentication has been defined in an Internet Engineering Task Force (IETF) RFC called “Generic Security Services Application Programming Interface” (GSS-API).³ Many technology companies have been working on implementations of the x.509 and Public Key Cryptography System (PKCS) as possible

² A *domain* is a set of networked computers or computer devices (such as file servers and printer servers) grouped together to simplify security, management, and administration of all the attached devices.

³ There are currently five “proposed standards” under review, dating back to 1996: RFCs 1961, 1964, 2025, 2478, and 2479.

frameworks. Some of them are working in industry consortia such as the Open Group, founded by IBM and Intel, and others are contributing to the open source Kerberos protocol.

The development of standards, however, is a lengthy process, and adds a fitting third example to the famous quote by Otto von Bismarck: “There are two things you never want to see being made: legislation and sausage.” Microsoft saw a business opportunity to become an identity service provider in a new market, combining the convenience of single sign-on with authentication for companies that agreed to become partners.

3.2. Service and Application Considerations (“Microsoft Passport”)

The Microsoft Passport single sign-on service rolled out in 1999. The basic model for the plan is shown in Figure 2.

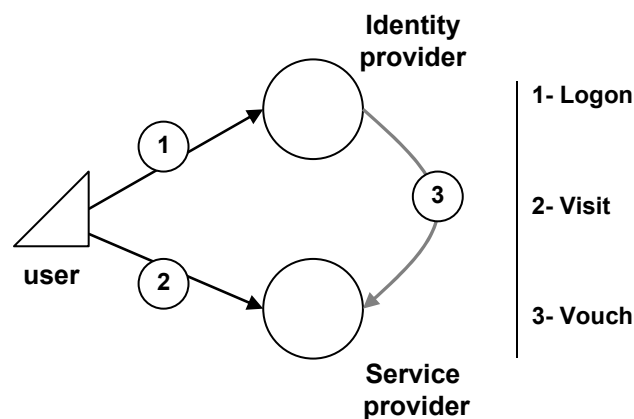


Figure 2: Identity Provider Concept

The identity provider can make money by charging a user service fee, charging a relaying party service fee, taxing the user or the service provider on transaction costs, bundling some value-added services,⁴ or exploiting the value of customer intimacy data.[Blakely, 2002 #124]

The initial release of Passport promised ease of use to the subscribers, who could sign on to the service for free. The design came from the authentication process for Hotmail and some personalization features from Firefly Technology, two companies that Microsoft acquired in

⁴ Such as instant messaging alerts or targeted advertising.

1998.[Rosoff, 2001 #56] A user gains a Passport account by signing in through the Passport web page or via the Passport Wizard in the latest version of the 32-bit consumer operating system, WindowsXP. People who are signed on to use the free Hotmail email accounts were automatically transitioned into Passport in 1999.

There are four main components of a Passport account, shown in Table 2. [Rosoff, 2001 #38; Rosoff, 2001 #56; , 2001 #58; Conry-Murray, 2002 #81; Microsoft, 2001 #63]

Table 2: Passport Account Components

PUID	Passport Unique Identifier (assigned by Microsoft)	
User Profile	Minimum requirements: <ul style="list-style-type: none"> • <i>Phone number or Hotmail or MSN.com email address</i> • <i>Name</i> • <i>Demographic data</i> <ul style="list-style-type: none"> - <i>ZIP Code</i> - <i>State</i> - <i>Country</i> 	Optional entries ("Passport Public Profile") <ul style="list-style-type: none"> • Gender • Age • Occupation • Marital Status • Personal statement • Hobbies and interests • Favorite quote • Favorite place, thing, or pet • Home page • Option to disclose profile in chat rooms • Notification preferences
Credentials	<ul style="list-style-type: none"> • Phone number or email address • 6-character password or PIN • 4-digit security key 	
Wallet	<ul style="list-style-type: none"> • Credit Card Number • Shipping address • Billing address 	

There is the capability of creating a "Kids Passport" as well, which checks for an optional "under-13" tag in order to redirect the user to parental consent screens.

There are two kinds of Passport Partner sites: Sign-In Sites and Express Purchase Sites. It is only the Express Purchase Sites who have paid a licensing agreement with Microsoft in order to access the information stored in the Wallet. All Passport Partner Sites are registered with and licensed by Microsoft to have secure access to the Passport login server. There are Passport

Manager software kits that enable Unix and Linux-based systems to be Passport Partners. However, only Windows systems can be the login server.

When a Passport user wants to make a purchase, they click the Express Purchase icon on the merchant's web site, which redirects to a Microsoft server for authentication, and then a SSL connection is made between the Express Purchase server and the merchant site to send the information in the e-wallet in order to complete the purchase. The merchant does not authenticate the user.

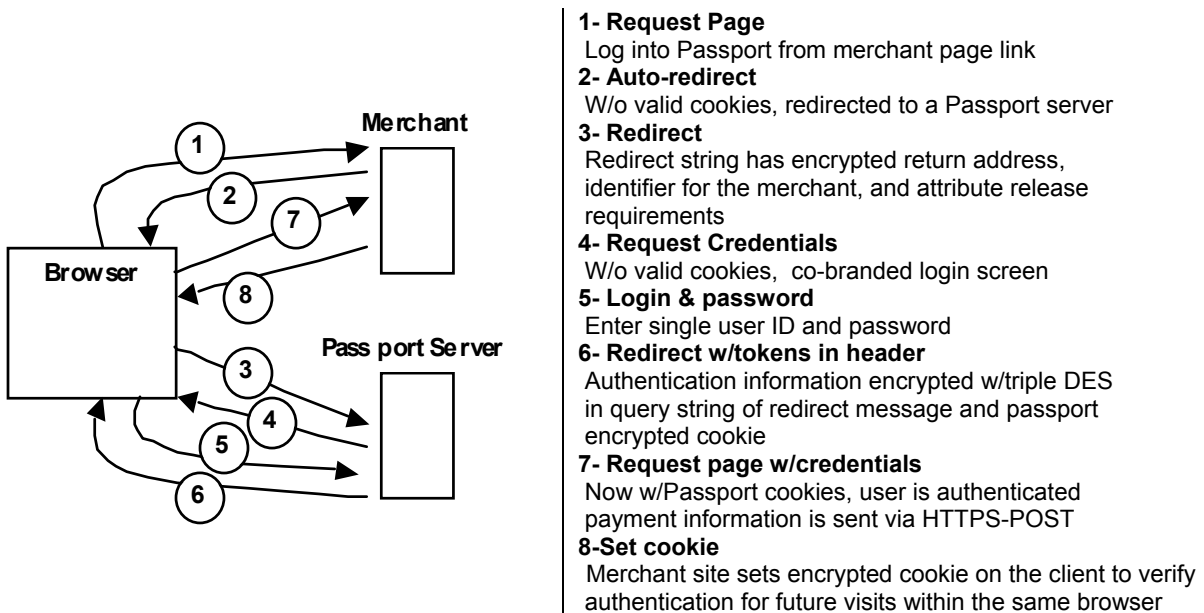


Figure 3: Initial Sign In Process

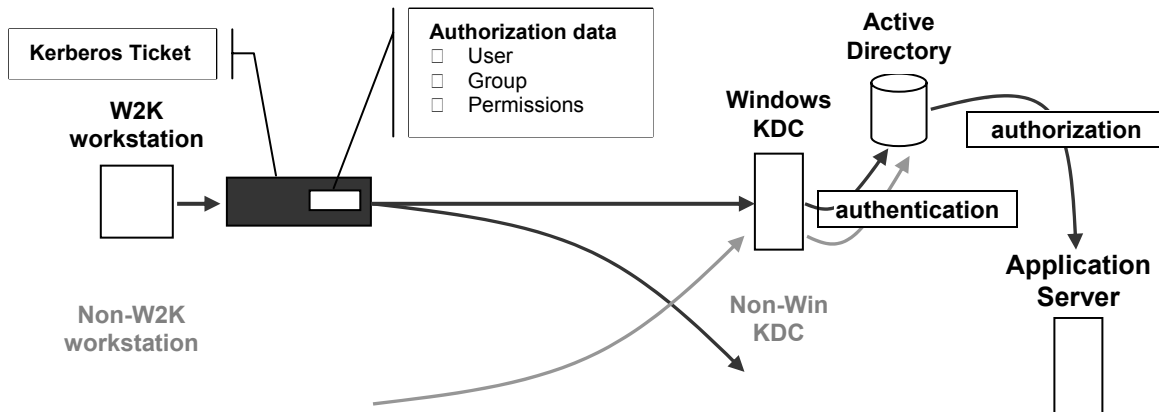
At the moment, Passport works using cookies and HTTP redirects. The initial sign-in process is demonstrated in Figure 3. [Kormann, 2000 #34; Conry-Murray, 2002 #81; Rosoff, 2001 #56; Swoboda, 2002 #111] Because it uses common Internet protocols such as HTTP, SSL, and cookies, it is essentially browser neutral (although there was a documented case where a JavaScript implementation discrepancy caused Netscape users to be unable to log out[Kormann, 2000 #34]). However, the use of these common protocols also means that

Passport is subject to all the same inherent security problems with them. These include bogus merchant attacks with fake Passport login sites, interception of HTTP-redirects, and denial-of-service attacks. There have also been numerous cases of other security failures, such as the unwitting release of Passport account information, transport of Windows9x and ME user passwords in readily-readable clear text, and service failures at Passport Partner sites that incorrectly implemented Microsoft's security requirements.[Kormann, 2000 #34; Rash, 2001 #13; McWilliams, 2001 #93; Slemko, 2001 #107] The Electronic Privacy Information Center maintains a web site called "Sign Out of Microsoft Passport" where they provide constant vigilance of security problems with continually updated news reports and white papers.

Microsoft is not unaware of the security issues, and they have not allowed them to go unaddressed. They have actively attempted to provide fixes and updates to Passport users with great alacrity, and are currently working on version 3 of their Passport SDK.

One of their efforts to improve security is their adoption of the Kerberos 5 protocol, an open source authentication system designed and maintained at the Massachusetts Institute of Technology and recommended by the IETF in the RFC 1510 specification. Support for Kerberos 5 has been built into the Windows 2000 Operating System and all of its successors, such as WindowsXP. Although the separation of authentication and authorization in Kerberos was a design goal to simplify functionality, Microsoft added proprietary extensions to include authorization capabilities. [Orlowski, 2001 #69; , 2000 #70] The process closely integrates Microsoft's Privilege Attribute Certificate (PAC) with a Kerberos 5 ticket, duplicating but not interoperating with the Open Software Foundation's PACs. The extensions therefore limit Microsoft's Kerberos interoperability to Windows 2000.[, 2000 #70]

What we have here is our first indication of a technical hook. Microsoft's version of the Kerberos Domain Controller (KDC) recognizes tickets containing these extensions, and then maps a username and password to an identity (and the identity's group, if there is one) inside a directory along with the necessary authorization information. The directory in this case is always Microsoft's Active Directory product. Unix-based KDCs can read and authenticate users from Windows 2000 systems, but it will ignore the authorization data. Therefore, a KDC running in a Unix or Linux environment will be unable to authorize client access to services hosted on an application server. This means that if a company chooses to use the advanced



security features of Kerberos 5 tickets for authentication and authorization, they will be tied into purchasing Active Directory, which only runs on Windows operating systems.

Figure 4 demonstrates how the authorization data included in Kerberos tickets by the use of the extensions allows a Windows KDC to forward the enclosed PAC to Active Directory. The

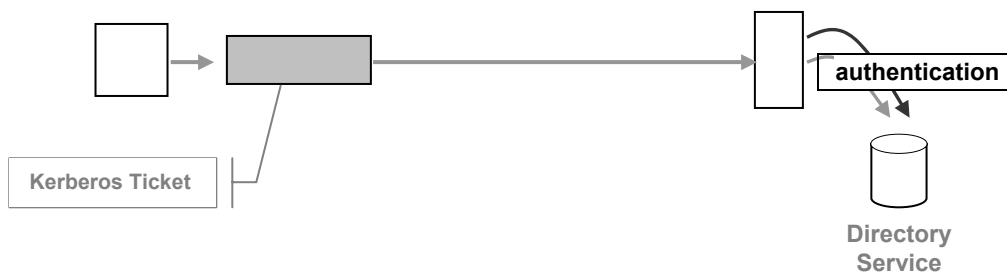


Figure 4: Kerberos authentication (and authorization)

username is matched with an existing entry, and an impersonation token is generated to allow access to the services running on the application server. A ticket from a non-Windows client, or from a pre-W2K client, cannot include this data, and cannot be authorized by Active Directory. Similarly, a non-Windows KDC will simply ignore the extra data, but still perform the authentication of the user. Authorization is decoupled from the standardized Kerberos process, and must be provided by some other means. Microsoft views this as added functionality and an integrated feature, much as the Internet Explorer browser has been described in relation to the Windows OS.

Authentication and authorization by Passport, whether via HTTPS and cookies or via Kerberos, always relies on entries in Active Directory. The use of Kerberos adds several advantages, such as greater security through mutual authentication (the client and the server are both required to authenticate to one another), transitive trust across domains, support for smart-cards, and the fact that it is an open standard.[De Clerq, 1999 #123] But most important, integrating support for Kerberos into their consumer OS, Microsoft is able to position themselves as a standards-bearer. Many companies already use Kerberos internally for authentication, so embracing these IT departments with interoperability and then extending the capabilities to require Active Directory guarantees sales.

3.3. “Federated” Digital Identity Systems

Moving the authentication from a browser-based system to one built into the Operating System creates a framework for a “federated” identity system. The concept of federation basically means that there is interoperability across enterprises and organizations. There are a few key assumptions in our definition of “federated”: 1) Authentication is enabled across multiple directories, 2) capability of multi-domain single sign-on, and 3) some form of synchronization exists that allows mapping of identities.[Mulchandi, 2002 #125]

Commitment to this new model poses significant challenges to Passport given the extant design. Not only does it entail giving up total ownership of the entries in the Passport databases, it may require changing applications, overhauling the backend, and addressing security concerns.[Rosoff, 2001 #57] Agreeing to validate users from other domains or from other trusted identity providers distinctly separates the act of authenticating from the act of authorizing. This means that either the user is in control of what identity information gets shared between the providers, or the identity providers have reached some form of contractual arrangement. In either case, the potential for one company to control identities is significantly reduced. The conceptual difference is shown in Figure 5.

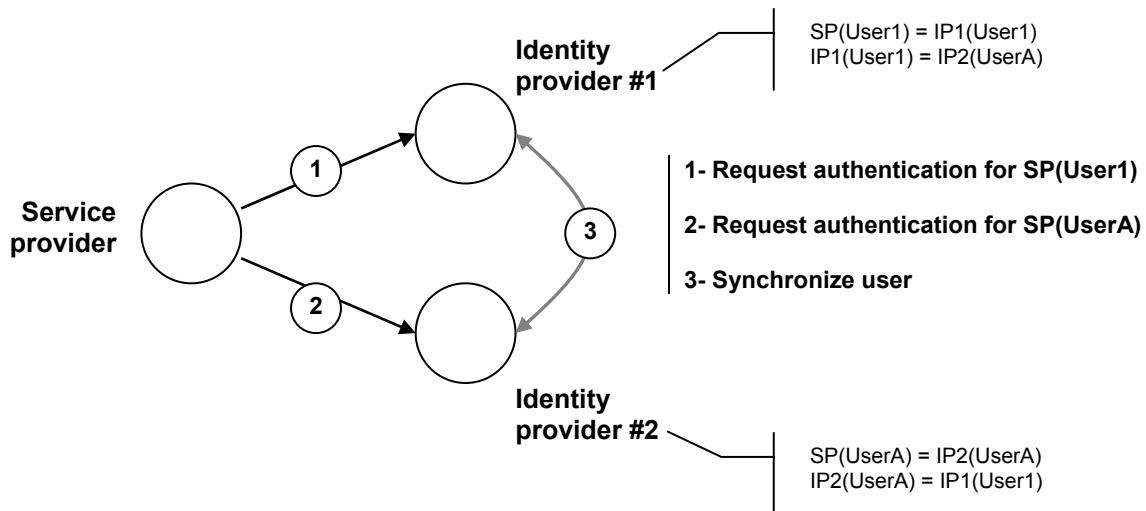


Figure 5: Sharing and synchronizing users between trusted Identity Providers

Why this shift in design? For one, it addresses some of the user privacy concerns that have been raised with the Federal Trade Commission: the “potential to track, profile, and monitor users of the Internet has far-reaching and profound implications for privacy protection in general and in particular with regard to the growth of electronic commerce.”[, 2001 #58; , 2001 #38; Manjoo, 2001 #28] This indicates that Microsoft is responding to the marketplace demands.

Another reason could be that even by late November 2001, two years after its inception, Passport had only managed to sign up 17 non-Microsoft-owned partners.⁵ In the middle of the 2001 summer, press reports were leaked that Sun Microsystems had been working on creating an industry consortium of companies unified by the common goal of creating an open standards-based Passport alternative.[McCullagh, 2001 #91] Microsoft announced that they would alter the Passport service on September 20, 2001.[Pescatore, 2001 #60] The Liberty Alliance was announced on September 26, 2001, with an initial member set including General Motors, Nokia, RSA, and Bank of America.⁶ [Shankland, 2001 #102] IBM, considered by some to be the current leader in Web services, has remained uncommitted to either system. Although ZDNet writer David Berlind speculates they will side with Liberty based on comments from Senior VP Steven Mills in favor of “open standards,”[Berlind, 2002 #126] the Tivoli Group has been quietly contributing development efforts to the Internet2 “Shibboleth”⁷ middleware working group, an academic endeavor funded primarily by grants from the NSF.

The move toward interoperable identity systems should be considered a natural one. Sun Microsystems provides an informative chart on “Network Identity Evolution” in a White Paper made available in conjunction with their efforts toward the Liberty Alliance project, and pictured in Figure 6.[, 2002 #129] Some analogies include the PSTN, email, and the Domain Name System. Similarly, the open protocol LDAP is rapidly becoming the de facto for interoperable directory services. Open and standardized interfaces unify all of these examples. The PSTN is kept open by regulation, and email, DNS, and LDAP all depend on commonly agreed upon

⁵ By late March, 2002, Microsoft claims there are 68 Express Purchase Partners (including Buy.com, Starbucks, Office Depot, Victoria’s Secret, and Godiva). There are only 57 Sign In Partners, and almost one-third are properties owned by Microsoft.

⁶ The Alliance has gained greater legitimacy by continuing to add influential members such as AOL Time Warner, American Express, Visa International, Novell Networks, and PriceWaterhouseCoopers.

⁷ The Shibboleth project is working on cross-domain authentication and authorization, and has been largely built around the Security Access Markup Language (SAML), a proposed standard by an industry standards group called OASIS. Interestingly, the IT companies who are members of the Liberty Alliance share a high crossover with the IT companies that are members and contributors to SAML standard.

references. In other words, an architecture specification is in place that guarantees no single entity can exercise absolute control.[Lessig, 2000 #130]

In describing the benefits of single sign-on and federated identity authentication, ATM cards are often cited as an example. This is a system where proprietary implementations had been in existence and in widespread use. There were no RFCs documenting a standard, and there was no government regulation mandating interoperability for the public good. Instead, banking institutions responded to a marketplace demand to have access to funds from any bank teller machine, and a federated system was developed.

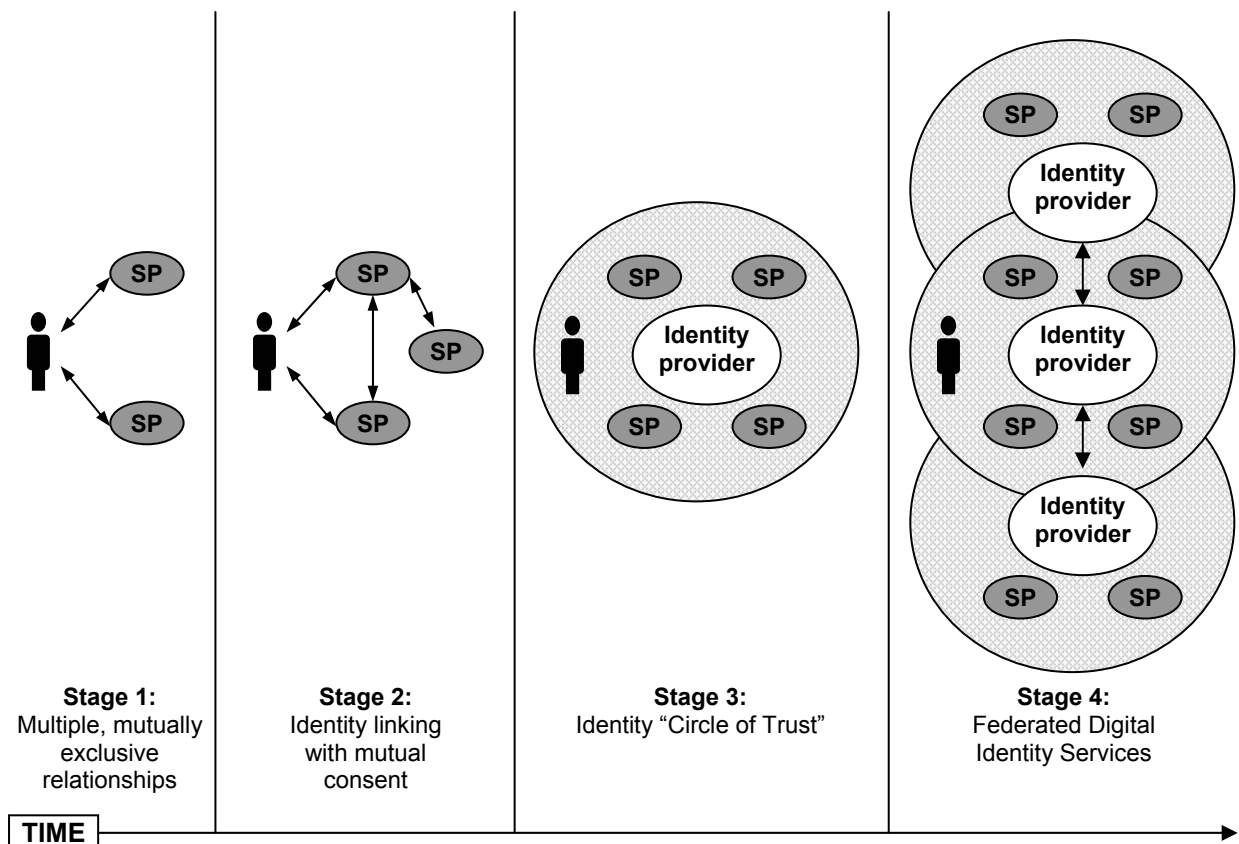


Figure 6: Evolution of identity management systems to interoperable "federation"

Is it possible that consumer demand will eventually drive a similar relationship between Microsoft Passport and the Liberty Alliance, or any other identity management standard that may come along? The Alliance has invited Microsoft to become a member, potentially leading to the adoption of Passport as the authentication mechanism. Microsoft CEO Steve Ballmer indicated in an interview with CNet News.com, however, that they would not like to surrender any of their intellectual property as a condition for joining. Brian Arbogast, a VP in charge of .Net core services, has also offered, “Absolutely, we are committed to interoperability. Our customers need it and we will deliver it. If the goals of the Alliance are to create a seamless identity exchange and services on the Internet, that's something that we could get behind. We think there is a tremendous opportunity for us to work with the Liberty Alliance.”[Lemos, 2002 #131]

These are the essential questions from the architecture discussion: Is a commitment to interoperability sufficient to justify non-intervention? What role might open standards (as with SMTP or DNS) or enforced standards (as with the PSTN or the proposed SSSCA) contribute to the amelioration of likely monopolization? Finally, how have standards been manipulated in network industries to tip the market?

4 The Case of Standards

A fundamental principle of commitment to standards should be “that standards serve to encourage economic interchange.” [Cargill, 1996 #24] However, standards are often used in the IT industry “as a marketing tool to create and expand the pool of possible buyers.” [Cargill, 1996 #24] The commitment to four canonical standards for interoperability by all the major players in Web services is a perfect example. They are SOAP (Simple Object Access Protocol), UDDI (Universal Description, Discovery, and Integration), WSDL (Web services Description Language), and XML (extensible markup language). Despite having published recommendations, the very act of the creation of the Web services Interoperability Organization,

designed to test for compliance with the specifications, shows that a published standard and an implementation of that standard does not guarantee interoperability.

4.1. Technical Standards

It is common practice in the IT industry to attempt to tip a market to a proprietary solution. There is nothing illegal about this – it is rational economic behavior. Microsoft has historically linked standards to their proprietary technologies to create lock-in effects. We have already examined the case of Kerberos 5.

The Active Directory product – Microsoft’s lynchpin product for taking control of the data center environment – uses a layered API model for access management. There are certain basic administrative functions that cannot be accomplished using the LDAP *inetOrgPerson* object, which is an RFC draft and considered the de factor standard. Instead, developers must write to the Active Directory Service Interfaces API. This is demonstrated in the figure below.⁸ [Blum, 2000 #67]

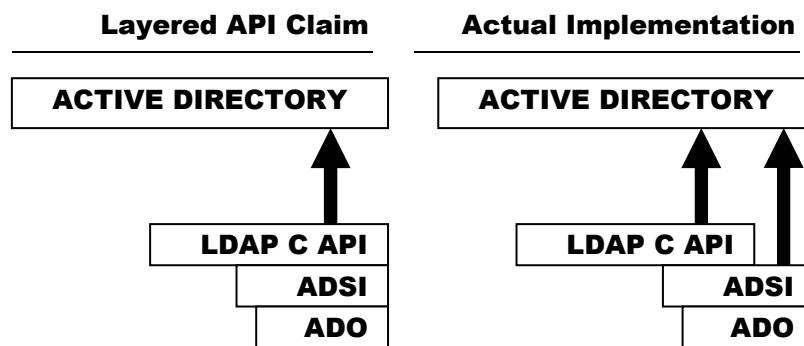


Figure 7: Active Directory Interoperability Claims

In various analyses of Web services providers, Microsoft has been called a “leader in Web services standards” by the Precursor Group[Whyman, 2002 #132] and declared the “leader in XML” by the Gartner Group.[Smith, 2001 #133] The use of XML guarantees neither openness

⁸ <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/dswriteaccountsnpn.asp>

nor interoperability, despite the assertions by marketing departments. An XML document, though readable in its non-binary format, is useless without an accompanying (and patentable) schema definition. These schemas are patentable. In an interview with ZDNet, Ballmer stated, “In adopting Internet standards such as XML ... as part of its .Net initiative, Microsoft will continue to protect any intellectual property that it embeds as objects in XML wrappers. We will have proprietary formats to protect our intellectual property.”

4.2. Standards in Network Industries

Once again, there is nothing illegal about this activity. It appears to match up well with a hypothetical scenario described by Carl Cargill below:

... if a participant in the process (call it ABC Corporation) has delegates on five committees who are working on standards ... and all five delegates are working toward a common purpose as defined by ABC Corporation, there is a high level of possibility that some form of synergy will take place, and the five committees will begin to move towards a common set of beliefs or practices that favor the ABC Corporation. [Cargill, 1996 #24]

Microsoft, we should note, participates in or founded the standards groups and industry consortia involved with the development of numerous Web services building blocks, including SOAP, UDDI, ebXML, DSML, WSDL, and many others. This does not preclude other firms from competing – having a standard gives Microsoft no competitive advantage without a corresponding implementation and use of that standard.

The role that Microsoft sees for standards is as a way to interoperate with “legacy” systems, as can be seen in this diagram from developer network web pages. [Microsoft, 2001 #68]

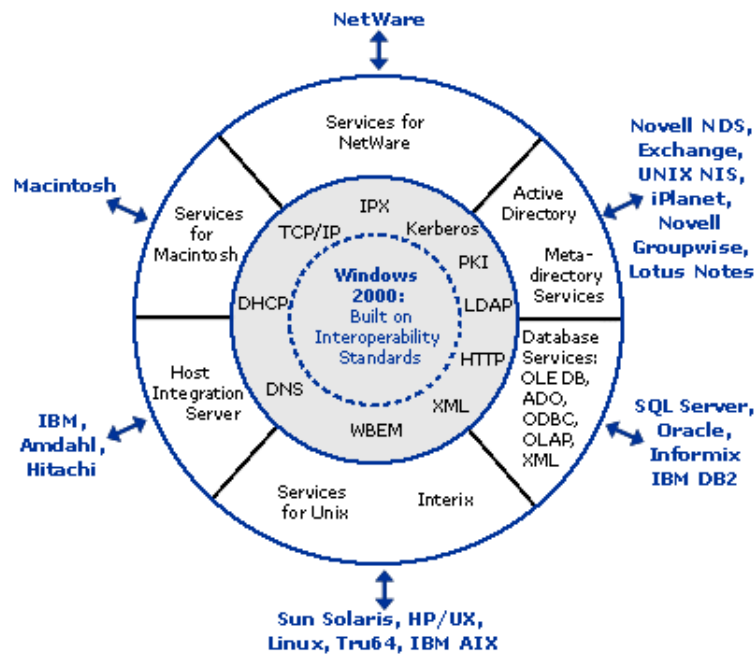


Figure 8: Windows 2000 interoperability strategy with standards

Their pattern of behavior coordinates well with the rational economic logic in a free market network industry: firms will attempt to monopolize whatever portion of a market that they can. Attaching proprietary extensions and creating dependencies gradually transitions users of “legacy” systems into the center of the diagram. This is the lock-in strategy from the data center side.

Microsoft already owns a monopoly on desktop operating systems – still the primary means by which people access the Internet worldwide – and is therefore in a uniquely advantageous position to leverage this bottleneck access point into further control of the identities of the users of those desktop operating systems. This is the lock-in strategy from the client side.

5 Legal and Policy Considerations

5.1. Social Standards and Privacy Policy

The privacy implications of single sign-on services are immense. Who stores the user data? Where are the passwords kept? How is this information kept secure? Because there is no statute in the United States today that demands protection of user data across communications networks,

there has been little opposition backed by legal legitimacy to the creation and implementation of such a digital service. (There are, however, privacy policy formation guidelines.⁹) The European Union, on the other hand, has a much more developed history of privacy protection policies in place that are backed by legislative actions.¹⁰ This probably comes from cultural history and the “European tradition that the state should play an active role in protecting the citizen from social harm.” [Strauss, 2000 #44]

The difficulty in designing a policy for the protection of privacy is that there is no absolute social, cultural, or even legislative standard upon which to base the code. [Cargill, 2001 #45; Lessig, 1998 #1] There is no universal declaration of human privacy rights,¹¹ although there have been attempts to create frameworks for adopting privacy policies.

Lessig claims that the United States government has traditionally not protected privacy by law. [Lessig, 1998 #1; Lessig, 1999 #2] The Privacy Rights Clearinghouse agrees by saying, “The U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level.” [Clearinghouse, 1997 #47] Strauss and Rogerson also concur: “privacy is not explicitly protected by the Constitution.” But they also condition this statement by saying, “Americans have traditionally considered privacy a valued right.” [Strauss, 2000 #44] Marc Rotenberg, executive director of EPIC, adds a proviso to Lessig in a paper submitted to the Stanford Technology and Law Review Journal: “In the absence of a general privacy law for the private sector, the US has routinely protected privacy in law as new technologies have emerged.”

⁹ For example, the Fair Information Practices of 1973 drafted by the U.S. Department of Health and Welfare, which led to the more international Organization of Economic Cooperation and Development (OECD) “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” in 1980. The Privacy Act of 1974 regulates the government’s ability to collect personal data, but not the private sector.

¹⁰ Such as Germany’s Federal Data Protection Act of 1977, Great Britain’s Data Protection Act of 1984, and the European Data Protection Directive drafted by the European Union in 1995. (95/46/EC)

¹¹ Although who is to say what Eleanor Roosevelt could have accomplished, given the time!

[Rotenberg, 2000 #74] This “reactive” history in regard to privacy protection explains why there are no laws on privacy that have been adopted for the Internet in the United States.

In Europe, on the other hand, the European Union, “saw the very important need to set up a global personal data protection system ... through directives, the most important being the 1995 directive on the protection of personal data. [Bégot, 2001 #43] Although the directive was not meant to deal directly with the Internet, Article 29 does specifically apply to privacy issues on the Net. It is important to note the following:

A directive is not a law, it is a ‘direction to Member States to enact law ... The Data Protection Directive balances the competing interests both directly, by mandating certain rules, and indirectly by permitting Member States to legislate accordingly. [Strauss, 2000 #44]

What does this tell us about privacy? In general, “The E.U. policy arguably procures a more stringent and regulated structure than that of the U.S.” [Strauss, 2000 #44] In a way, the Privacy Directives are a form of social standards – they are policy-based protections for consumer data and information privacy.

In the United States, traditionally standards have been used to help guide technology development, but in Europe, standards have more often been used for policy agents in the social sphere. [Cargill, 2001 #27; Cargill, 2001 #45] The European Privacy Directives are not statutes, but they are backed by legislative fiat. And with these privacy protections in place, how will they affect technological development? An interpretation of the Privacy Directives has already made the use of browser cookies illegal if, “the information is stored for any period longer than is necessary for the transmission and for traffic management purposes.” [Union, 2001 #49] It seems clear that a “federated identity” solution, such as that proposed by the Liberty Alliance, would not stand the test of these translations of 95/46/EC.

5.2. Policy – Market-based Solutions

Why doesn't privacy policy similar to the EU Privacy Directives exist in the United States?

“While the European privacy law is enforced proactively by the government and individuals have direct recourse through the judicial system, the U.S. counterpart calls for a system of self-regulation by the industries themselves.” [Strauss, 2000 #44]

Has market pressure worked to protect consumer privacy in the past? Three highly publicized cases of online privacy demonstrate how strongly the American public can react to these concerns.

1. **Intel Processor Serial Number.**

Intel had planned on burning a unique serial number into each Pentium III processor that could be accessed through software, and which, when first activated, would send information back to the company when online. The company thought that this would help them better serve their customers and provide secure transaction verification, but customers were afraid that Intel would use the Ids to track their online habits. Intel turned the software feature off by default.

2. **DoubleClick web usage tracking.**

DoubleClick announced plans to use browsing histories to deliver efficient and effective targeted banner ads to web users. But consumers demanded that Doubleclick provide this as an opt-in rather than opt-out service, and a public education campaign was started. [Weitzner, 2000 #51]

3. **Comcast cable network monitoring.**

It was revealed on Dave Farber's email listserv that Comcast cable was discovered to have been monitoring the IP addresses visited by their cable modem customers.¹² Although the company maintained that it was only using the information to provide input for how to best upgrade their network, and although they were not participating in any illegal activity due to the nature of their customer agreement forms, they stopped the storing the monitoring information altogether “in order to completely reassure our customers that the privacy of their information is secure.”¹³

¹² The original post can be found at: <http://www.interesting-people.org/archives/interesting-people/200202/msg00057.html>

¹³ A copy of the Associated Press article can be found at: <http://digitalmass.boston.com/news/2002/02/13/comcast.html>

We can see in all three cases an overwhelming concern for “information privacy” that was communicated to the companies. A fourth case gives us an example of voluntary restraint when the firm in question is a monopoly provider. In late 2001 Qwest Communications had planned on selling their customer data lists to advertising corporations, and had informed their customers that this would be an “opt-out” default policy. Even though they would likely have been granted the legal ability to do so under a commercial free speech defense,¹⁴ the amount of consumer pressure (and a threat to challenge the federal jurisdiction by the state of Arizona) was sufficient to convince the company to forego this exercise.

Given this kind of consumer response to potential privacy concerns, is it possible that firms attempting to become identity “trust brokers” will respond to the demands of the market? Thus far it appears as though market-based solutions are working. But why would they be more effective than regulatory or legislative protections, such as the Privacy Directives?

If we think of digital identity privacy as a property right, then if we gave the legal right to restrict the use of that property to the individual, what might the transaction costs be to the firms wanting to be identity providers? Declan McCullough speculates that the provider would tend to focus resources on providing extra security and ensuring legal compliance, possibly deterring innovation. On the other hand, if the provider has the right to use this digital identity information in whatever way they choose (within current legal guidelines), this may incent the creation of new services, such as privacy ratings, or tracking of security histories. In fact, we have already seen some new companies arise trying to fill the need for final “certificate authorities” (EnTrust and Verisign), and monitoring conformance to industry-wide privacy policies (BBBonline, TRUSTe, and WebTrust).[McCullagh, 2001 #53] This Coase Theorem

¹⁴ US West, the “Baby Bell” that Qwest purchased in 2000, had defended itself on these grounds and won in a 10th Circuit Court in 1999.

economic analysis indicates that regulating digital identity privacy might be less efficient than the current negotiated privacy brokering. Further support is supplied by the Consumer International report on Internet Privacy, which found that some of the best privacy policies were found on US web sites. [van Duifhuizen, 2001 #72]

5.3. Legal – Antitrust

One of the provisions of the Sherman Antitrust Act, part II, is that a monopolist is not permitted "to project its monopoly power into another market, *i.e.*, to 'exploit his dominant position in one market to expand his empire into the next'" *Eastman Kodak Co. v. Image Technical Service.* [, 2001 #38] This has been the basis for many of the complaints filed with the FTC in regard to Passport.

It is very likely that the decision in the Microsoft DOJ antitrust suit will significantly affect the legal landscape for the IT industry. However, despite the focus on WindowsXP and Passport in the filings under the invocation of the Tunney Act, there has been little indication that these components of their digital identity strategy will be included in the final remedy proposal.

Microsoft is also facing an antitrust suit in the European Union on counts of trying to monopolize the workgroup server market and illegally tying their Windows Media Player software to WindowsXP. But it appears as though the European courts are awaiting the final modified remedy proposal in the U.S. before proceeding with the case.

In short, there is little action in the U.S. courts at the moment to indicate there is any consensus or legitimacy behind a tangible threat of digital identity monopolization by Microsoft.

6 The Business Plan

We have thus far ignored the business logic. It is an interesting case of attempting to create a bottleneck and establish a monopoly that dictates the terms of participation in the Internet. To the companies involved in these efforts, it is nothing more than a natural transition from free

information to subscription-based services, much as advertiser-supported TV has an analog in the market for subscription-based cable and satellite services.

For Microsoft, the revenues will come from transaction and licensing fees. Sun, on the other hand, is betting on the identity and access market expanding and driving demand for their hardware and directory services software. In either case, we cannot say that demand for single sign-on convenience is being driven by consumer customers. Avivah Litan, a Gartner Group research director, noted in a widely quoted report, “Most consumers don’t see much relative value in having one credential to navigate the Web.”[Litan, 2001 #73] The tepid success of Microsoft in gaining Passport Partners indicates that there is not yet a great deal of value perceived by retailers. Sun is largely selling a business plan rather than a technology to the members of the Liberty Alliance – a technology is not even due until sometime in the summer of 2002.

Economic theory of network industries helps us understand why Microsoft tried to enter this market at such an early stage, and with a product whose security was suspect. Network externalities and “bandwagon effects” dictate that the greater the number of members in a network, the greater its relative value to those members. By taking losses in the short term, a company offering a new product may be able to drive demand and achieve a critical mass of customers quickly, also achieving positive feedback, and potentially locking in customers. The short-term losses are beneficial to consumers, who reap the benefits of the service offering. The provider, meanwhile, will tend to raise the fixed price to offset the early losses in the long term. The intent is that “the amount paid by each subscriber grows automatically over time as he or she uses the service and derives more benefits from this service.”[Rohlf, 2001 #121] Firms that enjoy substantial market power, in particular, can benefit most from first-mover advantages.

A net-value curve is a function of the network effects gained by the use of some technology. [Liebowitz, 1999 #122] A monopoly occurs when the curve is upward, and competition occurs when it slopes downward. However, if one particular technology has gained a critical mass of market share, users can be locked in and there will be no room for new entrants. (There may, however, be consumer preference variations that segment the market, and allow a dual-standard to co-exist.) Even if a superior technology is introduced by a new entrant, it will likely not be able to overcome the lock-in effects. Varian and Shapiro define the value of a customer base as equal to the sum of the cost per user to switch.[Shapiro, 1999 #120] The cost per consumer to switch from Passport to the Liberty product, however, may be zero. Nevertheless, small switching costs can still function as large barriers: telephone number portability is a classic example.

Microsoft introduced Passport in 1999 and claims over 200 million users, and 30 billion transactions (site log in, express purchase, Hotmail sign in, etc.) per month. Microsoft also enjoys a 93% market share for desktop operating systems, a 96% market share in office productivity suit software, and a 85% market share for internet browsers, according to IDC market reports. They have made significant investments in developing Windows CE.Net, their handheld and embedded operating system, for PDAs, set-top boxes, cell phones, and tablet computers or other internet appliance-type devices. They also released the Xbox gaming console in late 2001; signing up to play online games through the device requires a Passport account. The first-mover strategy has allowed them to populate Passport with the users of these various products. Although they will have to focus on providing disincentives to switching in order to maintain market dominance, the longer it takes the Liberty Alliance product (or other

alternatives) to come to market, the greater the potential for Passport to achieve critical mass. Conversely, the incentive to interconnect will decrease.

Even if the Web services market doesn't pan out, going the way of Web Portals, CORBA, push technologies, "convergence," and the dodo, Microsoft will still own and control a highly desirable database of user information. Twice in the past year, Jim Allchin, a Microsoft VP in charge of Windows and server software development, has admitted that the business plan for offering Web services is "not figured out." [Ricciuti, 2002 #128; Wong, 2001 #127] A report by the Gartner Group indicates that Microsoft may be having more trouble with their culture change from a software company to a services company than they let on. [Bittman, 2002 #134] If the business plan fails, how might Microsoft look to recoup their losses? Selling that user information sure starts to look like an intriguing idea.

7 Conclusions

To the users and the consumers, this is a world in which companies have access to an extraordinary amount of personal information, habits, and preferences. With the promise of great reward and utility comes the risk of absolute abuse.

We have seen that Microsoft has been able to attain a near-critical mass of customers. We have seen that there are proprietary extensions and technological dependencies between their products. We have seen that there is a history of relying on these strategies to lock customers in and grow market share. But we have also seen that rational businesses will respond to the marketplace demands, even in the case where there is no threat of litigation, and even in the case where a provider may own a monopoly. We have seen that certain industries, especially those that enjoy long standing relationships based on trust (such as banks and brokerages) and established billing arrangements (such as wireless providers), have been sufficiently worried about the threat of disintermediation by Microsoft to band together and commit to the

development of an alternative. Collectively, these members of the Liberty Alliance have committed to a federated model. They also own somewhere between one and two billion identities. Do these conditions indicate that the marketplace is healthy, and there will likely be choice and public welfare?

I propose that the digital identity access and management marketplace will be divided into high and low transaction segments. The differentiator will be the volume of transactions handled by each service provider. Each market segment will have their own de facto standard: Microsoft Passport for the low end, and the Liberty Alliance, or some other interoperable alternative, for the high end.¹⁵

Companies wanting to offer Web services and charge for them need to have a way to bill their customers for access to their product. This will be the primary driver for having an identity management system strategy. The potential benefits to these service providers include reduced fraud, greater knowledge of their customers, reduced integration and infrastructure costs, and new business opportunities. Choosing an identity provider partner or a technology set to implement will involve prioritizing and evaluating five key criteria: security, question of ownership, liability, technology lock-in, and the ability to deliver.

I demonstrate in Figure 9 how a high volume transaction service provider will place greater value on the question of ownership, and most likely choose an open standards-based system, such as that proposed by the Liberty Alliance. A low volume transaction provider may be more interested in the transfer of liability for fraud to an identity provider, and choose Microsoft Passport.

¹⁵ This conclusion is based on an assumption that there will be no interoperability between these identity systems in the short term.

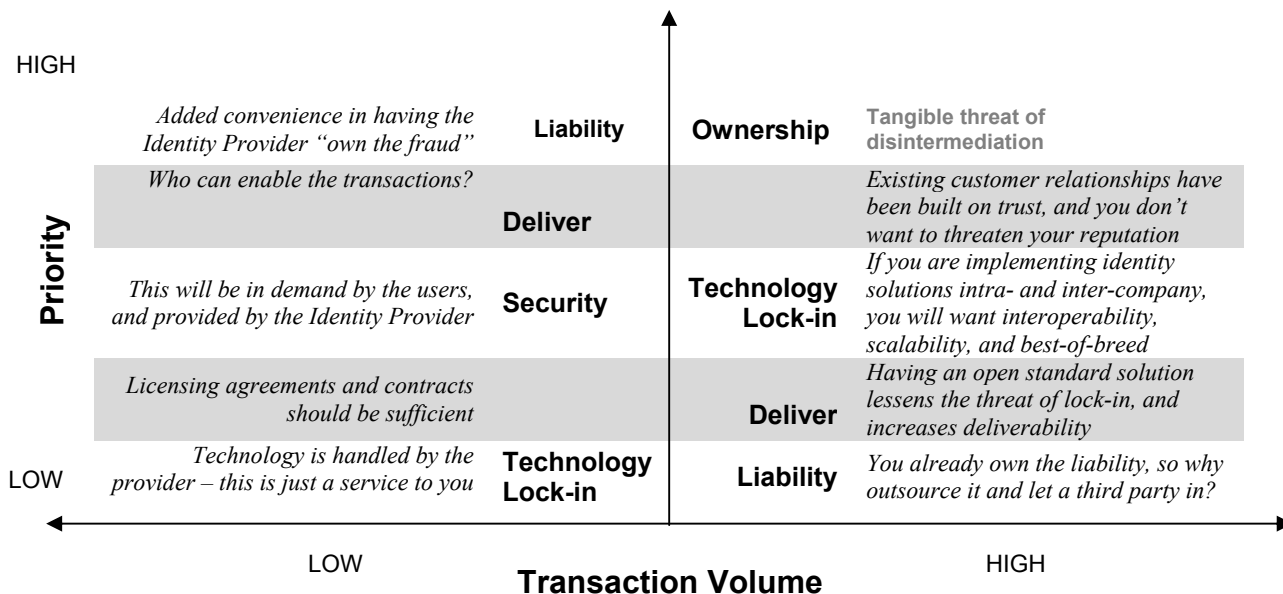


Figure 9: How to choose an identity provider?

Although I conclude that there will not be one dominant or monopoly provider for identity services, I also submit that the striated market will feature monopoly providers in each segment. The illusion will be that consumers enjoy a choice of providers, but the reality is that there will be two monopolies coexisting without any incentives to interoperate.

Even so, Microsoft will feel continuous pressure from their Passport Partners to guarantee their claims of liability ownership. The members of the Liberty Alliance will have made their choice to avoid Passport because they already have trusted relationships with their customers and do not want them to be jeopardized. Therefore, even though each market segment will probably be monopolized, there is little threat of that monopoly power being used to violate consumer privacy. Though the market for identity-based services may experience or demonstrate other inefficiencies associated with artificial scarcity, the privacy rights and preferences of the users will likely remain unaffected.

Finally, it is also possible that another scenario will play itself out. If identity information becomes more and more a commodity, perhaps the relationship that dictates the terms of “federated” trust brokering will evolve like that of peering relationships between Tier 1 backbone providers for the Internet. Smaller identity provider organizations could also participate in the game, but only according to the terms of the Tier 1 identity holders. “An identity is an identity is an identity” is probably too value-laden as a concept to match up with “a bit is a bit is a bit,” but it may be a natural outgrowth from *Cogito ergo sum* to “I am coded, therefore I am.”

References