LIBERTY ALLIANCE PROJECT

INTRODUCTION TO THE LIBERTY ALLIANCE IDENTITY ARCHITECTURE

Revision 1.0
March, 2003

http://www.projectliberty.org/

Iden·ti·ty [noun]: The distinguishing character or personality of an individual.

Abstract:

This paper provides a brief overview of the Liberty Alliance's federated network identity management architecture. 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.

The Current Environment

From the moment a person is born, they have an "identity." The identity starts with their name on a birth certificate and evolves over time as labels, interactions, and relationships are associated with that person. As people grow, they interact with an ever-larger group of individuals and organizations. While their family and friends have a deep and complex understanding of who they are, the organizations with which they interact know them as little more than a number.

Fast-forward to the grown up and modern world, pieces of their 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. Pieces of their identity are doled out across the many computer systems and networks used by employers, Internet Service Providers, bulletin boards, instant messaging applications, and online commerce and content providers. This all occurs with little coordination, interaction, or control on their part.

The result is a fairly high level of frustration for everyone involved. People have to repeatedly enter the same information within the workplace and in personal business dealings. The IT manager must provision dynamically changing accounts to reflect up-to-date roles and identities within the organization. The sales executive needs to reach the audience with the right identities to sell a product.

Everyone concerned may also have to deal with identity abuse. This can be something as "harmless" as unsolicited E-mail communications to something as costly as identity theft (which the Federal Trade Commission reports as the top "white collar" crime in the United States). Add to these frustrations the fact that these personal and business relationships and identities are continuously changing, and the challenge explodes.

What is Identity?

As defined in the dictionary, iden·ti·ty [noun] is the distinguishing character or personality of an individual.

An *identity* consists of traits, attributes, and preferences upon which one may receive personalized services. Such services could exist online, on mobile devices, at work, or in many other places. This is shown in Figure 1.

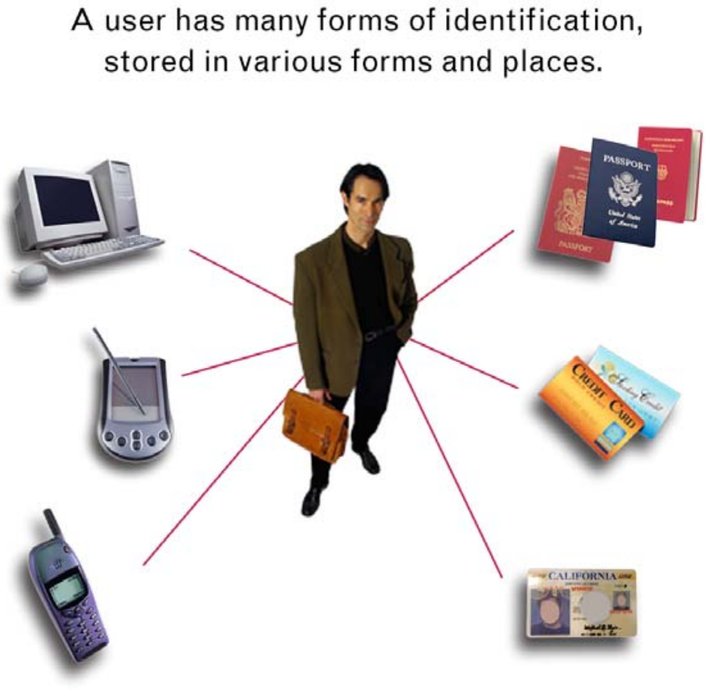
A user has many forms of identification,
stored in various forms and places.

Figure 1. The Various Forms of Identification

Traits are identities issued by governments (driver's license, passport, national ID cards, etc.), identities defined for an individual by companies, such as employee status and intranet sign-in information, and biometric characteristics such as fingerprints or retina scans.

Attributes and *preferences* are those characteristics associated with an individual such as a person's airline seating preferences (window seat vs. aisle seat), music preferences ("jazz" could be a style someone listens to and shops for), purchasing history, or medical history. Attributes and preferences can go beyond individuals and can include devices and processes, as well. For example, they could define a type of device (phone vs. desktop vs. kiosk) and its capabilities (text vs. HTML vs. audio).

The traits, attributes, and preferences that define individuals make up their identity, while the relationship of the individual with an entity determines which elements of the identity should be shared.

This maintenance of privacy and identity control is paramount in the Internet world, yet users also demand ease-of-use and rapid access. What is the best way to balance the two needs? By establishing a *federated network identity* that links the various user identities together.

A federated network identity delivers the benefit of simplified sign-on to users by granting rapid access to resources to which they have permission, but it does not require the user's personal information to be stored centrally. This increases security and delivers better identity control. With a federated network identity approach, users authenticate once and can retain control over how their personal information and preferences are used by the service providers. A federated network identity is also beneficial for businesses because it allows them to more easily conduct business transactions with authenticated employees, customers and partners.

The group of service providers that share linked identities and have business agreements in place is known as a *circle of trust*. The attribute sharing policies within a circle of trust are typically based on the following:

- A well-defined business agreement between the service providers
- Notification to the user of information being collected
- User granting consent for types of information collected
- Where appropriate, recording both notice and consent in an auditable fashion

The Need for Federated Network Identity

To address the inefficiencies and complications of network identity management for businesses and consumers in today’s world, there is a strong need for *a federated network identity* infrastructure that allows users to “link” elements of their identity between accounts without centrally storing all of their personal information.

There are many benefits to a federated network 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 identity information.

- Enables the IT manager to more easily and securely provision accounts and provide 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.

This is what the Liberty Alliance is all about. 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.

The Liberty Alliance was formed in December 2001 to serve as the premier open standards organization for federated network identity management and identity-based services. Its goals are to ensure interoperability, support privacy, and promote adoption of its specifications, guidelines, and best practices. The Alliance has grown from under 20 companies in 2001 to more than 160 companies in early 2003. These companies represent a worldwide cross-section of organizations, ranging from educational institutions and government organizations, to service providers and financial institutions, to technology firms and wireless providers.

The Liberty Alliance Specification Architecture Overview

The Liberty Alliance is developing and delivering specifications that enable federated network identity management. The work of the Alliance is ambitious and is occurring on several fronts simultaneously. Because of this, the vast majority of questions are centered on how future versions of the technical specifications will build upon the work that has been previously published. In other words, what is the architectural "blueprint"?

Figure 2 shows a high-level overview of Liberty Alliance Architecture modules.

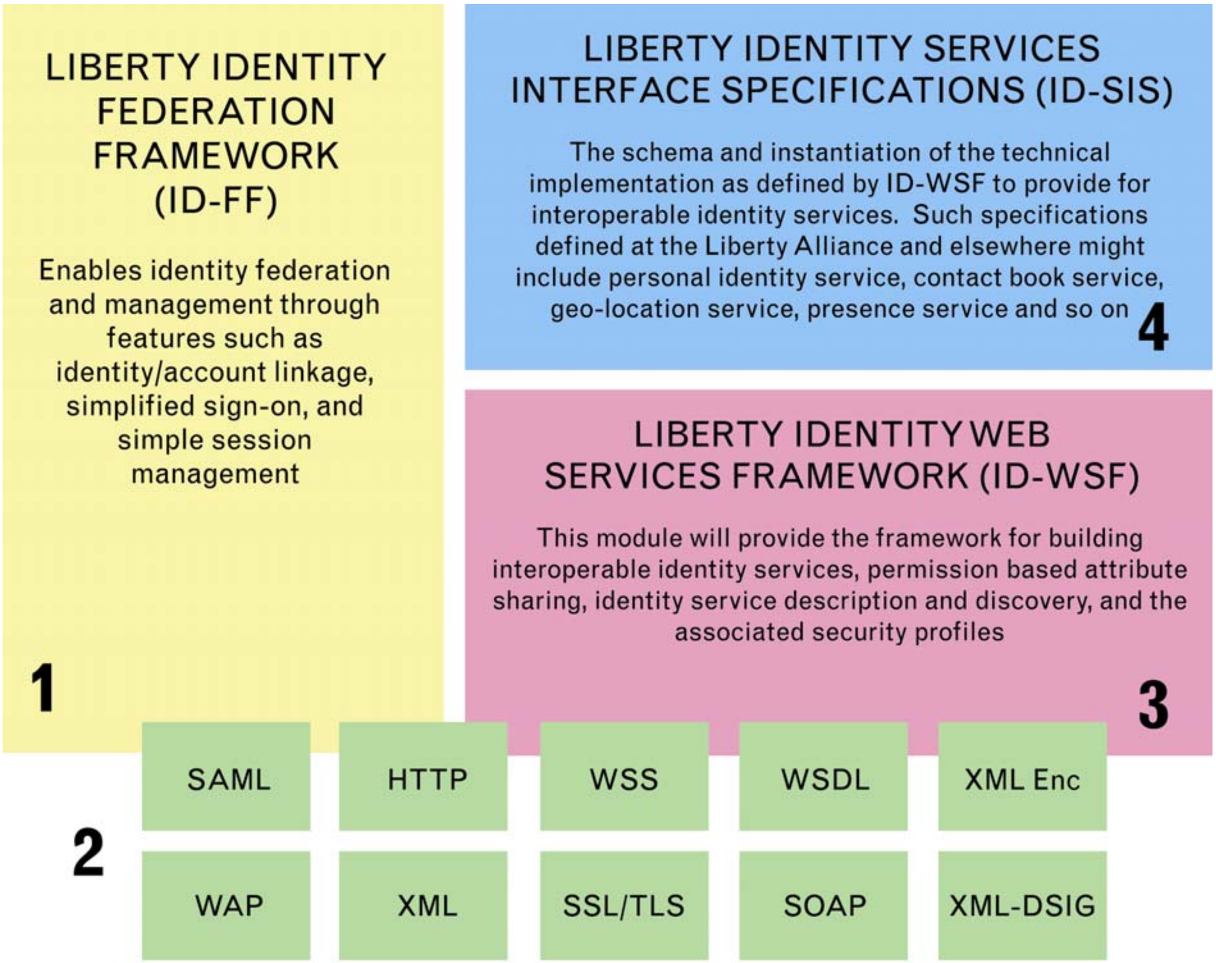
LIBERTY IDENTITY FEDERATION FRAMEWORK (ID-FF)
Enables identity federation and management through features such as identity/account linkage, simplified sign-on, and simple session management
1
LIBERTY IDENTITY SERVICES INTERFACE SPECIFICATIONS (ID-SIS)
The schema and instantiation of the technical implementation as defined by ID-WSF to provide for interoperable identity services. Such specifications defined at the Liberty Alliance and elsewhere might include personal identity service, contact book service, geo-location service, presence service and so on
4
LIBERTY IDENTITY WEB SERVICES FRAMEWORK (ID-WSF)
This module will provide the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles
3
2
SAML
HTTP
WSS
WSDL
XML Enc
WAP
XML
SSL/TLS
SOAP
XML-DSIG

Figure 2: High-Level Overview of the Liberty Alliance Architecture

Each of the major modules is discussed in the sections that follow.

Module 1: Liberty Identity Federation Framework (ID-FF)

The Liberty ID-FF enables identity federation and management. It can be used on its own or in conjunction with existing identity management systems. This framework is designed to work with heterogeneous platforms and with all types of network devices, including personal computers, mobile phones, PDAs and other emerging devices.

ID-FF includes the following specific features:

- **Opt-in Account Linking**

  Allows a user with multiple accounts at different Liberty enabled sites to link these accounts for future authentication and sign-in at these sites (i.e. federation).

- **Simplified Sign-On**

  Allows a user to sign-on once at a Liberty ID-FF enabled site and to be seamlessly signed-on when navigating to another Liberty-enabled site without the need to authenticate again. Simplified sign-on is supported both within a circle of trust and across circles of trust.

- **Fundamental Session Management**

  Enables companies or organizations that link accounts to communicate the type of authentication that should be used when a user signs-on. It also enables "global sign-out", i.e., once users sign-out of a Liberty-enabled site, they can be automatically signed-out on all the sites they've linked to in that session.

- **Affiliations**

  Enables a user to choose to federate with a group of affiliated sites, which is critical in addressing the needs of portals and in the business-to-employee environment.

- **Anonymity**

  Enables a service to request certain attributes without needing to know the user's identity. For example, in order to provide personalized weather information to a user, a weather service provider can ask for a user's zip code using anonymous service request without knowing the identity of that user.

- **Protocol for the Real-time Discovery and Exchange of Meta Data**

  For providers to communicate with each other, they must have previously obtained metadata regarding each other such as X.509 certificates and service endpoints. This feature of the ID-FF facilitates the real-time exchange of this information between Liberty-compliant entities.

Module 2: Adopting and Extending Other Industry Standards

The Alliance consciously continues to adopt and extend appropriate industry standards, rather than attempting to develop similar specifications. Each phase of the specification process draws upon work already conducted by the Organization for the Advancement of Structured Information Standards (OASIS), World Wide Web Consortium (W3C), and Internet Engineering Task Force (IETF) for the standards such as:

> SAML, WS-Security, HTTP, WSDL, XML, SOAP, XML-ENC, XML-SIG, SSL/TLS, and WAP

Module 3: Liberty Identity Web Services Framework (ID-WSF)

ID-WSF is a foundational layer that will utilize the Identity Federation Framework. Liberty ID-WSF defines a framework for creating, discovering, and consuming identity services. It will allow entities to offer users personalized and more valuable services. As with ID-FF, ID-WSF will continue to profile and use industry-leading security specifications to provide the maximum level of security for businesses, governments and users.

Figure 3 shows an overview of ID-WSF.

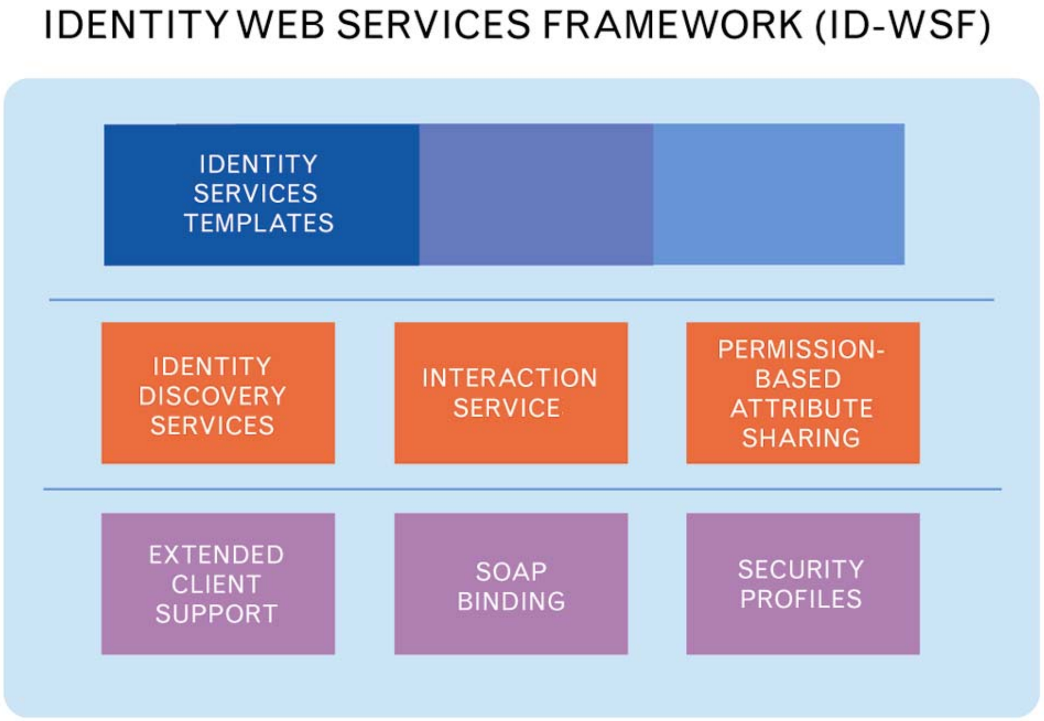
IDENTITY WEB SERVICES FRAMEWORK (ID-WSF)
IDENTITY SERVICES TEMPLATES
IDENTITY DISCOVERY SERVICES
INTERACTION SERVICE
PERMISSION-BASED ATTRIBUTE SHARING
EXTENDED CLIENT SUPPORT
SOAP BINDING
SECURITY PROFILES

Figure 3: Overview of ID-WSF

A few of the key features offered in ID-WSF include:

- **Permission Based Attribute Sharing**

  This feature will allow a company or organization to offer users individualized services based on attributes and preferences that the user has chosen to share. Protocols enable a dialogue to take place between an attribute provider and service provider regarding the exchange of attribute information. Protocols are also used to obtain permission from a user to share information and define the way in which it can be used.

- **Identity Service Discovery**

  In order for a service provider to offer an identity-enriched service to a user, it needs to gain access to portions of the user's identity information that may be distributed across multiple providers. The service provider can use the discovery service to ascertain the location of a specific identity service for a user. The discovery service enables various entities to dynamically and securely discover a user's identity services, and it responds, on a permission-basis, with a service description of the desired identity service.

- **Interaction Service**

  An identity service may need to obtain permission from a user (or someone who owns a resource on behalf of that user) to allow them to share data with the requesting services. The interaction service specification details protocols and profiles for interactions that allow services to carry out such actions.

- **Security Profiles**

  This specification describes profiles and requirements for securing the discovery and use of identity services. It includes security requirements to both protect privacy, and to ensure integrity and confidentiality of messages between service providers.

- **Simple Object Access Protocol (SOAP) Binding**

  The ID-WSF SOAP Binding provides a SOAP-based invocation framework for identity services. It defines SOAP Header blocks and processing rules enabling the invocation of identity services via SOAP requests and responses. Additionally, a usage directive container is defined for those implementations that wish to use an existing rights expression language to specify the required service and data usage policies.

- **Extended Client Support**

  Extended Client Support enables hosting of Liberty-enabled identity based services on devices without requiring HTTP servers or being IP addressable from the Internet. This is useful since many of today's devices have an HTTP client but do not have a server either because of memory, processing constraints, or not being IP reachable from the Internet.

- **Identity Services Templates**

  Identity Services Templates provide the building blocks for implementing an identity service (e.g. Personal Profile Identity service) on top of the Identity Web Services Framework. The specifications define how to query and modify data stored in identity services.

Module 4: Liberty Identity Services Interfaces Specifications (ID-SIS)

Identity Services Interface Specifications are a collection of specifications for interoperable services to be built on top of Liberty's ID-WSF. These might include services such as registration, contact book, calendar, geo-location, presence or alerts. These independent services will be made interoperable through implementing Liberty protocols for each specific service. The specifications will be written in such a way that organizations can quickly and easily extend existing Liberty Identity services, or create additional services that build upon the ID-WSF framework. Specifications for identity services might also be written by other standard bodies working with the Liberty Alliance.

The first ID-SIS to be made available will be the Personal Profile Identity Service (ID-Personal Profile). This service defines schemas for basic profile information of a user. This usually includes name, legal identity, legal domicile, home and work addresses and can also include phone numbers, email addresses, and some demographic information, public key details, and other online contact information. By providing organizations with a standard set of attribute fields and expected values, they will have a dictionary or a common language to speak to each other and offer interoperable services.

This and future services are designed to be built on top of web services standards, meaning they are accessible via SOAP over HTTP calls, defined by WSDL descriptions, and use agreed-upon schemas.

Roadmap to Interoperable Federated Network Identity Services

Bringing value to individuals and businesses in terms of convenience, cost savings, new business opportunities, productivity, and investment protection is what drives the need for federated network identity and the Liberty Alliance. As such, the Liberty Alliance has committed itself to ensuring that it publishes work every six to nine months. The Alliance has focused on publishing open technical specifications that:

- Enable federated network identity solutions that solve real and pressing business problems.
- Enable interoperability between disparate identity systems.
- Ensure consumer privacy and security needs can be met.
- Provide a flexible and extensible foundation.
- Build on and extend existing standards where possible.
- Anticipate both consumers' and businesses' future identity management needs.

The Liberty Alliance released its first set of open specifications for federated identity management in July 2002. This release was followed by a minor enhancement release in January 2003.

The Liberty Alliance is developing and delivering specifications in a phased approach to allow for fast and easy implementation of identity-based solutions. Each new release will build upon the last, providing richer functionality without requiring implementers to start over.

Additionally, the Liberty Alliance continuously examines the work of other standards bodies, looking for ways to adopt and extend current standards. It works with organizations to drive interoperability and convergence of emerging and existing network identity-related specifications. The Liberty Alliance strives to ensure that its work does not duplicate or conflict with the relevant work of other external, vendor neutral industry groups and standards organizations. Liberty Alliance also develops specifications and guidelines that support the range of fair information practices required within different jurisdictions and industries.

Figure 4 shows the high level roadmap for the Liberty Alliance Specifications.

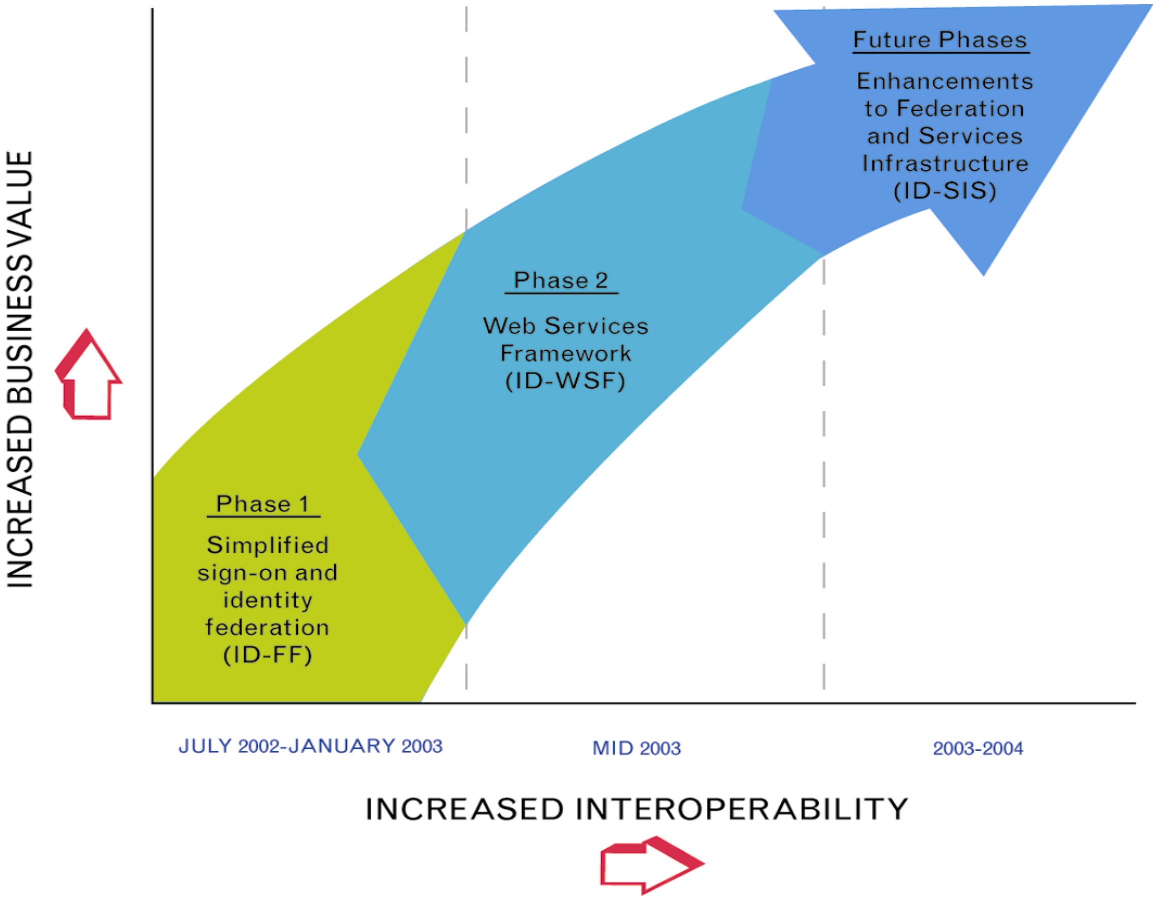
INCREASED BUSINESS VALUE
Future Phases
Enhancements to Federation and Services Infrastructure (ID-SIS)
Phase 2
Web Services Framework (ID-WSF)
Phase 1
Simplified sign-on and identity federation (ID-FF)
JULY 2002-JANUARY 2003
MID 2003
2003-2004
INCREASED INTEROPERABILITY

Figure 4. Roadmap to Interoperable Federated Identity Services

Phase 1 of the Liberty Alliance's work enabled federated network identity management. Among other features, it provided standards for single sign-on and linking of separate accounts within a group of service providers in a circle of trust. With phase 1, entities can allow their users to sign-on to an existing account with a member of a circle of trust once, and then navigate to various sites among that group without signing-on again. Phase 1 specifications provided the plumbing for a federated network identity management approach. This body of work is referred to as the Liberty Alliance's Identity Federation Framework (ID-FF).

Phase 2 of the Liberty Alliance specifications (due in mid-2003) will provide key features to enhance identity federation and enable interoperable identity-based web services. This new body of work is the Liberty Alliance's Identity Web Services Framework (ID-WSF). The Liberty Alliance will continue to evolve this framework, including its ability to utilize and support new open standards such as the WS-Security specifications being developed in OASIS (WSS Technical Committee).

Future specifications will rely upon the foundation that ID-WSF provides to build additional interoperable identity services such as registration services, contact books, calendar services, geo-location services, presence services, notification or alert services, etc. These specifications will be referred to as the Liberty Alliance's Identity Services Interfaces Specifications (ID-SIS).

In 2003, the Alliance will also introduce the first of several identity service specifications that make use of the ID-WSF. These specifications will provide interfaces and schemas for companies and organizations that want to build interoperable identity-based services.

The first identity service specification that will be released is the Personal Profile identity service (ID-Personal Profile).

Summary

This document has outlined the Liberty Alliance's vision for federated network identity management and has provided an initial view into the Liberty Alliance Identity Architecture. This Architecture is comprised of three major components, the Identity Federation Framework (ID-FF), the Identity Web Services Framework (ID-WSF) and the Identity Services Interfaces Specifications (ID-SIS). The ID-FF is available now and can be accessed through http://www.projectliberty.org/ site. The ID-WSF and the first ID-SIS (ID-Personal Profile) public availability will follow shortly.

The Alliance has continuously sought to gather requirements from its members and industry to serve as input into the development of specifications that solve the real business issues and challenges in the space of federated network identity management.

The work of the Liberty Alliance allows companies to increase the security of their information systems, lower maintenance cost of their infrastructure and provide flexibility to match their need for new business models across different technologies and services providers.

The Liberty Alliance has moved quickly to deliver key technologies to its members and the wider industry. The Liberty Alliance's ID-FF, ID-WSF and future Identity service specifications provide a comprehensive solution for federated network identity management.

For more information on the Liberty Alliance specifications and new member inquiries, please contact:

The Liberty Alliance Project
1-732-465-6475
liberty-admin@projectliberty.org