LIBERTY ALLIANCE PROJECT

Business Guidelines

Raising the Business Requirements for Wide Scale Identity Federation

July, 2003

1. Introduction

Identity federation and the Liberty Alliance specifications provide businesses, governments and individuals with substantial benefits; offering them choice, convenience and control over how they can manage and share identity information. However, the emerging concept of federation also raises some very real business issues that must be considered by any company implementing a federated identity solution, such as the Liberty Alliance specifications. The purpose of this document is to identify the general business considerations that must be addressed by any organization exchanging identity information beyond company boundaries in today's complex federated identity environment. Additional content from Liberty Alliance will describe B2B, B2C, B2E and mobile business scenarios and case studies for federated identity, based on the models explored in this document.

The information provided here is for reference purposes only and is not intended as a comprehensive list of all issues to be considered by any individual or entity exploring the value of adopting Liberty protocols, nor it is intended as substitutes for advise of counsel on the topics addressed in this document.

The Liberty Alliance or "Liberty" is an unincorporated contract-based group of more than 160 companies around the world. Liberty's vision is one of a networked world in which individuals and businesses can easily interact with one another, while respecting the privacy and security of shared user identity information. Liberty does not serve as an "identity network" operator or endorse specific products or services. However, Liberty develops federated identity specifications, guidelines and educational materials. For more information on the Liberty Project, see www.projectliberty.org, as well as the "resources" section at the end of this document.

2. BACKGROUND

Enterprises are faced with a complex set of challenges as they balance the need for security and the growing requirements for providing diverse users with seamless access to information. While existing identity management solutions can help reduce inefficiencies associated with managing roles, permissions and access to information within companies, there are a growing number of applications that require **inter-company** (federated) exchange of identity-based information (e.g. single sign-on, web services, etc). The emergence of these applications requires enterprises to re-examine their approach towards managing risks and liability within the context of the required interdependence.

Liberty's objective is to create open, technical specifications that: (i) enable simplified sign-on through federated network identification using current and emerging network access devices, and (ii) support and promote permission-based attribute sharing to enable a user's choice and control over the use and disclosure of his/her personal identification information.

3. TODAY'S ENVIRONMENT

From the moment an individual is born, he has an "identity." The identity starts with the individual's name on a birth certificate and evolves over time, as labels, interactions, and relationships are associated with that identity. As the individual grows, he interacts with an ever-larger group of entities and organizations. While the individual family and friends have a deep and complex understanding of who that person is, the organizations with which he interacts know him as little more than a number.

Fast-forward to the grown up and modern world, pieces of user's identity are now scattered across an endless list of entities: banks, credit card companies, brokerage firms, insurance companies, national IDs, pension funds, medical providers, and the places where they work. The Internet has become one of the prime vehicles for business, community and personal interactions, and it is fragmenting this identity even further. Distributed bits of user identity are doled out across many computer systems and networks used by employers, Internet Service Providers, bulletin boards, instant messaging applications, online commerce and content providers. This all occurs with little coordination, interaction, or control on the end-users' part.

The result is a fairly high level of frustration, especially in individual-to-business relationships over the Internet. All too frequently, users experience a series of isolated, one-to-one customer-to-business relationships that are irritating, cumbersome and wasteful.

At the enterprise level, with the introduction of new systems for managing customers, suppliers, and business partners, the Information Technology (IT) managers are challenged by the need to provide increased access to this larger and more dynamic group of users.

To address these challenges enterprises are integrating identity management solutions to automate the procedures for user and role provisioning, password management and access control. To date however, the bulk of these solutions have focused on the internal use and management of identity, and not on the interdependent management of identity information between companies. The most difficult identity challenge is is not that of managing identities within an organization's control, but handling or managing identities that are partly or completely outside the span of control.

4. EMERGING TRENDS

The Need for Federated Identity

Creating a federated identity infrastructure is a key to addressing the challenges of today's environment. Federated identity is a requirement for widespread distributed computing, for example. It recognizes that individuals move between corporate boundaries at a frequent rate. It strives to maximize convenience while accommodating privacy concerns by allowing users to "link" elements of their identity between accounts without centrally storing all of their personal information.

There are many benefits to a federated identity infrastructure. This infrastructure:

- ✓ Provides the end user a far more satisfactory online experience, as well as new levels of personalization, security, and control over his/her identity information.
- ✓ Enables the IT manager to more easily and securely provision accounts and provide user with access to the right resources.
- ✓ Enables businesses to create new relationships with each other and to realize business objectives faster, more securely, and at a lower cost.

Business Implication of Federated Identity

Driving the requirement to understand the implications of identity federation is the rise in popularity of Shared/Single Sign-On (SSO), which reduces redundant logons by allowing applications, systems and companies to share a user (identity) authentication. As a consequence of inter-company SSO, and the interdependencies it creates, companies are forced to deal with business issues such as liability, risk and the costs associated with establishing trust and security in a quality conscious manner.

"Over the next few years we have to deal with some very messy problems – namely, what it takes to deploy federated technology along with what it takes to bash out contracts between partners..."
Michael Barrett, Vice President of Internet Strategy at American Express
& President of Liberty Alliance

5. IDENTITY FEDERATION: BUSINESS REQUIREMENTS CONSIDERATIONS

Liberty is developing and delivering the technical standards that enable wide-scale identity federation. Enterprise customers, vendors, and service providers are in the process of implementing these standards. To efficiently enable wide-scale federated identity deployment, Liberty is also defining technology and business guidelines for creating inter-linked circles of trust between business partners and publishing scenarios and case studies as they become known or available. The following is a high-level overview of the Business Requirements that need to be considered during a large-scale deployment.

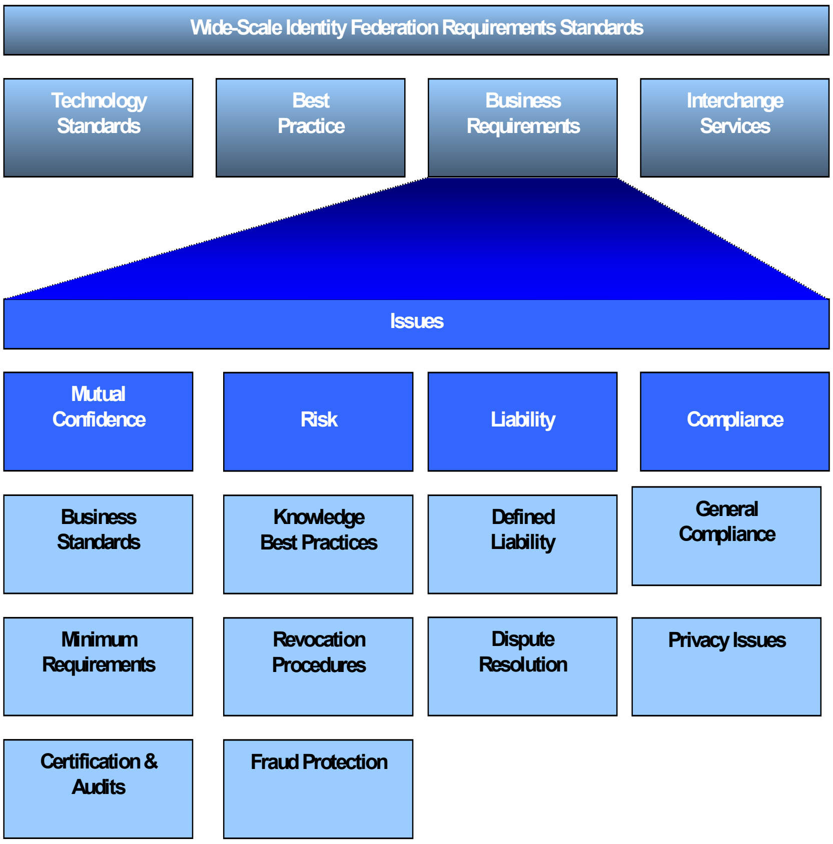

Figure 1- Federated Identity: Business Requirement Framework

Each of the major modules identified above is discussed in greater detail in the sections that follow.

Mutual Confidence

Within the context of federated identity, mutual confidence refers to the measures, and tasks that circle of trust members undertake or adopt together to:

- ✓ Enforce rules for compliance
- ✓ Manage the risks of exposure

Business Standards

Business Standards are the set of rules, conventions and guidelines that participating members of a circle of trust need to abide by. The business standards that will be most critical in creating a circle of trust related to identity transactions include:

- ✓ Accreditation standards and guidelines
- ✓ Technical standards and associated levels of performance
- ✓ Security and Privacy standards
- ✓ Trade standards for vertical and cross-vertical transactions
- ✓ Adoption and alignment with legal standards (such as HIPAA)

Federation governance provides the frameworks for the definition, development, implementation, and enforcement of these standards. The governance framework is one of the measures that can be used by the circle of trust members to demonstrate how the risk of federating identity is managed, and how regulatory compliance is achieved. Monitoring and enforcement of minimum acceptable standards for all members of a federation (or a circle of trust) is necessary to ensure that no weak link creates exposures for the participants. Additionally, liabilities may be incurred by lapses in adherence to the standards.

Minimum Requirements

These are the service delivery quality control measures that need to be articulated and enforced in order to mitigate operational performance risks:

- ✓ Internal controls
- ✓ Service Level achievement against controls and technical standards
- ✓ Employees' integrity/certification requirements
- ✓ Audit

Each member of a circle of trust needs to assert that they can and will adhere to a minimum level of standards and requirements. In addition, each member must have the ability to confirm and validate that these standards are being adhered to (see Certification & Audits).

Furthermore, recourse must be defined for both lapses in achievement of minimal requirements, as well as disqualification of any participant. It is likely that the federation will need to provide for continual improvement in the level of minimum requirements in order to ensure the quality of the services delivered over time.

Certification & Audits

Certification is the act of certifying or confirming that certain facts are true, and that the levels of performance and conformance are maintained.

Certifications and accreditations are measures that can be used by the circle of trust members to validate the effectiveness of their standards, and ensure ongoing mutual confidence vis-à-vis managing risks and complying with regulatory requirements.

Certification could be achieved by self-assertion of facts by a party, notification of compliance by accepted third parties such as external auditors, statement of compliance from an accredited testing organization, or by examination by representatives of the federation. It is possible that various methods would be adopted depending on the category of the standard, the maturity of the standard, and the criticality of the requirement.

Risk Management

All entities face risk in the form of potential exposure to financial injury or loss. Within the context of a federated identity, risk can manifest itself as actual losses due to fraudulent use of an identity, loss or exposure of identities or attribute information, and loss of business integrity due to insecure processes and data. Both the identity user and the service provider are subject to financial loss as well as loss of personal or business reputation (such as in the case of identity theft and fraud), but all parties in the identity network are exposed to the risks pursuant to insecure processes and data. Federations can manage risk through disseminating knowledge of best practices, revocation procedures, and fraud protection measures.

Disseminating Knowledge of Best Practices

Insight and experience in the creation of technical standards, entry criteria, and processes and rules, is inherent in the design and deployment of federation. However, risks will continue to present themselves as technologies, and experience in the marketplace evolve. The most effective way to keep current on these risks, design deterrents, and upgrade requirements and specifications will be to employ the best practices of the industry as the technology evolve. Best practices will be critical in the area of: sources of attacks, methods of attacks, sources of detection and safeguards.

Revocation Procedures

Revocation is the process of suspending the access rights of a principal, and is also a powerful potential tool to mitigate risk. This could be the result of a mutual agreement between the principal and one or more members of the circle of trust; or it could be the result of breach or a dispute between the parties.

The following set of federated procedures can be defined and integrated into the operational delivery environment:

- ✓ Procedures for revoking credentials
- ✓ Procedures for suspending an identity
- ✓ Procedures for lowering confidence in a particular interaction

Fraud Protection Measures

One area for particular consideration in the identity space is the fraudulent use of an identity following identity theft. This can entail the creation and use of invalid identities, a user's repudiation of a legitimate transaction, or a service providers' use of a networks capabilities without legitimate users behind its transactions. Each of these forms of fraud requires specific protections, and constant vigilance, actions and alerts. This implies the need for active management and oversight of operations, procedures, data, and pooled information.

In order to address identity theft, companies issuing identities may want to consider delivering a clear statement to their end users. Attribute Providers and Service Providers need to do the same for the attributes that they manage or use. The goal here is to inform the end user of the scope and responsibilities of the different entities:

- ✓ Security Policy for Identity Management Providers (IdP)
- ✓ Security Policy for Attribute Management Providers
- ✓ Security Policy for Service Providers (attribute confidentiality).

Any federation will find that it must constantly battle abuse of the system through its use of pooled data, and that it will need to continually respond to nascent approaches of fraud and threats through new methods of detection and intervention.

<u>Liability</u>

Failure to mitigate risk or to execute obligations as defined in an agreed upon process or specification can result in liability in the form of money damages or requirements to repair damages to another party in the event a) of an accident where the right of a principal (individual consumer or a company) was compromised; b) where laws or standards have been violated. In networked environments, there are potential liabilities to all parties, including providers, agents, and the network, based on agreements and expectations related to rules and performance.

Identifying up front who will bear what loses, and in what circumstances, (minimum standards not being met, processes being omitted or shortcut, etc.) can help limit unnecessary frustration and expenses. Over time, the web services and identity federation industry will likely evolve customary practices for assessing and determining the allocation of liability between parties in a business relationship. In the absence of allocation of risk by private contract, recourse will be made to other less preferable methods of dispute resolution.

Dispute Resolution

As is the case with allocation of liability, identifying agreed-upon processes for dispute resolution can help minimize or eliminate the need for parties to resort to traditional, and often time-consuming and costly, means of resolving conflicts.

For example, if a customer of an online brokerage firm is unable to perform a critical trade because of a problem related to shared authentication, who is at fault? Who is financially liable? What is the individual recourse? What are the efficient and timely procedures for resolving the incident?

Traditional means of dispute resolution include mediation, arbitration, or recourse to appropriate legal or regulatory authorities. The agreed upon means of resolving disputes may be specified in contracts.

Dispute Resolution methods tend to be human resource intensive and may not be appropriate for the high-volume and automated environment of web-services. Parties should consider the extent to which mediation or arbitration options can be adapted for the online environment.

Compliance

General Compliance

Compliance is the alignment with agreed standards, policies and procedures. These standards, policies and procedures may be governed by contract – be they unilateral, bi-lateral or multi-lateral.

Privacy Issues

Information privacy standards address the interest of an individual (or a company) in controlling, or at least significantly influencing the handling of data about himself or herself.

Within the context of a federated identity, there are a number of privacy compliance regulatory issues that needs to be considered from the perspectives:

- ✓ Privacy interest of the consumer
- ✓ Privacy interest of the business
- ✓ Privacy interest of employees

Within a deployed federated identity system, necessary information should be provided in order to be compliant with the local privacy requirements. It is assumed that any member of the federation will comply with applicable law (see Business Standards). As new legislation is enacted, on the national or local level, it should be considered a requirement for all participants.

6. Conclusion

Identity federation offers enterprises, non-profit organizations and individuals an opportunity to more efficiently, securely and effectively move identity information between organizational boundaries. But it also highlights the business issues that must be addressed for wide scale federated identity to occur.

The early work of the Liberty Alliance has focused upon the technical specifications that provide the underpinnings for identity federation. As the Liberty Alliance finds the adoption of its specifications accelerating, it is now also turning its attention toward facilitating the ease of that adoption.

This document is the first in a series of "business issues" documents that will seek to provide some baseline guidance as to the issues that should be considered. This document is in no way intended to replace the advice of legal counsel. Rather, this document (and subsequent documents) serve to raise some of the issues that must be considered in the event of wide scale identity federation.

7. Roadmap of Documents to Follow

This current document is meant to serve as an overview document (Tier 1) that raises the business issues of identity federation. Further documents are planned, including:

1. The Tier 2 Scenario document – an aggregation of the significant business issues that span across the differing Liberty implementation scenarios (B2B, B2Cmobile, etc.). This document is meant to provide generic guidance as to informational sources (legislation and articles) for examining the broad business issues.

2. The Tier 3 Implementation Document – this document examines specific Liberty implementation scenarios, in both vertical and, in some case, geographic context. This document is meant to highlight the differences in business issues, as companies in differing locations and industries move through Liberty implementation. This document seeks to include case studies and perspectives from Liberty members moving through the deployment process.

The net effect of this collection of documents is to allow business partners wishing to engage in Liberty implementation to have an easy "source library" to which they can refer. These documents are not meant to replace legal documentation and process, but rather seek to highlight the business process and framework issues that federated identity presents.

8. RESOURCES

Liberty Alliance Resources:

Backgrounder
http://www.projectliberty.org/membership/LAP_Backgrounder.pdf

Current Members
http://www.projectliberty.org/membership/members.asp

Membership Benefits
http://www.projectliberty.org/membership/LAP_Member_Benefits.pdf

Liberty Enabled Products
http://www.projectliberty.org/specs/enabled_products.html

Liberty Mission, Vision & Objective
http://www.projectliberty.org/faqs/main.html#02
http://www.projectliberty.org/faqs/main.html#03
http://www.projectliberty.org/faqs/main.html#04

Identity Networks and Assorted Groups Examining Federated Identity

Shibboleth Project – Internet 2 middleware
http://shibboleth.internet2.edu/

PingID Network
http://www.pingid.com/

Securities Industry Middleware Council – Identity Management Initiative
http://www.simc-inc.org/Initiative.htm

Financial Services Technology Consortium – Liberty Alliance Business Application Review
http://www.fstc.org/projects/liberty/index.cfm

9. GLOSSARY

The following is a list of definitions that may assist a reader in understanding the general concepts presented in this paper.

Access Control

A process by which use of resources is regulated according to a security policy and is permitted by only authorized system entities according to that policy.

Access Rights

A description of the type of authorized interactions a subject can have with a resource.

Account

A formal business agreement for providing regular dealings and services between a Principal and service providers.

Account Linkage

See identity federation.

Affiliation

A group of service providers that have chosen to act as a single entity on the network from the point of view of authentication, federation and authorizations.

Attribute

A distinct characteristic of a Principal. A Principal's attributes are said to describe it.

Authenticated Principal

A Principal who has had his identity authenticated by an identity provider.

Authentication (AuthN)

The process of verifying the ability of a communication party to "talk" in name of a Principal.

Authorization (AuthZ)

A right or a permission that is granted to a system entity to perform an action.

Circle of Trust

A federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment.

Cookie

A collection of information, usually including a username and the current date and time, stored on the local computer of a person using the Web and used chiefly by Websites to identify users who have previously registered or visited the site.

Credentials

Known data attesting to the truth of certain stated facts.

Data

Any information that a Principal provides to an identity provider or a service provider.

De-federate identity

To eliminate linkage between Principal's accounts at an identity provider and a service provider, such that the identity provider no longer provides user identity to the service provider, and the service provider will no longer accept user identity from the identity provider. See also "Federated Identity."

Digital Certificate

A digitally signed assertion. The same Principal that issued the underlying assertion must sign the certificate.

Digital Signature

A data structure that strongly depends on a private key and the contents of the message being signed. Digital signatures should be uniquely verified with the corresponding public key. Note: Digital signatures are not equivalent to hand-written signatures in most respects. Note: In an international legislation context, the definition of digital signature differs broadly. See also Public-key Cryptography.

Federated Identity

An identity that has been linked via the Liberty Alliance specifications. See "Identity Federation."

Federated Identity Management

Federated Identity Management refers to the management of a digital identity *between enterprises*. See also "Identity Management."

Federate

To link or bind two or more entities together within a circle of trust.

Federated Architecture (authentication)

An architecture that supports multiple entities provisioning Principals among peers within the circle of trust.

Federation

An association comprising any number of service providers and identity providers.

Identity
The essence of an entity; often described by its characteristics or attributes.

Identity federation
Associating, connecting, or binding multiple accounts for a given Principal at various Liberty Alliance entities within a circle of trust.

Identity Management
The process of managing the "life-cycle" of a digital identity. Typically, "identity management" refers to intra-enterprise applications.

Identity Provider (IdP)
A Liberty-enabled entity that creates, maintains, and manages identity information for Principals and provides Principal authentication to other service providers within a circle of trust.

Identity Service
A service that is an abstract notion of a web service which acts upon some resource to either retrieve information about an identity or identities, update information about an identity or identities, or perform some action for the benefit of some identity or identities.

Identity Service Framework (ISF)
A framework for creating, discovery, and consuming identity services, which are web services that act upon some resource to provide information about an identity or perform some action for an identity.

Liberty Alliance guidelines
Policies defined by the Liberty Alliance and recommended to be followed for maximizing the implementation of Liberty specifications.

Liberty Alliance principles
The commitments that an identity provider or service provider must contractually agree to (if any) to be Liberty-compliant.

Liberty Architecture
An architecture that supports the technical programs and specifications to provide a single sign-on with federated identities.

Liberty-enabled client or proxy (LECP)
A Liberty-enabled client is a client that has, or knows how to obtain, knowledge about the identity provider that the Principal wishes to use with the service provider. A Liberty-enabled proxy is an HTTP proxy (typically a WAP gateway) that emulates a Liberty-enabled client.

Network Identity
The abstraction of the global set of attributes composed from all of a Principal's existing accounts.

Non-repudiation
The inability of a Principal to legally repudiate its involvement with an action or a piece of information.

Password
A secret data value, usually a character string, that is used as authentication information.

Permissions
For the purpose of this document, the term 'permissions' encompasses both access controls and usage directives, unless otherwise explicitly stated.

Principal
A Principal is an entity that can acquire a federated identity, that is capable of making decisions, and to which authenticated actions are done on its behalf. Examples of principals include an individual user, a group of individuals, a corporation, other legal entities, or a component of the Liberty architecture.

Privacy
Proper handling of personal information throughout its life cycle, consistent with the preferences of the subject.

Profile
Data comprising the broad set of attributes that may be maintained for an identity, over and beyond its identifiers and the data required to authenticate under that identity. At least some of those attributes (for example, addresses, preferences, card numbers) are provided by the Principal.

Proxy
An entity authorized to act for another.

Pseudonym
An arbitrary name assigned by the identity or service provider to identify a Principal to a given relying party so that the name has meaning only in the context of the relationship between the relying parties.

Public-key Infrastructure (PKI)
A system of certificate authorities (and, optionally, registration authorities and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of Principals in an application of asymmetric cryptography [RFC2828].

Public-key Cryptography
Set of cryptographic techniques that uses two keys: The first key is always kept secret by an entity; and the second key, which is uniquely bound to the first one, is made public. Messages created with the first key (the *private key*) can be uniquely verified with the second key (the *public key*) in a "strong" way, where the strength of the verification is so high that the messages are called *digital signatures*. Finally, messages created using the public key can be deciphered only with the corresponding private key. See Digital Signature.

Repudiation
The rejection or renunciation of a duty or obligation.

Resource
A resource is either data related to some identity or identities or service acting for the benefit of some identity or identities.

Roles
The access controls granted to a principal within a given domain. See also "Permissions" and "Identity Management."

Service Provider (SP)

An entity that provides services and/or goods to Principals.

Shared Sign-On

See “Simplified Sign-On.”

Single Sign-On (SSO)

The ability to use proof of an existing authentication session with identity provider A to create a new authentication session with identity provider B.

Simplified Sign-On

Similar to Single Sign-On; a term used by the Liberty Alliance to designate sign-on in federated domain. See also “Single Sign-On.”

Trust Circle

See also “Circle of Trust.”

Web Service

A service that uses Internet protocols to provide a service designed to be used by programs.

Note: Some of the above definitions originally appeared in the “Liberty Architecture Glossary.”