LIBERTY ALLIANCE PROJECT

Whitepaper: Benefits of Federated Identity to Government

March 7, 2004

Editor:

Tanya Candia, Sigaba

Contributors:

Frank Kaupa, American Express
Luc Mathan, France Telecom
Paule Sibieta, France Telecom
Piper Cole, Sun Microsystems
Andrew Shikiar, Sun Microsystems
Stephen Deadman, Vodafone

Abstract:

Today's administrative and business environment calls for information sharing on an unprecedented scale, from government to business to citizen. Sharing and interoperating among agencies, businesses and governments around the world creates opportunities to simplify processes and unify work, as well as improve the overall performance of government. Secure interoperability, based on identity management solutions, enables substantial cost savings, streamlined processes, and faster communication of vital information to the benefit of governments and citizens of all nations.

At the core of this revolution is the concept of identity management and the need for a standard that is open, interoperable and decentralized. In addition, it must allow for privacy safeguards across all sectors. The Liberty Alliance Project was established to address this need, and to tackle the twin issues of standards and trust.

The Liberty Alliance is ushering in federated identity implementations that allow the public sector to find substantial benefits, including:

- Improved alliances, both within governments and between governments, through interoperability with autonomy
- Faster response time for critical communications
- Cost avoidance, cost reduction and increased operational efficiencies
- Stronger security and risk management
- Interoperability and decreased development time

The Liberty Alliance consists of over 150 leading organizations across the globe, including numerous government and non profit agencies. The US General Services Administration, the CIO Office of the Austrian government, the Royal Mail, Canada Post, Hong Kong Post, the US Department of Defense, the University of Hamburg, University of Chicago as Operator of Argonne National Laboratory, Financial Services Technology Forum, Helsinki Institute of Technology, International Security and Privacy Alliance, BITS, The Open Group -- all are examples of public sector organizations that add to the diversity and scope of the Liberty Alliance and provide intriguing examples of the role of federated identity management in today's evolving world.

Table of Contents

Background

Today's administrative and business environment has created an unprecedented need to securely share sensitive information among national, regional and local governments, agencies and organizations, as well as with citizens and business entities. The true distributed computing platform created by the Internet brings into sharp relief the importance of adhering to emerging privacy standards and data security regulations.

Identity is at the core of any information-sharing transaction: government to citizen, government to business, or government to government. An individual's identity not only proves that he is who he says he is, it also indicates what he can do and what resources he can access. Governments are often the source of core documents that relate to one's identity: birth certificates, drivers' licenses, employment and tax records, marriage and death certificates, and the like. Identity credentials are perhaps more relevant in today's digital society in their electronic form than on paper.

Identity Management Issues

Effectively managing one's identity means retaining control over the information relative to who one is, who has access to it and how it is used. While simple in the abstract, the task is enormously complex in reality. Even within a single organization an individual may rely on multiple identities: an employee may need to authenticate to a database, an application or a service using completely different mechanisms. Once outside the organization, the problem is compounded. Multiple organizations will hold multiple instances of identity and attribute information. The problem of effectively managing all these instances is enormously complex, resulting in ineffective identity management and complexity.

Furthermore, as governments, citizens and businesses extend their relationships, they are challenged to grant access to services and applications to the right people at the right time without sacrificing privacy, security or scalability. Since today's communities of interest are built and modified on a dynamically changing basis, trust must be able to be created or eliminated quickly. The old ways of managing identity dramatically reduce the organization's ability to move quickly enough to respond to changing relationships.

The Ideal Solution

Ideally, government would like to have the ability (whether through technology, business practices, policies, education or a combination thereof) to meet these seemingly conflicting requirements:

- Simplify access to services and applications both inside and outside the organization
- Reduce the need to maintain and manage multiple sets of identity credentials
- Reduce the cost and complexity of managing identities
- Enable dynamic creation and management of trusted relationships
- Preserve privacy and ensure data security

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, it is at the core of some of the oldest and most successful businesses in the world. An excellent example is Lloyd’s of London, one of the earliest insurance confederacies.

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

Federated Identity Management

Fortunately, there is an answer to this need: *federated identity management*. Federated identity management makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains. Federated identity avoids the pitfalls of centralized storage of personal information, while allowing users to link identity information between accounts. Since users can control when and how their accounts and attributes are linked and shared, they retain greater control over their personal information. In practice, this means that users can be authenticated by one organization or website and be recognized, and delivered personalized content and services, in other domains without having to re-authenticate.

Increasingly, governments are looking at network identity as a way of interacting with their various constituencies and partners. Examples abound: Japan, France, the UK, New Zealand, the United States and Canada all have e-authentication initiatives.

Foundation for Federated Identity

Federated identity requires two key components: trust and standards. The first component, trust, is realized through the important concept of a Circle of Trust: a group of organizations that have established trusted relationships with one another and have pertinent agreements in place regarding how to do business and interact with each other and manage user 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 organizations – 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) 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 second component relates to a common set of technical and business standards and guidelines that allows for the deployment of meaningful Web services. The Liberty Alliance Project was formed to foster development of these standards and specifications. More detail on the standards promulgated by the group is outlined at the end of this document. Thanks to the Liberty Alliance, governments can now capitalize on the promise of Web services by implementing federated identity systems based on products and technologies that support the Liberty protocols. They gain greater efficiency with information technology expenditures, create new communication and collaboration opportunities with partners, and expand service offerings to their citizens.

Public Sector Benefits

Within a single government organization, 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 reduction 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 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 an organization's vulnerability to security attacks by current or former employees and contractors.

However, the real benefits of federated identity management can be seen when communication takes place between and among various organizations. Below we briefly discuss several situations that call for federated identity.

Government to government

Many types of vital information must be shared across government and organizational boundaries. Interoperability is a requirement within agencies, among organizations, and even between nations. Indeed, the dynamically changing nature of national coalitions calls for dynamic Circles of Trust. A federated architecture now allows systems to interoperate while maintaining their autonomy. The Circle of Trust provides participating organizations with the framework to ensure that this interoperability is trusted and secure.

The compelling need for sharing sensitive information, and thus for federated identity management, can be clearly seen in times of disaster. A regional incident, such as an earthquake or avalanche, brings together myriad organizations that must freely share disaster response information among all relevant agencies and governments, often spanning multiple countries. When information about individuals, rescue and response actions and law enforcement activities are at stake, it is vitally important to ensure that individuals are properly authenticated prior to exchanging such sensitive information.

Government information sharing is a requirement not only in times of crisis; in fact, it permeates all aspects of government. For example, the European Commission's eEurope activity covers a number of initiatives including e-government, e-health, e-learning and e-business, all designed to foster the development of new and better services. Examples include initiatives related to the health sector in Spain and Finland, the management of relations between administrations and companies in Belgium, the indexing of public files in Italy, e-voting in some local consultations in France, and much more. In each, the need for interchange of information requires a federated identity management framework to enable free flow of information while preserving security and privacy.

[1] RBC Capital Markets: Safe & Sound – A Treatise on Internet Security (Nov. 2001)

Government to citizen

Perhaps in no other area of communication is the need for secure yet open access as important as in government-to-citizen interaction. Governments around the world are embarking on e-government and e-authentication initiatives, widespread broadband access, and electronic communication programs in order to bring the benefits of technology to their citizens.

In the public sector, various government departments and agencies give citizens and businesses access to online services through their e-authentication initiatives. To avoid any generalized interconnection of public files containing personal information, the federated approach is ideal: it ensures that data is not duplicated in a single central database.

Individual government authorities can act as identity providers for citizens by establishing Circles of Trust and offering a complete range of personalized applications across different government agencies and domains, such as online tax declaration, reimbursement for medical expenses, car registration and electronic passport and drivers license renewals. In addition, with strong yet manageable authentication, governments can ensure that benefits are going to the authorized recipients. Such a scheme can quickly lead to single-sign-on, with the resultant benefits of cost reduction and increased security.

The eEurope 2005 Action Plan embodies these initiatives, aimed at modernizing public services and giving everyone the opportunity to participate in the global information society. One area of focus is healthcare. Over the past few years much progress has been made in building integrated regional health information networks, standardized electronic health records and the like. New initiatives will enable rapid reaction to health threats, while protecting individuals' health information from unauthorized access.

Citizens' Growing Demand for Sophisticated Services

"Citizens are becoming used to ever-faster response times and ever-higher quality of products and services from the private sector. They expect the same performance from public administrations too. Obscure procedures, long queues, having to re-enter information that is already held by the administration, and "one size fits all" approaches are all practices that are increasingly criticized […]. Finally citizens […] expect authorities to become accountable for the management of taxpayers' money. They also demand more transparency of decision-making and democratic involvement in all phases of policy development."

From the European Commission communication on the role of eGovernment for Europe's future (September 26, 2003)

Government to business

Whether for government sales of assets, expanded tax products for business, one-stop business compliance, streamlining of international trade, or other activities, businesses have come to expect more electronic interaction with government. This is especially true for small and medium size enterprises: with limited resources for interacting with government agencies, they are eager to find convenient procedures for such activities as VAT declarations or company registrations. A federated architecture is essential, as it enables a single-sign-on capability and seamless and secure interaction with distinct functions or agencies, while leaving each user in control of his data.

When business interacts with the government, the conflicting requirements of privacy and interoperability must both be addressed in a delicate balance. An interesting example can be seen today in Japan's EduMart, part of the e-Japan Policy Priority Program and spearheaded by the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters). In an effort to bring rich educational content to students at more than 40,000 schools, the IT Strategic Headquarters established an open interface and built an educational content distribution network that will lead to a system in which both public institutions and private businesses can connect to interfaces and freely participate.

Naturally, the requirement to secure privacy had to be balanced with the need to establish openness. Since the users of the solution are students, personal information such as grade history would need to be protected. However, a certain level of personal information (such as focus of study) needs to be shared so that relevant, targeted content can be delivered. By employing Liberty Alliance Phase I Specifications, EduMart was able to ensure single sign on, interoperability and openness for content delivery, and personal information and copyright management. The result: the world's first e-learning system based on the Liberty Alliance specifications.

Additional examples can be seen across the value chain, from government-controlled healthcare programs that must communicate with providers and patients, to government contracts with foreign suppliers, to basic business licensing and taxation. Speed, timeliness, accuracy and user friendliness are the obvious outcomes of such initiatives.

E-Authentication Initiatives Benefit Industry and Government.

E-Authentication will minimize the burden on businesses, citizens, and government when obtaining services on-line by providing a secure infrastructure for on-line transactions, eliminating the need for separate processes for the verification of identity and electronic signatures.

"We have been working to put in place infrastructure for the government to be able to trust and use federated identity, however, we also recognize that rules and infrastructure for the federation of identity apply much more broadly than the Federal government and we are committed to work in collaboration with industry, states and local governments to best serve all of our citizens and customers."

Karen Evans, Administrator of the Office of Electronic Government and Information Technology, U.S. Government. December 2003.

To generalize across these public sector audiences, the benefits of implementing a Liberty-enabled federated identity strategy and infrastructure fall into five main categories that are detailed further below:

- Improved alliances, both within governments and between governments, through interoperability with autonomy
- Faster response time for critical communications
- Cost avoidance, cost reduction and increased operational efficiencies
- Stronger security and risk management
- Interoperability and decreased deployment time

More details on the benefits that a Liberty-enabled federated identity infrastructure, strategy and/or services can bring follow below.

Benefits Table

Benefit	Examples
Improved alliances through interoperability with autonomy	• **Stronger relationships among nations**: Enables the secure communication of vital information with other nations while enabling them to retain control over that information • **Control of information**: Provides for national and organizational autonomy, since individual identity information does not need to be stored in one single location/country. • **Enhanced collaboration**: Allows resources and applications to be shared among disparate communities in a way that preserves privacy and confidentiality. • **Strategic advantage through dynamic provisioning**: ability to quickly enter into collaborative arrangements to take advantage of immediate needs, and quickly de-provision when the need arises.
Faster response time for critical communications	• **Faster time to communicate with first responders** whether for terrorist threat, environmental hazard, or other time-sensitive information through dynamic provisioning of credentials. • **Standardization**: Creates a standard interface for identity services, making it easier to add and remove parties for critical communication services.

Benefit	Examples
Cost Avoidance, Cost Reduction and Increased Operational Efficiencies	• **Increase individual and national productivity** by granting citizens faster and easier access to applications and information throughout all agencies of an organization. • **Reduce help desk costs** for individual, business partner and citizen identity maintenance and administration costs through secure delegation and self-service of identity information and reduced expense of password resets. • **Service Development**: Allows governments and business 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 organizations to implement services that support key privacy policies and regulations around the world, including HIPAA and Gramm-Leach-Bliley Act (GLBA) in the US, and the EU Data Protection Directive.
Stronger Security and Risk Management	• **Authentication Levels**: Provides context-sensitive, gradient levels of authentication and risk management to support initiatives such as the U. S. eAuthentication and E.U. eGovernment initiatives • **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 the sending of a message that they originated). • **Fine-grained security**: Makes it easier for a government organization to more effectively grant fine-grained access to citizens and businesses, and to promptly terminate “orphan” accounts of ex-contractors and partners, alleviating a major source of security attacks.

Benefit	Examples
Interoperability and decreased development time	• **Speeds and eases deployment** since the components of the solution are based on commonly accepted standards and interfaces, eliminating the need to develop to myriad integration points. • **Interoperability**: Provides for more secure, more seamless interoperability between applications and systems, through standards-based identity federation. • **Integration**: Enables integration of legacy systems without re-engineering their authentication and authorization modules, because the Liberty specification is built on standards. • **Reduces deployment lags** since 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.

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 organization develop an effective federated identity infrastructure that meets your needs. A full listing of these companies and services can be found at the Liberty Alliance website (http://www.projectliberty.org).

An example of cooperation between government and citizen can be seen in the U.S. initiative called the Internet-based County Land Document Recording Exchange. Intended to dramatically streamline the land recordation process for participants, notably mortgage and title companies, it will save time and money while increasing the integrity of the participating local government land records systems.

This project comprises a Liberty Alliance-compliant Web application, utilizing standard off-the-shelf products from a Liberty Alliance member company. It enables mortgage and title company partners to establish and exchange credentials in an interoperable fashion, establishing a strong foundation for an industry "Circle of Trust". Land record exchange credentials can be extended to other applications, and the exchange is able to accept credentials issued by other Liberty-compliant identity providers.

Another example, the Joint Warrior Interoperability Demonstration (JWID) 2003, shows government-to-government interoperability. Spearheaded by the U. S., Joint Chiefs of Staff, JWID tackles identity issues across national and international boundaries. One key objective is to enable a standard solution for information sharing among coalition partners. Important issues are authentication and identity management, since each nation retains control of its own information, and desires to maintain its autonomy without impeding the free exchange of information.

In JWID 2003, military forces from six nations (Canada, Australia, New Zealand, United States, United Kingdom and Norway as the NATO representative), used Liberty Alliance member solutions to clearly demonstrate how federated identity management could save lives, increase communication and build stronger alliances. Because trust was set up among all the forces, no one country had to hold the root certificates for the others; each maintained its autonomy while benefiting from secure messaging. Using its federated authentication architecture, the solution tied together message traffic from land-based and maritime units from all six countries, showing the true potential and value of this approach in scenarios that required the ability to revoke credentials from field forces that may have been compromised.

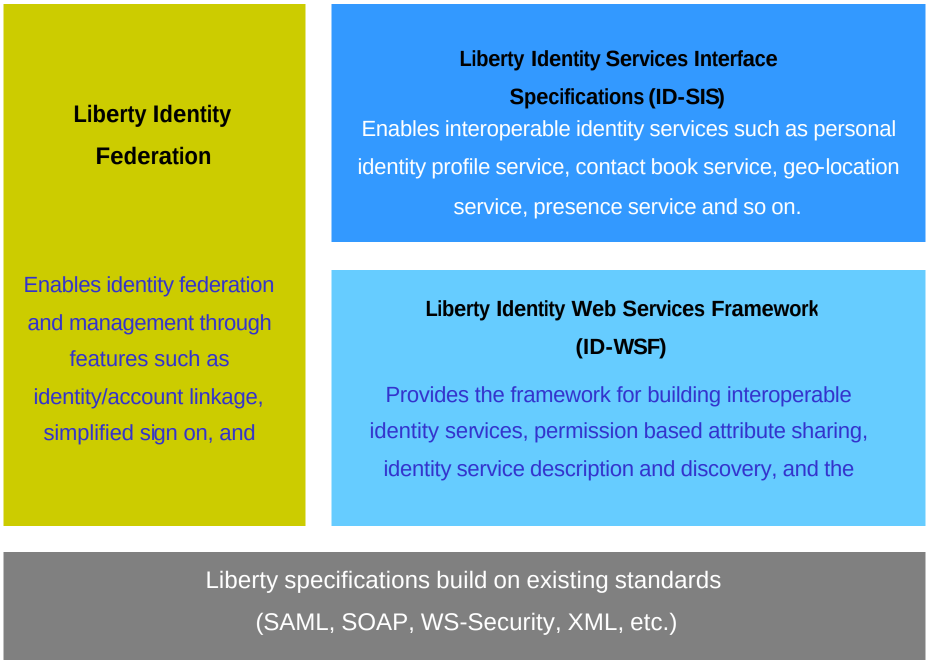
History of the Liberty Alliance and Federated Identity Management

The Liberty Alliance was established by 16 companies in December 2001 with the goal of creating open, interoperable standards and guidelines for federated identity management to meet 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 150 leading companies across the globe in a variety of industries and sectors.

Phase I of the Liberty specifications was released in 2002 and laid the foundation for cross-domain account linking and federation; leading technology companies have already released identity management products to support those protocols. The second phase of the Liberty specifications was released in November 2003 and included a framework for delivery of identity-based web services. Collectively, these specifications have created a complete foundation for identity services that will be released in future phases of the Liberty specifications. Some of these services will include geolocation, contact book, wallet and presence. The Liberty architecture and organization also allows for development of identity services based on vertical or market needs – fo instance, a group of government groups could come together to form e-citizen and/or e-authentication services based on the Liberty architecture.

Liberty Alliance Architectural Vision

The Liberty Alliance Architecture consists of four 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 below along with details on business benefits of each framework.



Liberty Identity Federation

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

Liberty Identity Services Interface Specifications (ID-SIS)

Enables interoperable identity services such as personal identity profile service, contact book 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

Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)

More detail on the Liberty Alliance Project architecture can be found in the "Introduction to the Liberty Alliance Identity Architecture" white paper (http://www.projectliberty.org/press.html). In addition, a growing library of case studies and use case 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.

Liberty Identity Federation Framework (ID-FF): ID-FF comprises the Phase 1 Liberty Specifications (released in July 2002), and provides the mechanism for single sign-on and linking of separate accounts within a group of service providers in a circle of trust.

Liberty Identity Web Services Framework (ID-WSF): ID-WSF is part of the Alliance's Phase 2 release (released in November 2003), and 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 allows businesses to implement services leveraging an authenticated user's attributes and preferences (beyond their basic identity), and allows for the user to have fine-grained control over which identity attributes are shared under specific circumstances. For example, this enables 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.

Liberty Identity Services Interface Specifications (ID-SIS): ID-SIS is a collection of specifications for interoperable identity-based service formats made possible by ID-WSF. Liberty has already released Service Interface Specifications for personal and identity profiles and is working on specifications for contact book, geo-location and presence; future Liberty releases will include specifications for other service interfaces. In addition, outside organizations can create their own Service Interface Specifications to plug into Liberty's Web Services Framework (ID-WSF). Companies can implement these services internally and/or as revenue-generating service offerings to external customers and business partners.

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 is supporting and incorporating other pertinent standards into the Liberty Alliance specifications. This means that a business can implement Liberty-enabled products and services with confidence in knowing 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 information technology pitfall of runaway development time and costs.

Follow-on Information and Resources

The Liberty Alliance realizes that technology specifications only address part of the challenge for implementing federated identity systems, which is why the Alliance also has published Business Guidelines in conjunction with the specifications.

These guidelines help organizations 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, liability, risk and fraud protection, compliance and information privacy.

The base set of these guidelines can be downloaded from the Alliance's website and can serve as a set of issues that organizations should consider when implementing the Liberty specifications. Future releases of the Business Guidelines will detail specific vertical and geographical business and policy issues associated with federated identity services.

Many of these considerations are also articulated in the Alliance's "Privacy and Security Best Practices" document; all documents can be downloaded from the Liberty Alliance website at http://www.projectliberty.org.

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 on Liberty-enabled products and services can be found on the Alliance's website at www.projectliberty.org.

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

- Participation in development of market requirements, specifications, roadmaps, and other guidelines that guide the work and perspective of the organization
- Networking across member organizations, gaining a better understanding of needs that exist across various vertical and horizontal sectors
- Pre-release review of specifications and other materials before publicly available

- Gaining a high-profile opportunity to understand and contribute to developing public policy across the globe

Membership information can be found on the website or by sending email to MembershipInfo@projectliberty.org.