LIBERTY
ALLIANCE
PROJECT

Business Benefits of Federated Identity

April, 2003

http://www.projectliberty.org/

Abstract:

This paper provides a brief overview of the benefits that implementing the Liberty Alliance's federated network identity management architecture can offer to businesses. The Liberty Alliance's vision is one of a networked world in which individuals and businesses can more easily interact with one another, while respecting the privacy and security of shared identity information.

1.0 Executive Summary

Web service development represents a burgeoning market opportunity that promises to:

- Bring substantial cost savings to enterprises in every industry.
- Bring revenue opportunities for service providers.
- Provide greater convenience and dynamic offerings for consumers.

At the core of this web service revolution is the concept of identity management, and the market's need for a global standard that is open, interoperable, and decentralized. In addition, it must allow for privacy safeguards across all markets.

The Liberty Alliance Project was established to address this need. Our goal is to develop standards for federated identity implementations that will allow companies to realize substantial business benefits, including:

- Revenue growth through development of strategic offerings
- Cost avoidance, cost reduction, and increased operational efficiencies
- Stronger security and risk management
- Interoperability and decreased time of development

The Liberty Alliance consists of over 160 leading organizations across the globe. Participants include companies in finance, wireless services, telecommunications, security, transportation, and infrastructure technology, as well as several universities, governments, and consumer advocate organizations.

2.0 The Current Environment

In today's economy, burgeoning e-business, outsourcing, and partnership arrangements have dramatically increased the importance of sharing information between businesses and their customers and partners. This has also impacted the amount of information that must be shared and highlighted the importance of adhering to emerging privacy standards and data regulations. The Internet computing challenge has shifted from interconnecting computers to interconnecting applications and services, all of which must be delivered to a growing number of people on an exploding number of devices and access points.

Identity is at the core of any business or data transaction. It is a critical component of the operations of any enterprise, and is interwoven into most business processes, including granting access to information and systems, enabling Customer Relationship Management (CRM) systems, and driving relationships with business partners and suppliers. Besides just presenting credentials for authenticated access to systems and services, an identity includes attributes that make for more targeted and productive use of these systems.

2.1 The Problem

Ineffective identity management is not only costly, inefficient, and prohibitive to new revenue opportunities, it is also a barrier to establishment of trusted business relationships. This “crisis” affects a company’s management of identities at all levels:

- Customer identities
- Employee and contractor identities
- Business partner and supply chain identities

Add into the mix the need to manage these identities across multiple devices and the problem multiplies. Ineffective identity management plagues all organizations on a global basis.

The previously accepted business model for identity and resource management was to limit access to valuable data in the name of security by focusing on keeping the “bad guys” (hackers) out. This was typically accomplished by designing closed and proprietary systems.

The new model calls for an interoperable and decentralized architecture that focuses more on letting the “good guys” (authenticated and trusted employees, customers, and business partners) in, allowing them to access targeted information and web services. Doing so, however, is no simple task, especially when you consider that many businesses already have substantial investments in diverse systems for identity and application management as a result of mergers and acquisitions or piecemeal IT planning.

Furthermore, as companies become more virtual and face greater demands to be less internally focused, they are increasingly challenged to grant access to services and applications to the right people at the right time without sacrificing security or scalability. One means of increasing efficiency is the implementation of a simplified or single sign-on for access to services and applications. This reduces the need for users to remember and re-key a myriad of username/password credentials, which provides an easier user experience while at the same time reducing IT administration and help desk costs. While password-based secure access to services or resources has existed for years, the ability for a user to access services from multiple domains within an enterprise or across multiple companies has remained a challenge that has forced individuals to maintain countless account credentials, thereby limiting the value of services that they receive.

2.2 The Solution

Fortunately, there is an answer to this crisis: *federated network identity management*. Federated identity management makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains. For this concept to become a reality, however, there needs to be a common set of technical and business standards. Without such standards for federated identity, businesses would continue to be held back by many business challenges, such as:

- Inefficient, insecure, and expensive enterprise identity management
- Lack of streamlined visibility and partner access across a business-to-business value chain
- Impediments to the delivery of bundled, context-sensitive services to end-users

The desire of businesses in virtually every industry to develop and deliver federated identity services to address these challenges has rapidly emerged as a strategic imperative. The IT industry analyst firm IDC estimates that up to 60% of the identities in enterprise directories or databases may be expired or "orphan" accounts. This presents a major security risk, in addition to creating an unnecessary IT burden. In addition, according to projections from IDC, the total value of the market for enterprise, business-to-business, and consumer web services will reach $21 billion (USD)[1]. To date, however, only 5% of companies have completed such projects; although 80% expect to have these projects underway by 2008[2]. Clearly, there is a great deal of opportunity in the future.

Good Privacy is Good Business

37% of users would be "a lot" more inclined to make a purchase on a web site that has a privacy policy (Business Week, 3/00), and 68% of people cite privacy and security as the top factor that would convert them from researchers into buyers.
(Jupiter, 6/99).[1]

[1] TRUSTe.org website

However, a definite impediment remains. One of the gating factors for identity-based web service development has been the lack of coherent standards and business and policy guidelines that will allow the deployment of meaningful web services. ***The Liberty Alliance Project was formed to address this void.***

By implementing products and technologies that support the Liberty federated identity systems protocols, a business can capitalize on the promise of web services while gaining greater efficiency with IT expenditures. It can realize new revenue opportunities with its business partners, and expand its product and service offerings to its customers.

[1] IDC, U.S. Web Services Market Analysis, February 2003

[2] IDC, U.S. Web Services Market Analysis, February 2003.

3.0 The Need for The Liberty Alliance and Federated Identity Management

The Liberty Alliance was established in December of 2001 by 16 companies with a common goal of creating open, interoperable standards and guidelines for federated identity management that can meet all of the current and future business challenges. The Liberty Alliance is the only global, cross-industry standards effort that is working to address these business challenges. Its membership has rapidly grown to more than 160 leading companies across the globe in a variety of industries, including leaders in finance, wireless services, telecommunications, security, transportation and infrastructure technology, as well as several universities, national and local governments, and consumer advocate and privacy organizations.

The first phase of the Liberty specifications was released in July 2002 and laid the foundation for cross-domain account linking and federation. Several leading technology companies have already released identity management products to support those protocols. Future phases of the Liberty specifications will allow for permission-based attribute exchange between domains and specify frameworks for federated identity web services.

The Liberty Vision:

To enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of vital identity information.

As the web services market evolves, it is critical for companies to be able to implement an identity strategy that is sensitive to privacy issues and instills confidence in its customers. The Alliance’s Public Policy Expert Group is working with governments and leading consumer advocacy and privacy groups around the world to establish the Liberty specifications and business guidelines. This ongoing effort will result in standards and practices that will comply with emerging policies and regulations on a global basis.

Federated Identity allows users to link identity information between accounts without centrally storing personal information. The user also controls when and how their accounts and attributes are linked and shared between domains and Service Providers. This gives them greater control over their personal data. In practice, this means that users can be authenticated by one company or web site, and be recognized and delivered personalized content and services in other locations without having to re-authenticate or sign on with a separate username and password.

For the federated identity vision to be implemented effectively, there needs to be *trust* established between all parties involved. Trust has always been at the core of any high-value relationship, and trust credentials are part of our daily lives – from the uniform and badge of a police officer, to membership cards, passwords, and secret handshakes. More advanced trust credentials include smart cards and biometric data such as fingerprints or retinal scans.

No matter what the credential, once trust is established, doors are opened to a meaningful relationship. While technology can accelerate trust-based relationships, trust can only be established through formal or informal business agreements and contracts.

This vision can also be articulated through the important concept of a *Circle of Trust*, which is defined as a group of service providers that share linked identities and have pertinent business agreements in place regarding how to do business and interact with identities. Once a user has been authenticated by a Circle of Trust identity provider, that individual can be easily recognized and take part in targeted services from other service providers within that Circle of Trust.

The Circle of Trust concept is not new to business – there have been Circles of Trust in the offline world for years, ranging from the world's preeminent insurance company, Lloyds of London (see sidebar on page 7) to affinity partnerships between travel providers to government management of citizen records. Bringing the "Circle of Trust" to the online world of identity-based web services, however, is a new concept that the Liberty Alliance is driving through its specifications and guidelines.

The concept of a Circle of Trust is shown in Figure 1:

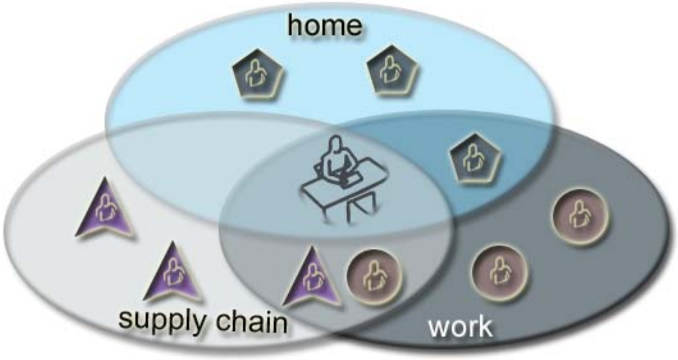


FIGURE 1. Circles of Trust

Figure 1 shows multiple Circles Of Trust. While authentication typically will take place within each Circle, identity attributes remain federated throughout the Circle, and, with the user's permission, can also be shared between multiple Circles. For example, an individual may use an online travel agency both at work and at home. They can access their attributes whether they are authenticated at home (via an ISP) or authenticated at work (via an outsourced travel agency), or even if they log in directly to the travel site. Note that attributes from the Supply Chain Circle are not shared with the Home Circle.

LLOYD’S OF LONDON: A 300-YEAR-OLD CIRCLE OF TRUST

The concept of a “Circle of Trust” is nothing new to business; in fact, trust has been at the core of some of the oldest and most successful businesses in the world. An excellent example is that of one of the world’s earliest insurance confederacies: Lloyd’s of London.

Lloyd’s began in Edward Lloyd's Thames-side coffee house in London in the 1680s. Lloyd himself was not involved in insurance but provided a forum whereby ship captains, merchants, and ship owners could carry on their business of insuring ships and their cargoes. These wealthy individuals would sign their names one after another (incidentally, this is the source of the term “underwriter”) on a policy, along with the amount of cargo that they agreed to cover. This list would be available for seafaring business owners to review and to engage for marine insurance.

Over time this list of underwriters grew from a loose confederacy of individuals into the exclusive list of Lloyds’ members, growing from several dozen individuals into 122 underwriting syndicates and companies. To this day, only members of the Lloyd’s circle of trust can carry on insurance business under the Lloyd’s name.

The Liberty Alliance realizes that technology specifications only address part of the challenge of implementing federated identity systems. This is why the Alliance also plans to publish business guidelines in conjunction with the specifications. These guidelines will help companies to implement federated identity systems that are sensitive to the latest global privacy and regulatory issues by highlighting and giving consideration to issues such as:

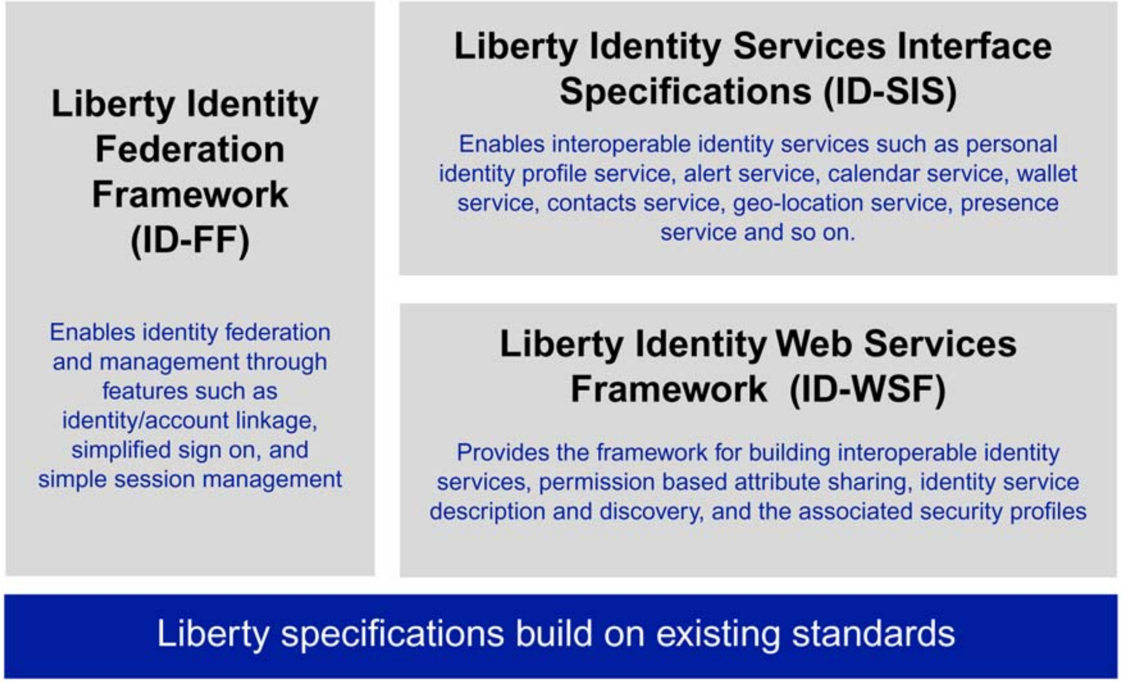
- Mutual confidence between parties to enforce rules for compliance and managing risks of exposure
- Liability to all parties, including service providers, network providers, and customers
- Risk and fraud prevention
- Compliance and information privacy for all parties in a “circle of trust” or federated identity value chain

These guidelines will be provided by the Alliance and will serve as a set of business issues that companies should consider when implementing the Liberty specifications. Many of these considerations are also articulated in the Alliance’s “Privacy and Security Best Practices” document that can be downloaded from the Liberty Alliance web site at:

http://www.projectliberty.org.

4.0 Business Benefits of the Liberty Alliance Architectural Vision

The Liberty Alliance Architecture consists of three key components, or frameworks, that have been developed and released in a phased approach. Each framework focuses on a different aspect of the identity puzzle. The Architecture is diagramed in Figure 2 along with details on business benefits of each framework.



Liberty Identity Federation Framework (ID-FF)

Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, alert service, calendar service, wallet service, contacts service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)

Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards

FIGURE 2. High-level Overview of the Liberty Alliance Architecture

More detail on the Liberty Alliance Project architecture can be found in the white paper *Introduction to the Liberty Alliance Identity Architecture.* This can be found at:

http://www.projectliberty.org/press.html.

In addition, a growing library of case studies and use scenarios for employee/intranet, customer, and business-to-business federated identity implementations are available for free public download at http://www.projectliberty.org/press/casestudies.

1. **Liberty Identity Federation Framework (ID-FF):** ID-FF comprises the Phase 1 Liberty Specifications (released in July 2002). It provides the mechanism for single sign-on and linking of separate accounts within a group of service providers in a circle of trust. For example, if a bank and a wireless service provider are part of the same circle of trust, a customer can choose to link those two accounts, allowing the customer to seamlessly take part in online services from both companies without having to log on to

both sites separately. This could allow the customer to pay its phone bill directly from the bank's web site, or conversely could allow the customer to transfer funds between a savings and checking account from a mobile phone.

2. **Liberty Identity Web Services Framework (ID-WSF):** ID-WSF is part of the Alliance's Phase 2 release. It provides an infrastructure for identity-based web services through aspects such as permission-based sharing of users' attributes, discovery of additional identity-based services, allowing for user security profiles, and support for differing types of client devices. This will allow businesses to implement services that leverage an authenticated user's attributes and preferences (beyond their basic identity). It also allows the user to have fine-grained control over which identity attributes are shared under specific circumstances. For example, this would enable users to personally control what information about themselves is available to other online services that they link to, such as mailing addresses, personal preferences, etc.
3. **Liberty Identity Services Identity Specifications (ID-SIS):** ID-SIS is a collection of specifications for interoperable identity-based service formats made possible by ID-WSF. These will be part of future releases, and may include support for specific formats and functions such as contact books, calendars, geo-locations, or alerts. A company will either be able to implement these services internally, and/or as revenue-generating service offerings to external customers and business partners.
4. **Adoption and Adherence to Other Industry Standards**: The Liberty Alliance is not only committed to developing and publishing an open standard for federated identity, but it supports and is incorporating other pertinent standards into the Liberty Alliance specifications. This means that a business can implement Liberty-enabled products and services have confidence that they will interoperate with the company's infrastructure, as well as the infrastructure of its customers and business partners. Proprietary identity systems may or may not support these standards, creating a potential IT pitfall of runaway development time and costs.

5.0 Business Benefits Summary

Within an enterprise, a Liberty-enabled identity management infrastructure can bring substantial cost savings, operational efficiencies, and increased security. These benefits come in the form of more effective employee provisioning and password management (cost reductions of up to 80%[1]), focused development efforts on a single standard that will be supported by a variety of technology providers, and the ability to more easily outsource certain employee applications in a more secure and flexible manner. Also, since employee identities can be managed internally and brought online and offline quickly, deployment of a federated identity infrastructure limits a company's vulnerability to security attacks by current or former employees and contractors.

For technology providers or device manufacturers, there is a burgeoning marketplace of companies looking not only to deploy web services, but federated web services based upon the Liberty specifications. In addition, the Liberty standards allow these companies to focus their product development efforts on offerings that are able to leverage the fact that Liberty was built from the ground up to support identities accessing information from multiple devices.

For service providers, the Liberty Alliance opens a world of benefits including greater efficiency and new revenue opportunities through the development and deployment of bundled services based on the "circle of trust" concept. These valuable services will also decrease the cost of customer retention and acquisition, while at the same time increasing a company's revenue per user.

To generalize across these three audiences, the benefits of implementing a Liberty enabled federated identity strategy and infrastructure fall into four main categories:

- Revenue growth through development of strategic offerings
- Cost avoidance, cost reduction and increased operational efficiencies
- Stronger security and risk management
- Interoperability and decreased time of development

More details on the benefits that a Liberty-enabled federated identity infrastructure, strategy, and/or services can bring are shown in the following table:

[1] RBC Capital Markets: Safe & Sound - A Treatise on Internet Security - 11/2001

Benefit:	**Examples:**
Revenue Growth through Development of Strategic Offerings	**Bundled Offerings:** Enables the business infrastructure required for the development of bundled customer offerings with strategic partners via “circle of trust” relationships. **RPU:** Increases customer satisfaction and revenue per user (RPU) by delivery of value-added, targeted services supplied to customers on a variety of devices in multiple locations. **Simplified Outsourcing:** Allows service providers to more easily create and offer a variety of outsourced services, ranging from identity-related services (e.g., authentication or identity management) to more “traditional” value-added services (e.g., HR or payroll) that can be more easily integrated into a customer’s enterprise. **Accelerated Development:** Development in the web services marketplace is expected to reach $21 billion by 2008, thereby establishing a huge market for Liberty-enabled infrastructure and service offerings. **Differentiation:** Use of the Liberty-enabled federated identity infrastructure delivers a competitive edge for companies. Providing Liberty-enabled products differentiates them from companies that support only proprietary technologies or closed identity systems. **Market Demands:** Implementing this technology meets a current market requirement as many government and institutional RFPs already have Liberty support as a pre-requisite, a trend that is expected to explode.
Cost Avoidance, Cost Reduction and Increased Operational Efficiencies	**Increase employee productivity.** Productivity is improved by granting employees faster access to applications and information throughout all of the business units in an enterprise. **Reduce Help Desk Costs.** Costs are reduced for employee, business partner, and customer identity maintenance and administration through secure delegation and self-service of identity information. **Customer Relationships:** Reduces CRM and customer acquisition costs by unifying identity systems, thus providing a more holistic view of the customer. This allows development of “sticky” web services and “viral marketing” programs. **Standardization:** Creates a standard interface for identity services, making it easier to add and remove outsourced service providers for enterprise services. **Product Development:** Allows technology and device manufacturers to develop to a standard, driving more focused product development efforts and reducing longer-term maintenance and upgrade costs. **Regulatory Support:** Provides consideration for regulatory compliance issues, including a strong framework for companies to implement services that support key global privacy policies and regulations including HIPAA, Gramm Leach Blyley Act (GLBA), EU Privacy Directive and others.

Benefit:	**Examples:**
Stronger Security and Risk Management	**Authentication Levels:** Provides context-sensitive, gradient levels of authentication and risk management. **Security control:** Offers integrated and tighter security controls through ubiquitous enforcement of security policies. **Nonrepudiation support:** Reduces security exposure through nonrepudiation support (i.e., the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or deny the sending of a message that they originated). **Fine-grained security:** Makes it easier for an enterprise to more effectively grant fine-grained access to current employees and to promptly terminate “orphan” accounts of ex-employees, contractors and partners. This alleviates a major source of security attacks within an enterprise, which frequently come from current or former employees or contractors. **Standards and business templates:** Provides guidelines for dispute resolution, audit management, policy-based compliance, and liability assignmen. This reduces the risk associated in implementing federated partnerships, and product and service offerings based on the Liberty specifications.
Interoperability and Decreased Development Time	**Speed and Ease of Deployment:** Systems can be deployed quickly and easily since the components of the solution are based on commonly accepted standards and interfaces, eliminating the need to develop to a myriad of integration points. **Interoperability:** Provides for more secure, more seamless interoperability between applications and systems, without the need for gateways; applications can natively “know” how to do this through a web service. **Integration:** Enables integration of legacy systems without re-engineering their authentication and authorization modules. **Reduces Deployment Lags:** Deployment delays are reduced because different parties in a “circle of trust” don’t have to agree on the same technology and products at each point of the network, but rather have a common plan from the beginning. **New Deployments:** Allows service providers to deploy new systems that interoperate and communicate with existing systems, minimizing system and customer downtime.

6.0 Liberty Alliance Technology in Action

Several leading technology providers and system integrators have developed products and services that support the Liberty specifications and can help your enterprise develop an effective federated identity infrastructure that meets your business needs. A full listing of these companies and services can be found at the Liberty Alliance web site:

http://www.projectliberty.org.

There are already many leading companies that are gaining a competitive advantage by building Liberty technology into their enterprise infrastructures to address business challenges. For example, General Motors, a leading member of the Liberty Alliance, has tackled identity issues across internal and external identity systems. Chances are that some of these business issues will match those of your own organization. GM's ongoing business objectives are to:

- Reduce design cycle times
- Build vehicles to dealer and individual order
- Ensure more valid customer demand information
- More tightly integrate real-time business processes

For some, this may sound like an easy task, but consider that GM has 362,000 employees and more than 200 manufacturing facilities throughout the world. It sells more than 8.5 million units a year, in 200 countries, through 14,000 dealers. And if that is not enough, GM globally has no common E-mail system, no common desktop environment, and is still continuing to phase out the 7000 legacy IT systems it has had since 1996. Currently, they are still dealing with approximately 3,500 legacy systems.

The Liberty Alliance specifications will make it possible for these identity and infrastructure systems to interoperate so that GM can deliver valuable services to its customers, suppliers, dealers and employees. One of the ways GM is incorporating federated identity management and Liberty technologies is within their employee intranet, called MySocrates. MySocrates provides access to many of the outsourced HR services that GM employees receive, such as health benefits and 401K plans.

"While MySocrates offers central access to these services, our employees have to log-in and authenticate themselves every time they access each service," explained Rich Taggart, director of enterprise architecture for GM's global technology division. "We want to make access more seamless and efficient to our employees, but you can imagine that some may not want to share the same profile and password with both their 401K provider and their health care provider. Federation makes this customer control possible."

GM also offers employees a significant discount on AOL's services for home Internet use. Using Liberty's specifications, GM hopes to federate an employee's AOL screen name with their MySocrates ID, thereby allowing employees to move easily between work and home life.

7.0 Summary and Call to Action

The Liberty Alliance Project has developed a business-ready architecture that will result in cost savings, new revenue opportunities, increased security, and greater technical flexibility and efficiency. More information on the Liberty specifications and business guidelines, as well as information on Liberty-enabled products and services, can be found on the Alliance's web site at:

www.projectliberty.org.

In addition to implementing a Liberty-enabled identity infrastructure, there are also tangible business benefits to joining the Alliance. There are multiple levels of membership, with membership dues that scale according to the size of your business. By joining the Alliance, your company can actively influence the future of federated identity management and the activities of the Alliance by:

- Participating in the development of market requirements, specifications, roadmaps, and other technical guidelines that guide the work and perspective of the organization.
- Networking across member companies and gaining a better understanding of needs that exist across various vertical and horizontal sectors.
- Reviewing pre-release specifications and other materials before they are available for public consumption.
- Gaining a high-profile opportunity to understand and contribute to developing public policy across the globe.

Membership information can be found on the web site or by sending E-mail to:

info@projectliberty.org.