LIBERTY ALLIANCE PROJECT WHITE PAPER

Liberty Alliance & WS-Federation: A Comparative Overview

October 14, 2003

Executive Summary

This white paper serves business audiences and technology strategists who want a foundational understanding of identity and a high-level overview that contrasts the Liberty Alliance specifications and the proposed WS-Federation draft technology. Note that this analysis of WS-Federation uses information published as of September 2003 as its basis. This white paper explores:

- Reasons why business processes and Web services depend fundamentally on identity, and why an open set of specifications and business guidelines best addresses the issues and opportunities that arise from federated identity management
- The Liberty Alliance Project's business-centric approach toward federated identity management and the momentum and industry support behind the approach and deliverables
- Common elements between the Liberty Alliance Project and those proposed in the WS-Federation technology white paper
- A call for convergence between the specifications of the Liberty Alliance Project and the emerging proposals from other parties, including WS-Federation

Identity: the core of any high-value relationship

Identity represents the core of any high-value business relationship – from relationships with customers and business partners to understanding the needs of employees and devices that access valuable data and information. Identity encompasses attributes and characteristics critical to developing and deploying valuable web services. When managing identities, companies must consider the current and emerging business and policy issues of identity and data management as well as the technology implications of various authentication and authorization mechanisms. Effective identity management eliminates costs, enhances security, prevents the ever-increasing threat of identity theft, and executes new services, revenue models and business opportunities.

As transactions and data continue to move online, identity relationships prevalent in the 'offline' world must enter the online world as well. This triggers new considerations – from the need for stronger authentication for data and financial transactions to the necessity to adhere to emerging laws and regulations for the management of personal, customer or employee data. Customer service and satisfaction remain priorities. This explains why leading companies seek single sign-on systems that allow their constituents – employees, business partners and consumers, among others – to access targeted online services as easily as possible – without the burden of multiple username/password combinations. In certain scenarios, such as from a mobile terminal or handset, this burden serves as a significant barrier to entry for the majority of users.

Many companies are extending the single sign-on concept to their partners' Web sites as well as to their own Web site and those of their divisions. This exemplifies federated identity management. When implementing this type of system, one must consider how and where to store and share the pertinent identity data, and also how to address the legal and regulatory issues associated with data and commerce transactions.

Most significantly, for this type of vision to be easily implemented on a global basis a common set of technology specifications and business practices must exist that companies in various industries agree upon. The absence of such standards inhibits widespread interoperability, limiting the network effect by creating significant cost and complexity barriers to the development and deployment of federated identity services.

In September 2001, the Liberty Alliance formed to address this need for open standards. It has issued mature and robust specifications for federated identity services. Recently, five technology vendors – IBM, Microsoft, RSA, VeriSign and BEA – published a technology white paper titled "Web Services Federation Language (WS-Federation)" that outlines another potential approach for addressing certain issues in this area. It is clear, based on the available information within the draft specifications, that potential overlap exists with the specifications of the Liberty Alliance Project. This overlap is detailed later in this white paper.

Liberty's business-centric approach to identity standards

The Liberty Alliance's membership comprises leaders in many industry sectors including technology, financial services, telecommunications, mobile services, government and manufacturing. The Liberty Alliance Project remains the only global organization actively working to address the technical, business and policy issues associated with identity and federated identity management.

> *"Business issues [for federated identity] are more complicated than technical issues"*
> *-Burton Group, "Federating ID – Why and When," July 2003*

When Liberty set out to establish a standard means for federated identity management, it recognized that technology constitutes only part of the challenge. Therefore, it put business

issues at the core of its development and output, basing each of its specifications on a business use case articulated in Market Requirement Documents (MRDs). These market requirements reflect the use of technologies for identity-management solutions that satisfy business, policy and regulatory needs. The Alliance, working from a platform of these requirements, strives to utilize technologies from other open bodies in the industry, such as the W3C and OASIS. As such, the Alliance's technical specifications reuse and build upon output and works in progress from such organizations as SAML, WS-Security, SOAP, and XML.

When parties seek to form a business relationship, some form of contractual agreement typically underpins that relationship. With this in mind, the Alliance has developed Business Guidelines that serve as inputs into such contractual agreements, driving to reduce the amount of contractual review required for a company to participate in business relationships built upon the use of federated network identity. The first set of Guidelines highlights such issues as liability, risk, mutual confidence and compliance. Future Business Guidelines will focus more granularly on specific industries and regions.

Liberty Alliance adoption, momentum and proven interoperability

The Liberty Alliance, by its nature, commits itself to open, tested and proven standards. The mature Liberty ID-FF (Identity Federation Framework) specifications, released in July 2002, emerged after eighteen months of broad collaboration, public review and numerous interoperability tests by multiple vendors. Likewise, ID-WSF (Identity Web Services Framework), released with the second phase of Liberty Alliance work, reflects more than a year of active work by members representing both the vendor community and major end-user companies.

Liberty Alliance's comprehensive and rigorous approach has triggered substantial support and adoption throughout the industry. As of July 2003, more than 20 technology vendors have released products and services that allow companies to implement the Liberty protocols for federated identity management. Many leading organizations, including General Motors and American Express, have begun internal Liberty implementations. Several additional products and internal installations are slated for completion and shipping by the end of 2003, indicating sustained, growing global support for the specifications.

An ongoing commitment to development of open standards

Reflecting its mission to develop and deliver a comprehensive set of standards for federated identity, the Liberty Alliance commits to working with organizations with complementary efforts. For example, the Alliance submitted its Identity Federation Framework protocols (part of the 1.1 Liberty specification) to OASIS for consideration in SAML 2.0. In addition, Liberty has engaged in dialogue with industry standards efforts such as the Open Mobile Alliance (OMA), the Open Group and OASIS.

With the release of the WS-Federation technical white paper, the Alliance conducted an analysis to assess areas of overlap and reinvention and to determine possible points of convergence.

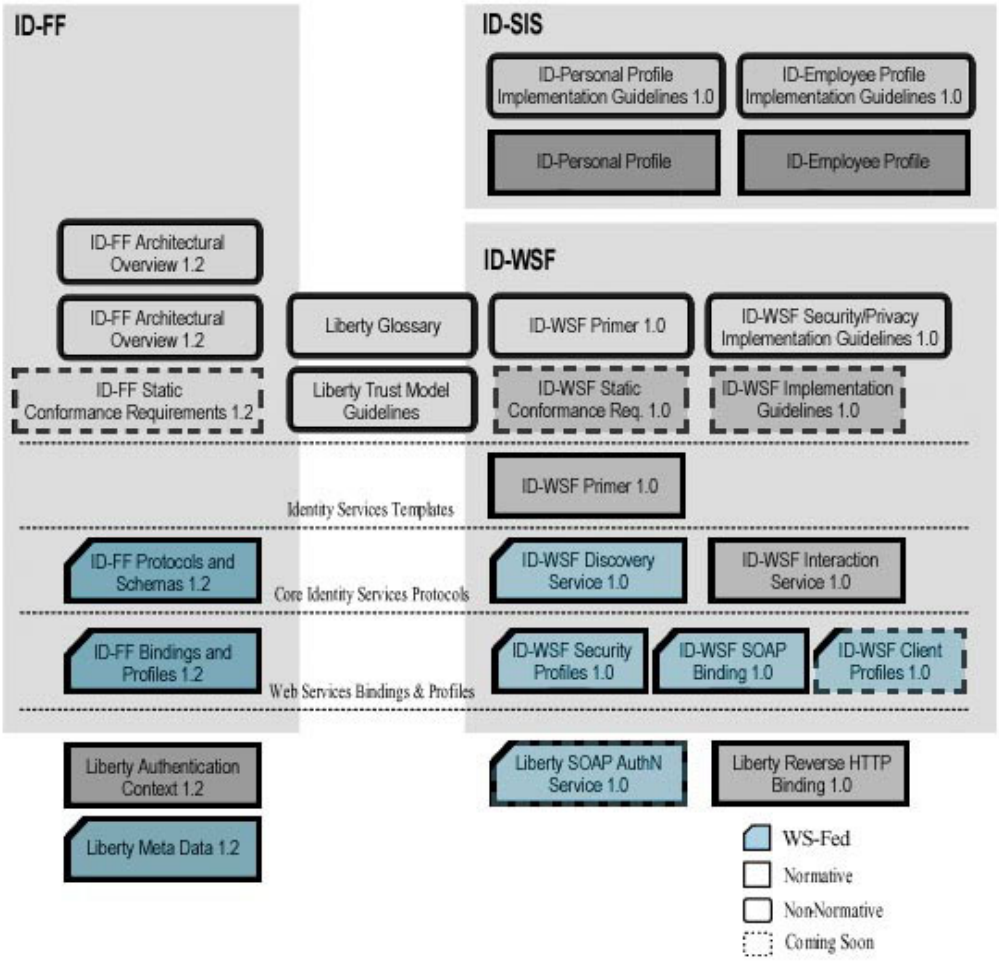
Clearly, opportunities exist for convergence. As previously stated, Liberty has adopted a strong policy in its technical work to seek to reuse technologies available from other open standards organizations. Liberty Alliance members call upon others within this industry to follow a similar path. This would help to limit conflicting efforts that distract the industry and impede delivery of identity-based web services.

Comparative Analysis between Liberty Alliance and WS-Federation Specifications

Based upon review of the WS-Federation white paper, it appears this more recent effort seeks to replicate some, but not all, of the Liberty Alliance specifications as an alternative means to implement federated identity services.

Detailed below are the building blocks of the Liberty specifications. The highlights (blue boxes with cut on top left corner) denote those components of the Liberty architecture that WS-Federation also proposes to address in some form as presented in its technical white paper. A more detailed comparison of these overlapping technical components resides in table form at the end of this document. It is important to note that since WS-Federation is in its early stages of development and still evolving, the nature of the identity information it supports is still unclear. This presents a review challenge comparing the exact scopes of the two specifications.

Liberty Alliance Project Phase 2 Draft Specifications



Privacy

Respecting an Identity's privacy represents a fundamental tenet of the Liberty Alliance and provides an important focus across all types of businesses and identity implementations (i.e. B2E, B2B, and B2C). The Liberty Alliance has a Public Policy Expert Group that actively engages with leaders in government, consumer and privacy advocacy groups. This ongoing work on current and emerging privacy issues and regulations positively impacts the development of specifications and business guidelines sensitive to these issues.

Liberty's ID-WSF specifications aim to ensure privacy by recommending access-control policies on attribute information and by allowing for the placement of usage directives on released attributes. This technology allows users of the Liberty specifications to federate or link the accounts of customers who have opted-in, without exchanging any personal identity information. When a user federates their account in an identity implementation that supports the Liberty specifications, the pseudonyms linking concept creates a random identifier that is unique to that relationship, ultimately avoiding a global identifier and providing an added layer of security to the process. The Liberty Alliance was presented with the Digital Identity Industry Award based on this "pseudonyms linking" approach at Digital ID World in October 2002.

At this time, the WS-Federation proposal does not specify privacy mechanisms (e.g. encryption of pseudonyms) to the extent of the Liberty Alliance's specifications. WS-Federation defers to WS-Policy (and presumably WS-Privacy, for which details are unavailable) for optional access controls on personally identifiable information (PII). It introduces a Pseudonym Service to manage (optional) privacy-protecting identifiers.

Specification Commonalities and Differences

At the specification level, Liberty's Federation Framework (ID-FF, ID-WSF, and ID-SIS) and WS-Federation share some core principles and mechanisms, including:

1. Distinguishing between browser and smart clients (although the nature of these clients likely differs) through profiles of basic messaging protocols.
2. Trust brokering through the issuance of *security tokens.*
3. Privacy-controlled attribute sharing
4. Rudimentary session management through federated sign-out.

The means of applying these principles, however, differ largely in approach and in underlying technologies. The matrices below present these differences in further detail:

	Feature / Functionality	Liberty Alliance Project	WS-Federation
Areas of overlap with similar technical approaches	Client profiles	Specifies client profiles for both browser and smart clients	Specifies client profiles for both browser and smart clients
	SSO control flows	SSO control flows specify both front-and-back channel mechanisms	SSO control flows specify and strongly recommend the front-channel mechanism and mentions, but discourages use of "pointer-based" back-channel mechanisms

	Feature / Functionality	Liberty Alliance Project	WS-Federation +
Areas of overlap with divergent technical approaches	Account federation	Account federation via Identity Mapping enabled by opaque identifiers (a key privacy feature)	Account federation via Identity Mapping enabled by the Pseudonym Service
	Privacy	Privacy controls are written into the specifications (Recommend access-control policies, usage directives, and pseudonymity)	Optional privacy support by deferring to WS-Policy (and presumably WS-Privacy) for access controls
	Security Tokens	Extends SAML assertions for communicating authentication and authorization security tokens between providers	Builds on WS-Security's profiles of X509v3 and Kerberos for communication of security tokens
	Business & Policy Issues	Addresses business issues tied to establishing trust via Business Guidelines and authentication context	Makes no attempt to address the business trust issues at this time
	Underlying Technology	Underlying technology extends and builds on SAML and relies on SSL and WS-Security for transport and message security	Underlying technology builds on WS-Trust, WS-Policy and WS-Metadata foundation and relies on SSL and WS-Security for transport and message security

	Feature / Functionality	Liberty Alliance Project	WS-Federation
General Differences between Liberty and WS-Federation	Approach	Developed by an open standards community that includes vendors, end-users and non-profit organizations	Developed by Microsoft, IBM, VeriSign, BEA and RSA Security
	Scope	Holistic focus on technology, business and policy issues associated with federated identity services	Focus on technology specifications for federated identity services
	Maturity	A mature specification developed collaboratively over the past two years; over 20 implementations supporting Liberty specs at time of publishing	Currently in early draft stage; no available vendor implementations at this time
	Public review/access to specs	Specs have undergone broad public review and multiple interoperability testing by many vendors and end-users	No public review and comment mechanism
	Implementation costs	Specs are free to implement in products and services *http://www.projectliberty.org/specs/ipr.html*	Specs free to review; implementation and distribution costs unknown (white paper states: "the authors do not grant, either expressly or impliedly, a license to any intellectual property, including patents, they own or control" *http://www-106.ibm.com/developerworks/webservices/library/ws-fed/*

Conclusion

The two-year-old Liberty Alliance Project addresses the need for an open industry standard for federated identity management. Liberty recognizes the interests and the effort of the technology vendors proposing WS-Federation, and welcomes the authors' input into further development of the Liberty Alliance specifications. Liberty encourages these vendors to consider the substantial progress already made by the 160-plus organizations involved with the Liberty Alliance, and to evaluate the overall benefits of a converged solution (open industry standard, economies of scale, faster product development, same-user experience irrespective of the technology used, faster adoption, etc.)

To achieve these benefits for the whole industry, Liberty Alliance calls for a series of public workshops to discuss a path toward convergence. Liberty Alliance is willing to drive, co-sponsor or attend these meetings and, in the best interest of its members, urges that they occur as quickly as possible.

Appendix: Detailed technical analysis between Liberty Alliance and WS-Federation:

Category	Component	Liberty	WS-Federation +
Linkage	Account Linking	ID-Federation Framework	Yes, through Set messages of Pseudonym Service
Single Sign On	Authentication Request	SAML Request	WS-Trust Token Issuance Request
	Authentication Response	SAML Response	WS-Trust Token Issuance Response
	Assertion	SAML Authentication Statement	Arbitrary tokens
	Authentication Details	Authentication Context can be specified on request and response	
	Profiles	Browser Artifact, Form POST, LEC	Passive and Active with variations
Session	Single Logout initiated by IDP	Yes	Yes
	Single Logout initiated by SP	Yes	Yes
	Session Credentials		WS-SecureConversation
Privacy	Opaque Identifiers	Yes	Optional (can use non-opaque & persistent identifiers)
	Management	NameRegistration protocol	Yes, through Set messages of Pseudonym Service
	Policy for released attributes	Usage Directives	
	Encrypted identifiers and URIs	Yes	
Authorization	Authorization Request	Implicit	WS-Trust
	Authorization Response	Implicit	WS-Trust
	Attributes (roles)		Yes
Trust	Legal Agreements	Can be referenced from Authentication Context	
	Business agreements	Can be referenced from Authentication Context	
	Affiliations	Yes	
	Introduction	See below	
	Token Exchange/Mapping		WS-Trust

Category	Component	Liberty	WS-Federation +
Security	Message Security	XML Signature/XML Encryption/WS-Security protected messages	XML Signature/XML Encryption/WS-Security protected messages
Metadata	Publishing	DNS & Known location; Can be published in UDDI directory	
	Retrieval	DNS & Known location	
	Schema	ID-WSF Metadata	WS-MetadataExchange
Discovery	Principal IDP	Common Domain cookie	
	Publishing	ID-WSF DiscoveryLookupUpdate	UDDI
	Query	ID-WSF DiscoveryLookupRequest	UDDI
	Security Policy		WS-SecurityPolicy
Introduction	Trust brokering	Yes	WS-Trust
	Notification of Principal Federation	Yes	
	Notification of trust termination	Yes	
Information Sharing	Access	Yes, Identity Service	Attribute Service
	Store		UDDI
	Privacy policy	Privacy Policy Expression Language	WS-Privacy?
	Data manipulation	WSF Data Service Template	Not in WS-Federation, perhaps .Net My Services HSDL
	Data interface	ID-Personal Profile	Not in WS-Federation, perhaps .Net My Services?
	Brokering	Yes	
User Interaction	User Consent	ID-WSF Interaction Service	
	Federation termination	Yes	