CATAVAULT SM

All Access Pass to the Internet

Open Sesame White Paper
Online Identification & Authentication Federations

Revised - January 2002

Overview – It's All About Interoperability

Given the high profile interest in universal authentication platforms by players such as AOL with its Magic Carpet initiative, Catavault with its All Access Alliance initiative, Microsoft with its .Net My Services initiative and the Liberty Alliance initiative started by Sun, Catavault recently held an industry seminar for its key clients to discuss the role and implications of "federated functionality" in terms of online identification and authentication. While there are currently multiple federations forming, this White Paper, resulting from the seminar, argues that the lynchpin for success with real world online identification and authentication federation(s) rests with real world business interoperability much more so than technological interoperability. Authentication and federation service providers need to be extremely sensitive to business issues because of the proprietary and sensitive nature of customer data. Accordingly, businesses in general are reticent about sharing customer data because it is considered the "holy grail," and when it comes to sharing customer data in the digital age across networks with third parties, some of which are competitors, those concerns are greatly heightened.

In order to understand why business interoperability issues and their associated business models are paramount, this White Paper will briefly address:

1) the historical framework necessitating online identification and authentication services.
2) the various approaches that have been discussed to date.
3) the various analogies, research and challenges that confront "federated" online identification and authentication services.
4) the recommended action steps that need to be taken in order to successfully attain universal authentication across federated networks.

Historical Framework - ATMs

The proliferation of user names, PINs (personal identification numbers) and passwords (collectively referred to as "Authentication Credentials" hereafter) is a relatively recent phenomenon stemming from the tremendous growth of high technology dating back to the mid-1980s. Many consumers received their first PIN in the 1980s when they received their first ATM (automated teller machines) card. At that time, consumers were often randomly assigned four digit PINs, yet sometimes they could request a personalized PIN, depending whether their bank offered that customization option.

The days of remembering just one or two Authentication Credentials for all applications did not last very long. Given the short time period that it took to gain widespread penetration and usage of ATMs, banks aggressively promoted bank-by-phone services. In some circumstances, banking by phone utilized a consumer's existing ATM PIN, however, sometimes consumers needed to get another PIN. With the advent of many new high tech products and services during the past twenty years, including, for example, computerized banking, wireline and wireless telecommunications and primarily the Internet, consumers have witnessed a proliferation of services and applications, both offline and online, that require unique Authentication Credentials.

Historical Framework – The Internet

The need for common online identification and authentication services arose from the open, democratic nature of the Web. Many Web sites, services and applications (collectively referred to as "Sites" hereafter) require that users register to view the site through a unique set of Authentication Credentials. In the absence of a standard authentication procedure, Sites independently created their own requirements for access. Technology, and not common sense, provided most of the rules for formatting; thus causing some Sites to use minimum and maximum character length, some Sites to use case sensitive parameters and/or some Sites to require a combination of letters and numbers. *The New York Times*, for example, requires a Member ID of five to fifteen characters, and a password that is a minimum of five characters in length.[1] For American Express, the rules are more stringent for its User ID:

- Must be greater than 5 characters in length.
- Must contain at least one letter.
- Must not contain spaces.

And that's just for the User ID. The password for American Express:

- Must be between six and eight characters in length.
- Must contain at least one letter and one number.
- Must not contain spaces or special characters.[2]

With thousands of Sites, each one demanding a different format, there was a clear need for solutions that would create an "open sesame" for the Web. This open sesame solution serves as a master key that would unlock most, if not all, of the doors that people are enabled to access on a daily basis, and free them from the cumbersome task of managing and using their Authentication Credentials each time that they visit various Sites.

Boston Globe columnist John Powers articulated the problem of disconnected silos of content, commerce and application Web sites: "I am the Man of 1,000 Passwords, and I'll be damned if I can remember more than three of them. Actually, I can remember more than three. I just can't remember which goes with what. Is **** the password for my Fidelity account or my Marriott Rewards account or my United Airlines Mileage Plus account? And I won't even talk about personal identification numbers."[3]

Password Panaceas

Just as the open nature of the Web was responsible for the lack of a unified authentication system, so too has it spawned the solutions to cure consumers of "password-itis" which is caused by "registration rage" and "invalid login frustration." In typical Internet fashion, a variety of services have been created, offering various forms of user experiences, processes, business models, etc. Various approaches and terminology have been used in the sector to describe different businesses including: aggregators; e-wallets; form fillers; online identity and authentication services; redirect providers; single sign-on services; etc. Specifically, technological solution providers such as AOL, Catavault, ezlogin, Gator, In1Place.com, Katmango, Microsoft Passport, Obongo, VerticalOne and Yodlee, among others, were developed since there were a whole host of unorganized suppliers - Sites - requiring Authentication Credentials.

As the identification and authentication services which are still operational (some have been acquired while others have gone out of business) begin to interoperate with the developing federations and various third party Sites, it is paramount that all of the constituents work in concert with one another, even with competitors, in educating consumers of the utility that will be derived from authentication services and federations that cure "password-itis."

Fundamental Tenets – Universal Authentication

There is general agreement among various authentication services and federated approaches that the universal authentication model is built on the cornerstones of enabling consumers access to their vital information with any device, at anytime, from anyplace, with any band, and through any protocol enabled over a network. Moreover, the technological cornerstones of a universal authentication model are based on providing a secure, private, scalable, reliable, available, flexible and individualized service to consumer and business users. However, much more attention absolutely needs to be focused on business models and how constituents will make money. Business models are a paramount concern since the promise of financial rewards will drive the successful implementation of single sign-on in a federated framework. As such, technology will be the underpinnings of business interoperability and business models, and this approach needs to be emphasized by the forming federations if they hope to turn words into action. Thus, business issues need to drive technology and not vice-versa.

Distributed Authentication

The distributed computing environment in which consumers can access the Internet with any device has led to a distributed identification and authentication environment. As such, in a Web-based software-as-a-service world, online identification and authentication is emerging as the "key" to the Internet. Case in point, players such as AOL, Catavault, Microsoft and Sun are all perceived to want to control their customer data, directly or indirectly, and reinforce their position as the "gateway" to the Internet, directly or indirectly, with these new federated middleware solutions.

In discussing the future of online identification and authentication, various pundits have brainstormed regarding the development of "open" and "federated" technology standards rather than the development and endorsement of specific technologies or services. However, it is important to understand that while the development of these federated standards is arguably critical to the future of this nascent sector, there will most likely continue to be centralized authentication services by AOL and Microsoft, for example, possibly using some/all of the open standards developed by the various federations which are forming.

Today's Authentication Solutions Transcend Tomorrow's Federated Goals

Today, the dominant online identification and authentication processes that have arisen entail:

- **Authenticated links enabled over a network:**
  - **Authentication service to third party site –** For example, when a consumer wants to visit Yahoo! Mail, he/she can request that his/her corresponding Authentication Credentials which are encrypted and stored within the master database of a service such as Catavault or Obongo are sent to Yahoo! Mail in order to log onto that site.
  - **Third party site to authentication service, back to third party site** - For example, when a consumer visits Starbucks.com and wants to purchase coffee online, the consumer is identified and authenticated through Microsoft's .Net Passport and "redirected" back to Starbucks.com.

Tomorrow, in a federated framework, the processes above transcend:

- **Site-to-site authenticated linking and peering enabled over a network:**
  - **Authentication service to third party site, and to other third party site(s)** - For example, when a consumer wants to visit Yahoo! Mail, he/she can request that his/her corresponding Authentication Credentials which are encrypted and stored within the master database of Catavault or Obongo are sent to Yahoo! Mail in order to log onto that site. Then, in theory, the consumer may be able to go to Hotmail and log into Hotmail using the corresponding identity ticket from Yahoo! Mail and the authentication service

and/or the federation. Given the competitive nature among Hotmail and Yahoo! Mail, it is easy to see how a federated framework will be challenged in terms of successful implementation.

- **Third party site to authentication service, back to third party site, and to other third party site(s) -** For example, when a consumer visits Starbucks.com and wants to purchase coffee online, the consumer is identified and authenticated through Microsoft's .Net Passport and "redirected" back to Starbucks.com. Then the consumer would be able to go to Hotmail in theory and log into Hotmail using the corresponding identity ticket from Starbucks.com. The consumer could then go from Hotmail to Yahoo! Mail and be logged in based on the original identity ticket from Starbucks.com. Given the competitive nature among Hotmail and Yahoo! Mail, it is easy to see how a federated framework will be challenged in terms of successful implementation.

ATM Analogy – A Lack of Short-term Interoperability & High Fees

Since September 2001, companies such as Microsoft have unofficially invited third parties to participate in the creation of an "Internet trust network" that will function in a similar manner to the ATM network in the financial services industry. While this ATM analogy seems plausible in theory, one would be remiss in not addressing the practical shortcomings of the ATM network comparison because of some primary issues: 1) the long time period for ATMs to become ubiquitous and interoperable, and 2) the resulting high costs of ATM usage passed onto consumers who have become dependent on ATMs.

Given the historical context previously discussed with ATMs providing consumers with their first PIN, one also has to remember that when ATMs were originally introduced, interoperability, or the lack thereof, was big issue between various bank ATMs offering differing services such as Girard Bank's "George" and Bank of America's "Versateller." Accordingly, one was most likely unable to use competing bank's ATMs because of nascent, disparate, emerging and geographically dispersed networks such as Cirrus, NYCE, and Plus. Moreover, the business interoperability issues such as ownership of the account holder relationship precluded various banks from working together. While technical interoperability issues were solved over time, consumers liked the convenience afforded by ATMs which were becoming much more ubiquitous, and consequently consumers became dependent on ATMs. As such, when financial services institutions started limiting the number of monthly transactions and charging excessive fees for using "foreign" ATMs from another bank, consumers were harmed.

The "federated" approaches outlined by Microsoft's Internet trust network and Sun's Liberty Alliance are very ambitious, and as such, consumer choice and technological innovation may benefit in the long-run. However, ambitious initiatives such as multiple federations take a long time to implement and may already be technologically grounded with unilaterally set standards that may or may not be acceptable to competitive businesses, Sites, authentication services and federations. Additionally, as larger players set their goals on dominating the online identification and authentication sector, smaller companies will arguably find it harder to secure funding, access distribution channels, acquire customers and compete; thus, technological innovation may be stifled which in turn may cause consumer harm with more limited choices. The consequence to the average consumer is that there will be a time lag for any federated solution to provide real consumer utility across a broad number of third party Sites. Moreover, just as banks started charging its account holders high ATM fees, the same is arguably true in the online identification and authentication sector. For example, "Microsoft is betting that consumers find passwords and data access so painful that they will pay for tools that let them regain control. The company said it will charge between $20 and $40 a year for core HailStorm [renamed .Net My Services] services such as identity management and electronic alerts."[4]

In the absence of ubiquitous and integrated networks in these identification and authentication federated solutions, third party service providers, Sites and authentication services should follow the leadership position in online identity and authentication similar to AOL, "…because Liberty Alliance is not a centrally-controlled system, AOL and other companies can continue to enhance their existing authentication and identity services and develop new services," stated Barry Schuler, Chairman and CEO, America Online, Inc.[5]

Federations of Solar Systems – Decentralized Affiliations

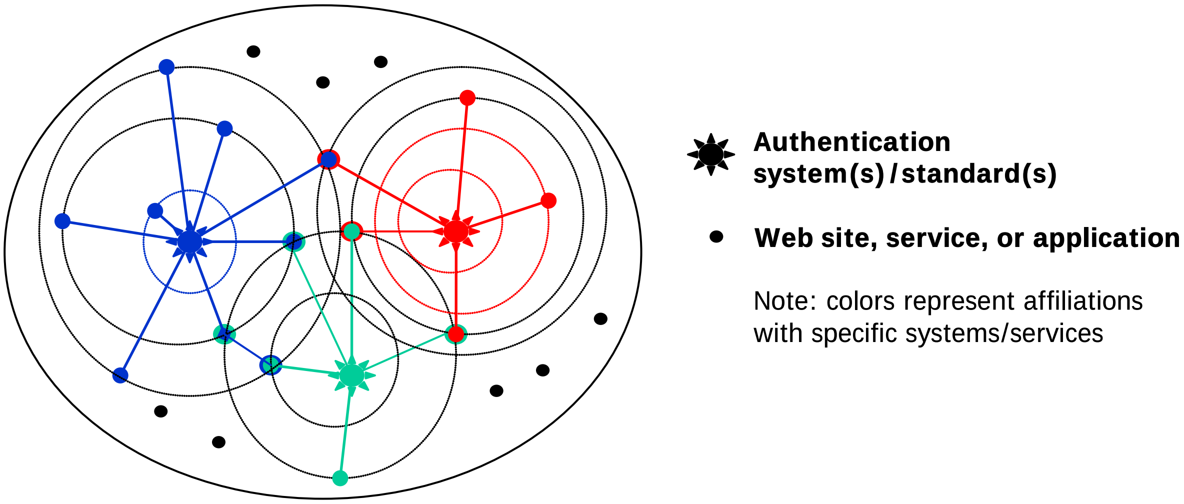
In reviewing the definitions of the term "federate" and "federation," one can see various meanings including "the formation of a political unity, with a central government by a number of separate states." Using that singular definition, it is unclear which company or organization would serve as the “central government,” and one does not have to be an industry pundit to know that neither AOL nor Microsoft will acquiesce with alacrity to having its archrival serve as the “central government” or authority in online identification and authentication. Additionally, favoritism may prevail. For example, it is a safe assumption that MapQuest will receive more favorable treatment by AOL’s Magic Carpet initiative than Rand McNally because AOL operates MapQuest. Thus, while it is technologically possible to chart an Authentication Credentials mapping database in a federated framework across Sites, business issues will be that much more critical in order to provide consumers with utility in accessing a compelling plurality of third party Sites which will ideally interoperate transparently to consumers.

Today, the federated framework is very loosely defined and slowly evolving by “name space providers,” companies such as American Express and eBay which have large installed user bases. Most interested parties recognize the need for universal authentication because their customers just simply cannot remember all of their Authentication Credentials, and thus suffer from “password-itis.”

With the online identification and authentication market potentially evolving from a large host of unorganized Sites and fragmented alliances of Sites requiring Authentication Credentials to several federations of authentication services, one needs to understand all of the complex business relationships in order to avoid continued fragmentation. For example, as various federations form, the universe of third party Sites that require identification and authentication will consist of multiple “solar systems” containing third party Sites. Essentially these third party Sites are represented as sets and subsets of data. Each solar system may contain at least one third party site that “orbits” around, in other words, functions with, the solar system’s centralized star or sun.

The centralized sun or star is analogous to various processes, standards, technologies, specifications, and/or agreements used with respect to identification and authentication. Additionally, in terms of identification and authentication interoperability, Sites can also be represented in one or more solar system and function in and with one or more solar system. Please see Figure 1 for more information. For example, eBay has taken an industry leading approach in offering multiple sign-in options: 1) sign-in directly using their eBay User ID and eBay Password or 2) sign-in with Microsoft’s .Net Passport. Additionally, eBay has also joined the Liberty Alliance which signals that it intends to offer online identification and authentication alternative(s). Today, when a consumer visits "my eBay," the right column header above the .Net Passport sign-in option states, "Or sign in with other services:"[6] This is a positive harbinger for consumer choice as multiple authentication service providers and federations form and are implemented by market leading early adopters such as eBay.

Figure 1
Authentication Services Interoperating Across Federated Solar Systems of Sites


✸ Authentication system(s)/standard(s)
● Web site, service, or application
Note: colors represent affiliations with specific systems/services

With respect to identification and authentication, some solar systems use heterogeneous or homogeneous processes, standards, technologies, specifications, and/or agreements. The various solar systems may be formed by multiple groupings that are included in union(s) and intersection(s) of individual third party Sites. There are complementary and competitive processes, standards, technologies, specifications and/or agreements that Sites may implement by themselves or in conjunction with other Sites within their particular solar systems and with Sites in different solar systems. Individual solar systems may provide dominant processes, standards, technologies, specifications and/or agreements on which other solar systems are dependent, directly, indirectly, in whole, and/or in part. Additionally, individual Sites may implement multiple processes, standards, technologies, specifications and/or agreements that can connect a specific site's users with Sites that are members of its solar system and other solar system(s).

Business Interoperability

Business interoperability issues come into play in constructing the aforementioned federated solar systems. For example, in theory, the Liberty Alliance should enable a consumer to be authenticated at AmericanExpress.com to view his Gold Card balance and then be authenticated at eBay's site across its federated framework. While this is technologically possible and operationally reasonable to believe, what happens when that same consumer then goes from eBay and visits Bank of America's Web site to check on his MasterCard bill? Will that same authentication chain or "identity ticket" that originated at American Express, in conjunction with the authentication service and/or federation, log the consumer onto American Express' competitor(s) such as Bank of America and MasterCard? Arguably speaking, American Express will have strong concerns about sharing data in a "chain of custody" like this, but one can see how quickly this tangled Web of federated authentication will become across Sites and businesses that may compete with one another.

Alternatively, let’s say a consumer logs onto Hotmail with .Net Passport to check his email. From there, the consumer visits Expedia and is authenticated accordingly with the federated chain from .Net Passport to check airfares travelling from Seattle to Dulles. After seeing really high rates on Expedia, the consumer then wants to check the fares on Travelocity. Will the same authentication chain or identity ticket that originated with Hotmail log the consumer onto Expedia’s primary competitor? Arguably speaking, again, it is difficult to imagine a real world implementation among online travel archrivals like this. Moreover, even if Microsoft accepts the “olive branch” extended by the Liberty Alliance and joins AOL and Sun in the Liberty Alliance, the fact is that there will be many technological issues that still need to be addressed. Even in this hard to imagine scenario, business interoperability issues will be even more paramount as the titans vie for control, technologically, operationally, and financially, and as such, these issues may handicap any real site-to-site functionality across Sites and federations.

United States Passport Analogy

The business rationale of a universal authentication network is based on the fact that consumer utility should not be a function limited only to the number of affiliated Sites like the Microsoft .Net Passport model.

For example, imagine if your United States Passport only allowed you to travel to the United Kingdom, but not to France. Furthermore, imagine if your United States Passport only let you travel back to the United States via O’Hare and not through LAX. And to make matters more complicated, imagine if your United States Passport only let you travel via United Airlines. This would not provide American citizens with great utility, and it would cause frustration and limited international travel until such time as restrictions were removed and/or alternative identification approaches with greater utility emerged.

With respect to virtual travel with online identity and authentication, services such as Catavault, Gator and Yodlee work with both affiliated Sites, like Passport’s model, as well as non-affiliated Sites, unlike Passport’s model. The open model of working with both affiliated and non-affiliated Sites has been arguably very important in terms of providing maximum utility to consumers; this utility has helped drive adoption and usage of those services embracing that approach.

Decentralized Federated Framework

Given that there could be multiple federations of password “solar systems” forming, it is paramount to create a “common denominator” identification and authentication linkage for the universe of multiple solar systems and their respective third party Sites, as well as Sites that are independent of various federated solar systems. This will be accomplished by providing a “decentralized” framework for authenticating users across individual Sites that exist in the series of distinct and sometimes overlapping solar systems described herein. These solar systems and their third party site members may or may not in fact share various data points (consumer information) with each other based on established processes, standards, technologies, specifications and/or agreements. The depth and breadth of information which they share will be largely dependent on the successful implementation of real world business interoperability issues.

Federated Site-to-Site Authenticated Linking & Peering

In this view of linking multiple federated solar systems together, it is also paramount to enable or restrict identification and authentication of users across two or more different, distinct or overlapping Sites in one or more solar systems. Essentially, this would be site-to-site authenticated linking and peering enabled over a network. This common denominator approach offers interoperable methods, processes, techniques, specifications and/or agreements of establishing “associated” networks of third party Sites to identify and authenticate users across otherwise non-affiliated Sites.

Market Research - Gartner Survey

The following are excerpts from a Gartner survey on public opinion of Passport as it pertains to Microsoft’s .Net My Services initiative (formerly known as HailStorm). The August 2001 survey indicated:

- "Consumers are much more interested in Passport's basic feature - single-sign-on - than they are in personalized web services that will be offered by Hailstorm and enabled through Passport."
- "Microsoft will be severely limited in its ability to provide single-sign-on to consumers since it has to wait for e-tailers and other destination Web sites to integrate Passport into their Web Platform."[7]

Case in point, it is critical to the success of multiple solar system federations, that the opportunity exists to launch interoperable services that:

- Provides consumers what they want...a single sign-on solution that works at all their favorite Sites, and
- Empowers Sites and businesses with what they need - a more turnkey means of implementing an identification and authentication service into their Web Platform with the caveat of understanding their business issues and needs, especially as it pertains to customer data and competitive concerns.

Challenges to Implementing a Federated Approach

In addition to various market research as to consumer and business needs, Sites, authentication services and federations may be able to agree to technological interoperability, but the most paramount issues will involve business interoperability. For example, while the principles below are common sense, it is nonetheless necessary to address them so that all interested constituents can work together to attain the ideal password panacea derived from federated frameworks:

- Reconciling the discrepancy between a centralized system with, for example, .Net Passport and the proposed decentralized system with, for example, the Internet trust network by Microsoft.
- Appreciating that customer data is the “holy grail” of most businesses.
- Understanding that businesses do not like sharing data, especially about customers, and potentially with competitors.
- Recognizing that both competitive and complementary businesses generally do not cooperate with one another.
- Recognizing that technology will be the underpinnings of business interoperability and business models, and this approach needs to be emphasized by the forming federations if they hope to turn words into action, and in sum, business must drive technology.

- Earning trust among businesses potentially sharing data and earning faith among consumers to entrust various businesses with their personal information in a digital age.
- Recognizing that the various industry experts including the press and analysts perceive the Liberty Alliance as a Sun versus Microsoft fight that has now attracted the interest of AOL into joining the Liberty Alliance as part of its battles against Microsoft.
- Migrating from proprietary identification and authentication standards such as AOL Screen Name or Passport to industry processes, standards, specifications, technologies and/or agreements.
- Getting third party Sites to dedicate the resources in a timely manner to adopt new industry processes, standards, technologies, specifications and/or agreements.
- Providing tangible business incentives to third party Sites to integrate new industry processes, standards, technologies, specifications, and/or agreements to foster both business and technological interoperability in a federated framework.
- Fostering and sustaining a “crawl, walk, run” development road map to allow for the time lag for these new industry processes, standards, technologies, specifications, and/or agreements to be developed and implemented by third party Sites in a federated solar system model.
- Creating common definitions, understanding and usage of various terminology that has been bantered about by various third parties and industry pundits in an inconsistent and confusing manner. For example, various terminology has recently been applied to describe different methodologies and processes of online identification and authentication, both in use currently and in development for the future, including: federated vs. non-federated; centralized vs. decentralized; open vs. closed; affiliated vs. non-affiliated; participating vs. non-participating; proprietary vs. non-proprietary; exclusive vs. non-exclusive; etc.

Recommended Action Steps

Based on the analysis herein, following are some of the top-level recommended action steps for authentication services, Sites, businesses and emerging federations:

- Supporting the principle voiced by AOL that companies should continue to enhance their existing authentication and identity services and develop new services.
- Creating business models and financial rewards since the promise of financial upside will drive the successful implementation of single sign-on in a federated framework.
- Securing additional market leader early adopters such as eBay to offer consumers choices in terms of online identification and authentication.
- Ensuring that name space providers work in concert with existing and new authentication services and federations to ensure that both technological and business interoperability issues are adequately addressed.
- Addressing consumer needs in terms of real world issues such as, will you be able to use your .Net Passport to login to Yahoo! Mail, a competitor of Microsoft Hotmail? Alternatively, will you be able to use your AOL Screen Name to log into your Hotmail account, a competitor of AOL?
- Educating consumers that they control their own security and more often than not, they are the weakest link in the security chain since no amount of technical security can prevent a user from scribbling a password on a sticky note and posting it on a monitor where others can see it.
- Educating consumers that Sites operating in a federated framework do not necessarily share the same privacy policies when it comes to the use of customer information, even though the

authentication chain may work transparently to the consumer instilling a belief that the Sites work with one another in terms of authentication and privacy policies.

- Communicating to consumers the utility that they can derive from authentication services and federations that cure "password-itis" which is caused by "registration rage" and "invalid login frustration."
- Establishing integrity over time by both businesses and consumers in a "trusted" framework of data exchange enabled over a network.
- Recognizing that even with best industry intentions, there will still be competitive choices, just as there are with payment services such as American Express and Visa.
- Recognizing that there are those individual third party Sites which will not want to join one or more authentication services and/or federations. For those particular third party Sites and federations, interoperability is still an issue since the value of any authentication service and federation to a particular consumer is a function of that person being able to access the Sites that he/she wants to access, regardless of that individual site's affiliations with third party authentication service(s) and/or federation(s).

Conclusion

Just like the ATMs were not a magical panacea to the financial services industry in terms of solving the ailing banking industry problems by eliminating the costs associated with expensive bank branches and the like, federated authentication services are not the magical password panacea either in solving "password-itis." The lynchpin for success with online identification and authentication federations rests with real world business interoperability much more so than technological interoperability. Moreover, developing new business models that are tangible and attainable will drive the successful implementation of single sign-on in a federated framework.

Authentication and federation service providers need to also be extremely sensitive to business issues because of the proprietary and sensitive nature of customer data. Accordingly, businesses in general are reticent about sharing customer data because it is considered the "holy grail," and when it comes to sharing customer data in the digital age across networks with third parties, some of which are competitors, those concerns are greatly heightened.

Given all of the high profile attention on this emerging sector, it is important to recognize that it is incumbent on the industry to attain small wins along the product development roadmap, all while being cognizant of the market opportunities, challenges and action steps articulated herein. If the stars align in the federated solar systems, even partially, the financial rewards could be very huge to consumers, Sites, authentication services and federations alike.

For more information about licensing Catavault's technology, retaining Catavault's consulting services on online identification and authentication, or to learn more about Open Sesame, contact Dan Trotzer, Catavault's Director of Marketing and Business Development, via phone at 610.941.3388 or via email at dan@catavault.com.

[1] www.nytimes.com
[2] www.americanexpress.com
[3] "In Person: Number Crunched," Powers, John, The Boston Globe Magazine, July 2, 2000.
[4] "Gates's Bold New Persona: Your ID Manager," The Washington Post, March 29, 2001.

[5] AOL Press Release, “America Online Joins Liberty Alliance as Charter Member; Federated Approach Will Help Ensure Consumer Choice, Promote Competition While Protecting Privacy and Security,” December 4, 2001.

[6] www.ebay.com

[7] http://www3.gartner.com/5_about/press_releases/2001/pr20010823a.html