



Liberty Alliance & Network Identity Overview

Fulup Ar Foll
Chief Architect Office
Professional Services
Sun Microsystems, Inc.



Contents

- Liberty Alliance Definition and Concepts
- Liberty Organization
- Liberty Competition and Interoperability
- Liberty Specifications
- Liberty Platform Environment
- Sun's Network Identity Approach
- Sun Infrastructure Solution for Network Identity

What is Liberty ?

- A business alliance, formed in Sept 2001 with the goal of establishing an open standard for federated identity management
- Global membership consists of consumer-facing companies and technology vendors as well as policy and government organizations
- The only open organization working to address the technology and business issues of federated identity management
- <http://www.projectliberty.org/>



The Value of Liberty Alliance

- Privacy and security of consumer identity
- Federated authentication for SSO accross multiple independent providers
- Control of own customer relationships for organizations
- Network Identity infrastructure that supports all current and emerging network access devices



Defining Liberty

Liberty Alliance IS...

- IS a member community delivering technical specifications, business and privacy best practices
- IS providing a venue for testing interoperability and identifying business requirements
- IS developing an open, federated identity standard that can be built into other companies' branded products and services
- IS driving convergence of open standards

Liberty Alliance IS NOT

- IS NOT a consumer-facing product or service
- IS NOT developed and supported by one company
- IS NOT based on a centralized model



Liberty Alliance Membership

- More than 170 member organizations globally
- Driven by end-users, government orgs and vendors
- Led by Technology, Business and Public Policy Exprt Groups

Novell

Entrust
Securing the Internet

AMERICA
Online

 **Consignia**

**Deloitte
Touche
Tohmatsu**

EDS

hp
invent

ERICSSON

Bank of America

 **Communicator Inc**

Fidelity Investments

 **france telecom**


GEMPLUS

GM

Intuit

MasterCard

NEC

NEUSTAR

NTT Do Co Mo

Netegrity

NEXTEL

**AMERICAN
EXPRESS**

NOKIA

 **NTT Group**

 **OPENWAVE™**

Schlumberger

PingID

PRICEWATERHOUSECOOPERS

 **PHAOS**

**RSA
SECURITY**

SAP

SK Telecom

SONY

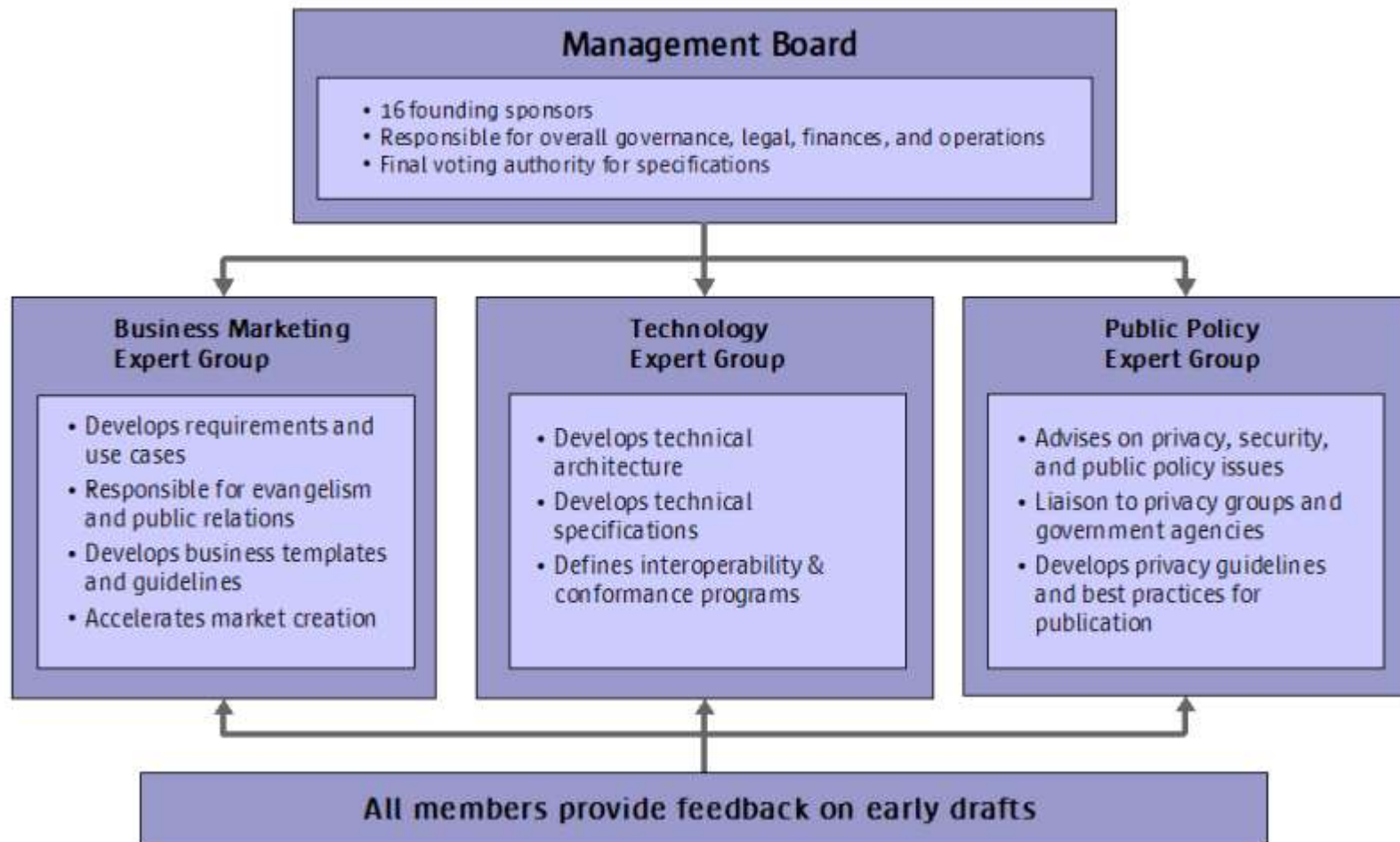
 **Sun**
microsystems

VeriSign
The Sign of Trust on the Net

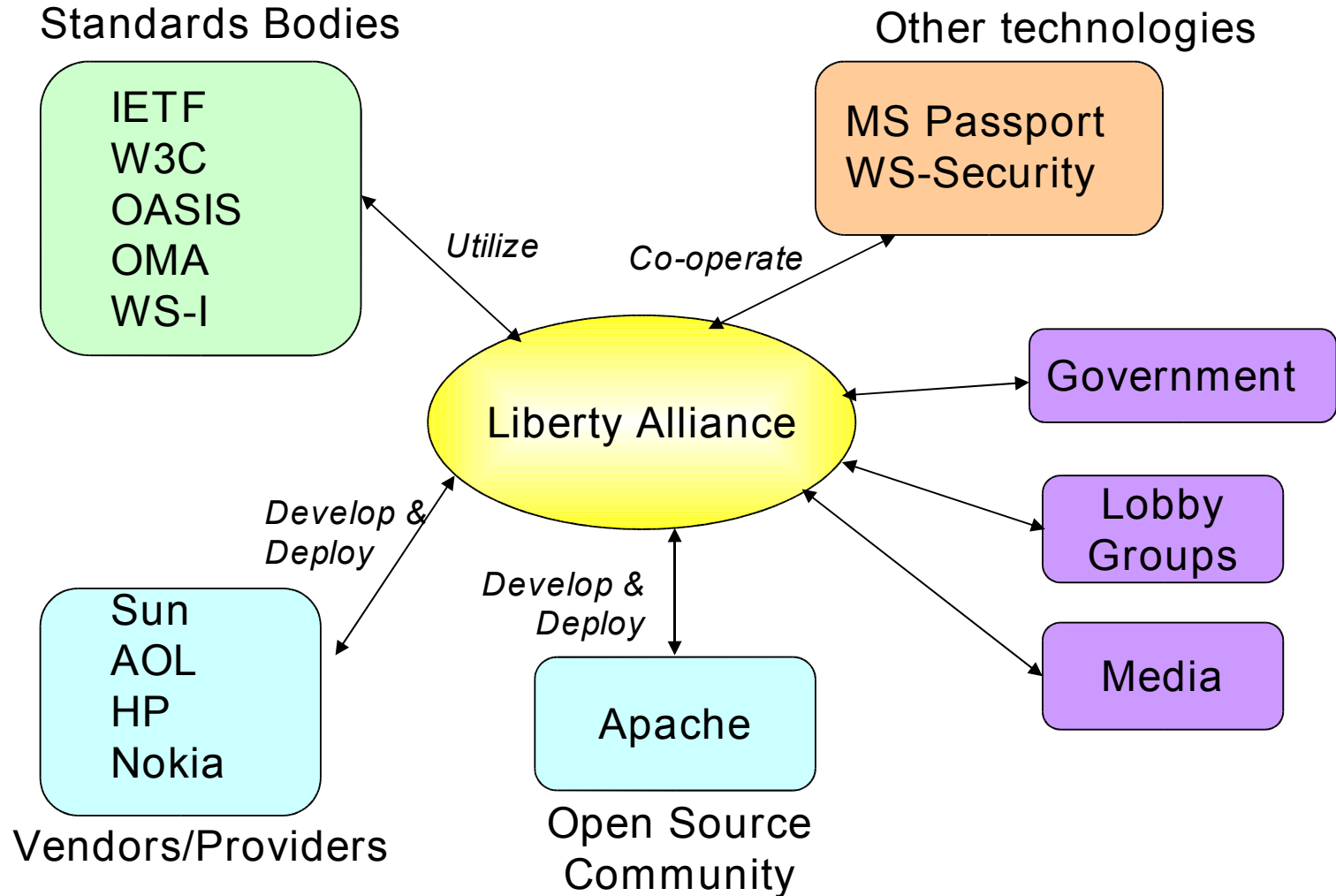
VISA

vodafone

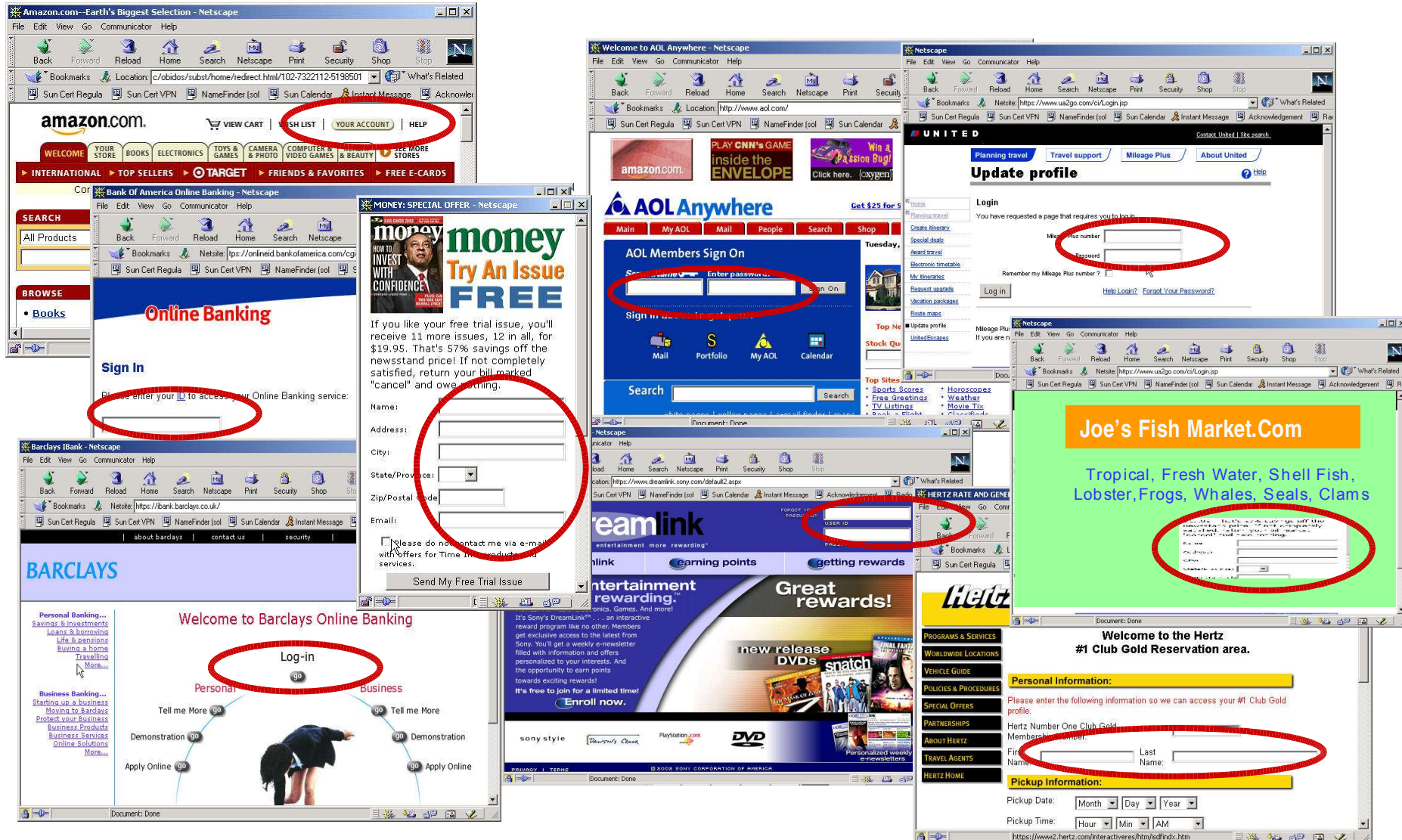
Liberty Alliance Structure



Open Interaction and Participation



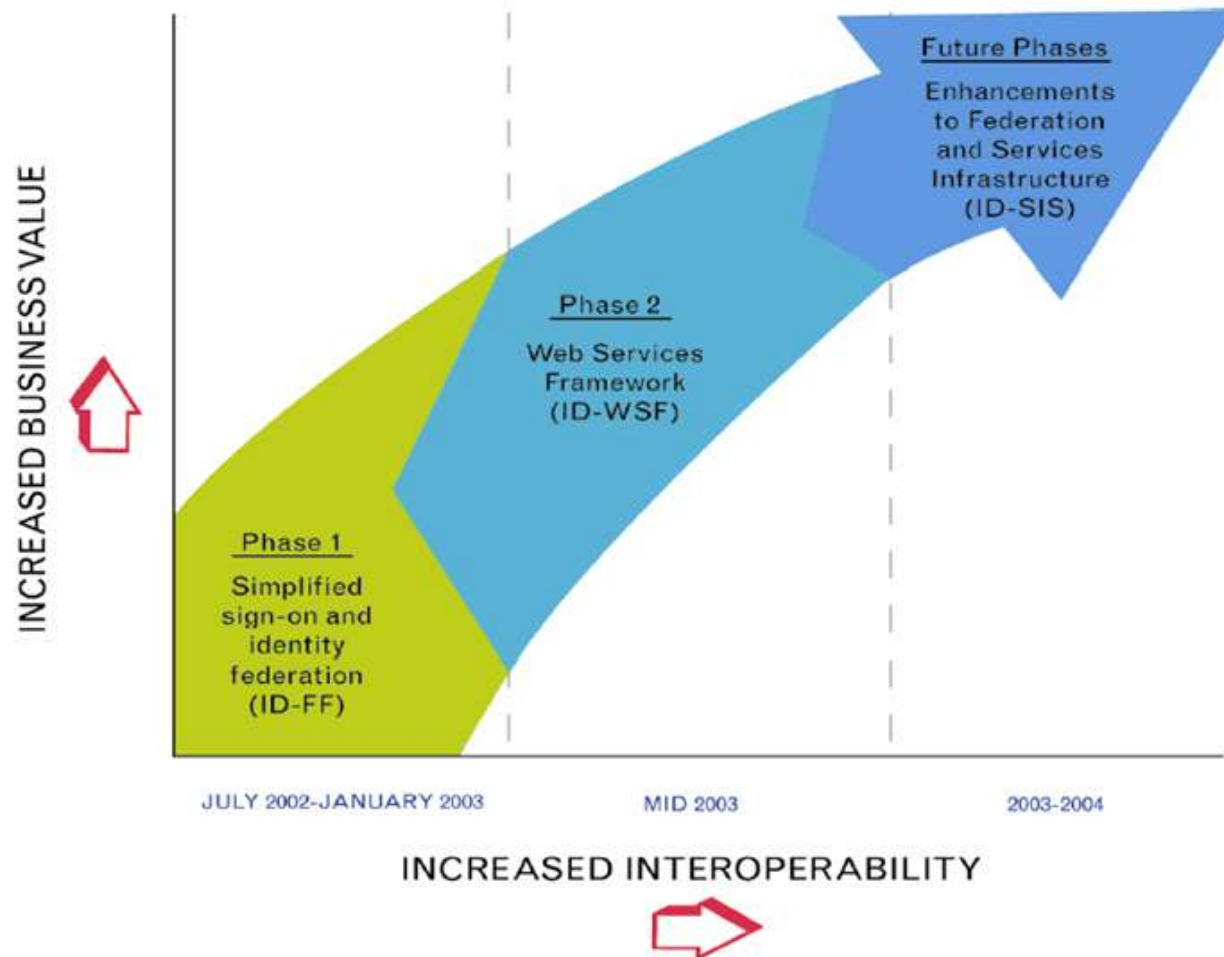
Identity Crisis



The collage consists of several overlapping browser windows:

- Amazon.com**: Shows the top navigation bar with links like 'WELCOME', 'YOUR STORE', 'BOOKS', 'ELECTRONICS', 'TOYS & GAMES', 'CAMERA & PHOTO', 'COMPUTER & VIDEO GAMES & BEAUTY', and 'FREE MORE STORES'. A red circle highlights the 'YOUR ACCOUNT' link.
- AOL Anywhere**: Shows the AOL Members Sign On page with fields for 'Username' and 'Password'. A red circle highlights the 'Sign On' button.
- Bank of America Online Banking**: Shows the 'Online Banking' sign-in page with a red circle around the 'Sign In' button.
- Barclays Online Banking**: Shows the 'Log-in' page with a red circle around the 'Log-in' button.
- Joe's Fish Market.Com**: Shows the 'Tropical, Fresh Water, Shell Fish, Lobster, Frogs, Whales, Seals, Clams' page with a red circle around a form field.
- Hertz**: Shows the 'Welcome to the Hertz #1 Club Gold Reservation area' page with a red circle around the 'Personal Information' section.

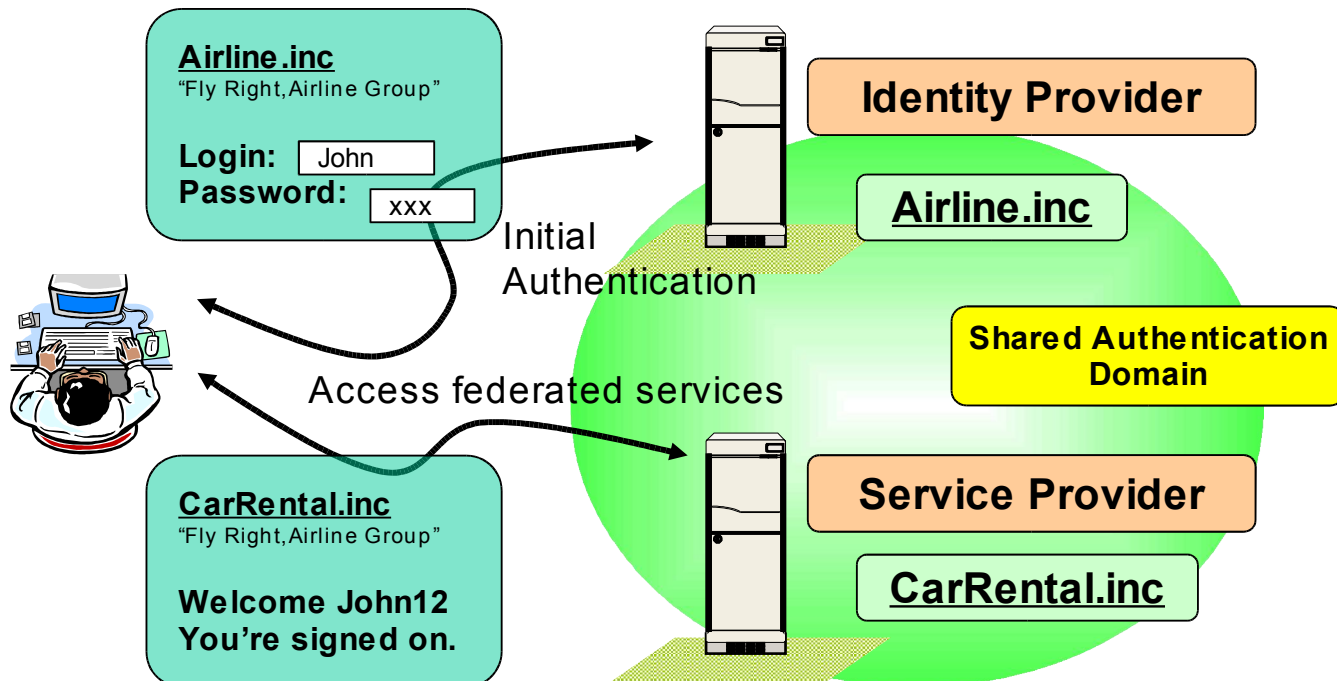
Liberty Alliance Roadmap



Simplified Sign-On

Federated Network Identity

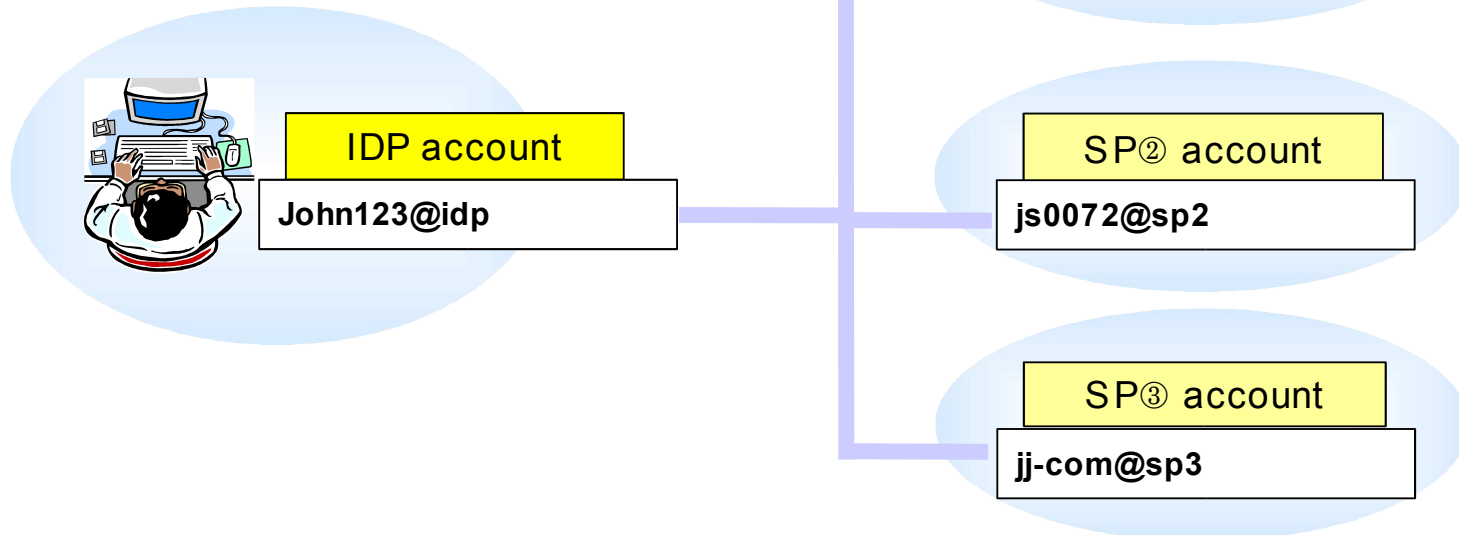
No longer need to provide username and password for each service. Once a user has authenticated she can use the other services directly and securely.



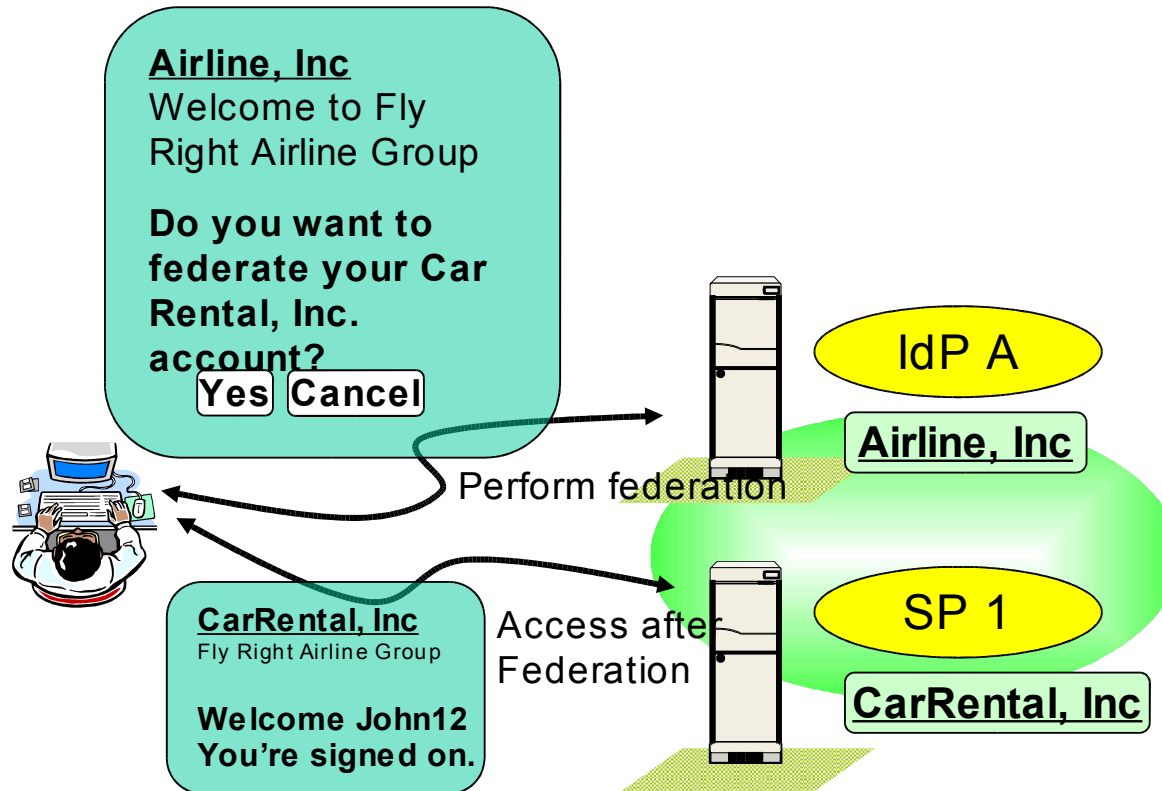
Simplified Sign-On

Federated Network Identity

Even with different usernames and passwords at each service provider the initial authentication provides secure and simplified access to federated services.



Federating an Identity



Key Concepts and Terminology

- Identity
- Simplified Sign-On
- Single Logout
- Network Identity / Federated Identity
- Circle of Trust
 - Principal
 - Identity Provider (IdP)
 - Service Provider (SP)
 - Liberty Enabled Clients or Proxies (LECP)
- Pseudonyms & Anonymity
- Authentication Assertion (SAML)

Key Concepts

Network Identity Concepts

COMPONENT

ATTRIBUTES:



AUTHENTICATION:



AUTHORIZATION:



DEFINITION

Traits, profiles, preferences of an identity, device, or business partner

A level of security guaranteeing the validity of an identity representation

The provisioning of services or activities based upon an authenticated identity

EXAMPLE

- Personal consumer preferences (e.g., travel, entertainment, dining)
- Identity-specific histories (e.g., purchases, medical records, etc.)
- Device capabilities information (e.g., text-only, video, etc.)
- Govt issued (Drivers license, social security, Passport)
- Biometric (Fingerprint, Retinal Scan, DNA)
- Self-selected (PIN number, secret password)
- Services based on attributes (e.g., Travel, entertainment, dining)
- Transaction consummation
- Gradient levels of service (e.g., based on employee level)

Key Concepts

Simplified Sign-On (aka Single Sign-On)

- 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.

Key Concepts

Single Logout

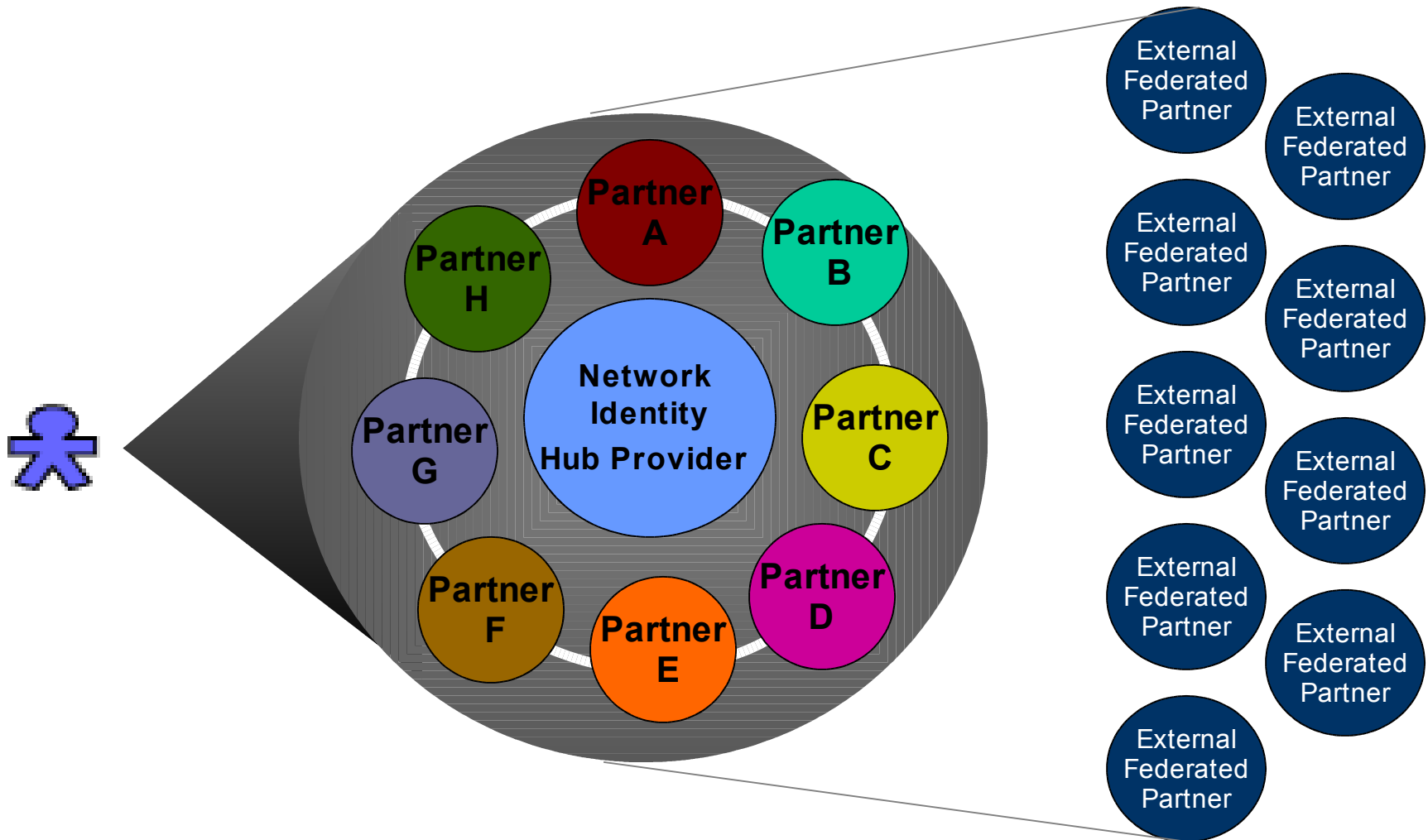
- Single Logout provides synchronized session logout functionality across all sessions that were authenticated by a particular identity provider.

Key Concepts

Federated Network Identity

- Network Identity is the fusion of network security and authentication, user provisioning and customer management, single sign-on technologies, and Web services delivery.
- A federated identity architecture 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.

“Circle of Trust” Concept

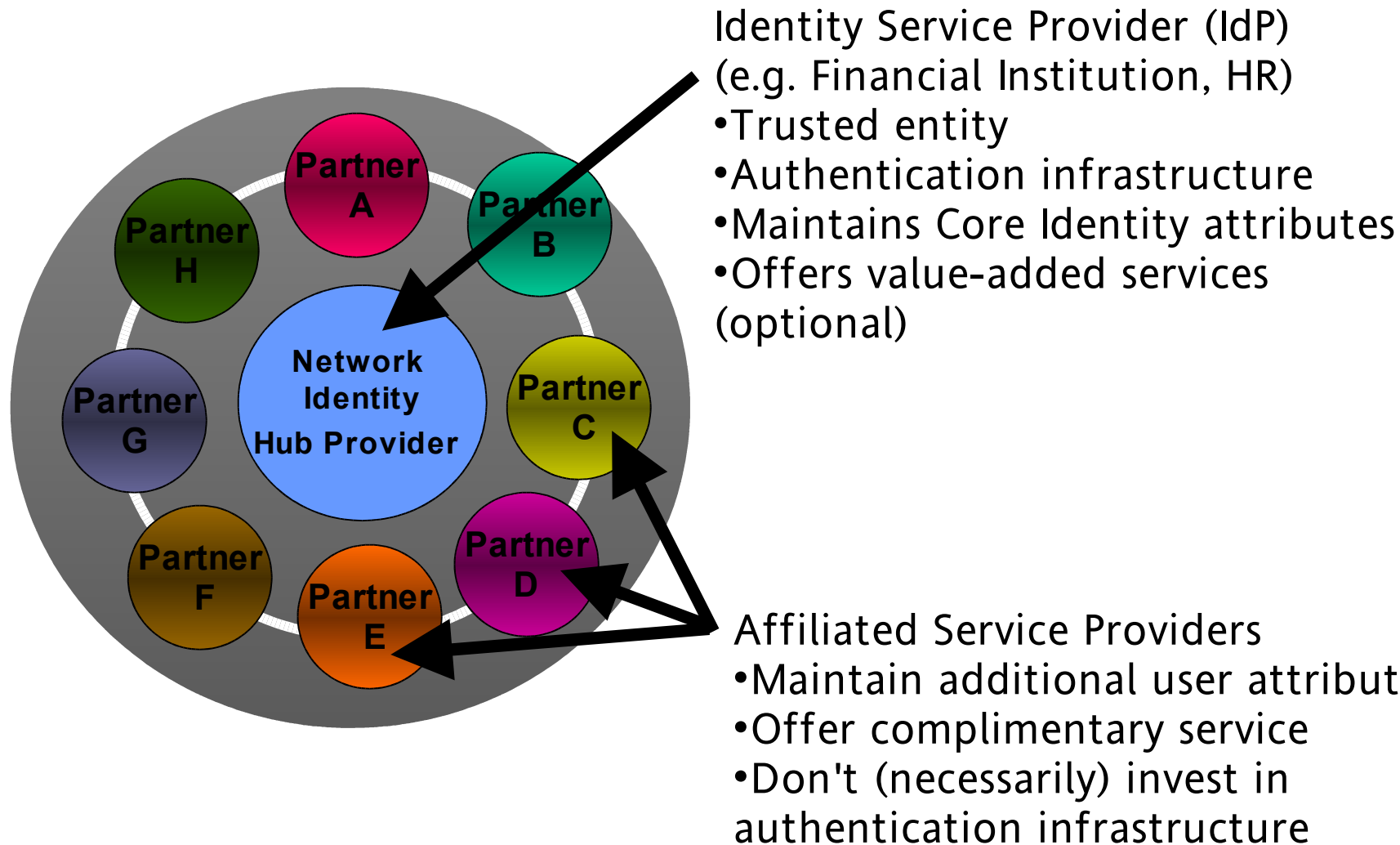


Key Concepts

Circle of Trust

- A circle of trust is 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.

“Circle of Trust” Model



Key Concepts

Circle of Trust Participants

- 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.
- An Identity Provider (IdP) is 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.
- A Service Provider (SP) is an entity that provides services and/or goods to Principals.

Key Concepts

Liberty Enabled Clients or Proxies (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.

Key Concepts

Pseudonyms & Anonymity

- Pseudonyms are arbitrary names 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.
- 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.

Key Concepts

Authentication Assertion (SAML)

- An assertion is a piece of data produced by a SAML authority regarding an act of authentication performed on a Principal, attribute information about the Principal, or authorization permissions applying to the Principal with respect to a specified resource.
- SAML is an XML standard for exchanging authentication and authorization data between security systems.

<http://www.oasis-open.org/committees/security/#documents>

Liberty Alliance Phase 1

- Liberty Alliance 1.0 specification (July 15, 2002)
 - Account linking
 - Identity federation / de-federation
 - Cross domain authentication (CDSSO)
 - Single logout
- Liberty Alliance 1.1 specification (January 15, 2003)
 - Meta-data / Identity and Service Provider descriptors
 - Introducing SAML support (OASIS)
- Relies on SAML specifications
 - SOAP bindings
 - Browser profiles

Liberty Alliance Phase 2

- Enhancements to Phase 1 (ID-FF version 1.2 specification)
 - Affiliations
 - Anonymity
- Introduction to Liberty Identity Web Services Framework (ID-WSF)
 - Permissions-based attribute sharing
 - Identity discovery service
 - Interaction services
 - Security profiles
 - Extends client support
- Introduction to Liberty Identity Service Interface Specifications (ID-SIS)

Liberty Alliance Phase 3

- Scheduled in 2004
- Focused on Identity Services Deployment (ID-SIS)
 - Alerts Services
 - Calendar Services
 - Contacts Service
 - Location Service
 - Presence Service
 - Wallet Service
 - ...

Complete Liberty Architecture

Liberty Identity Federation Framework (ID-FF)

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

Liberty Identity Services Interface Specifications (ID-SIS)

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

Liberty Identity Web Services Framework (ID-WSF)

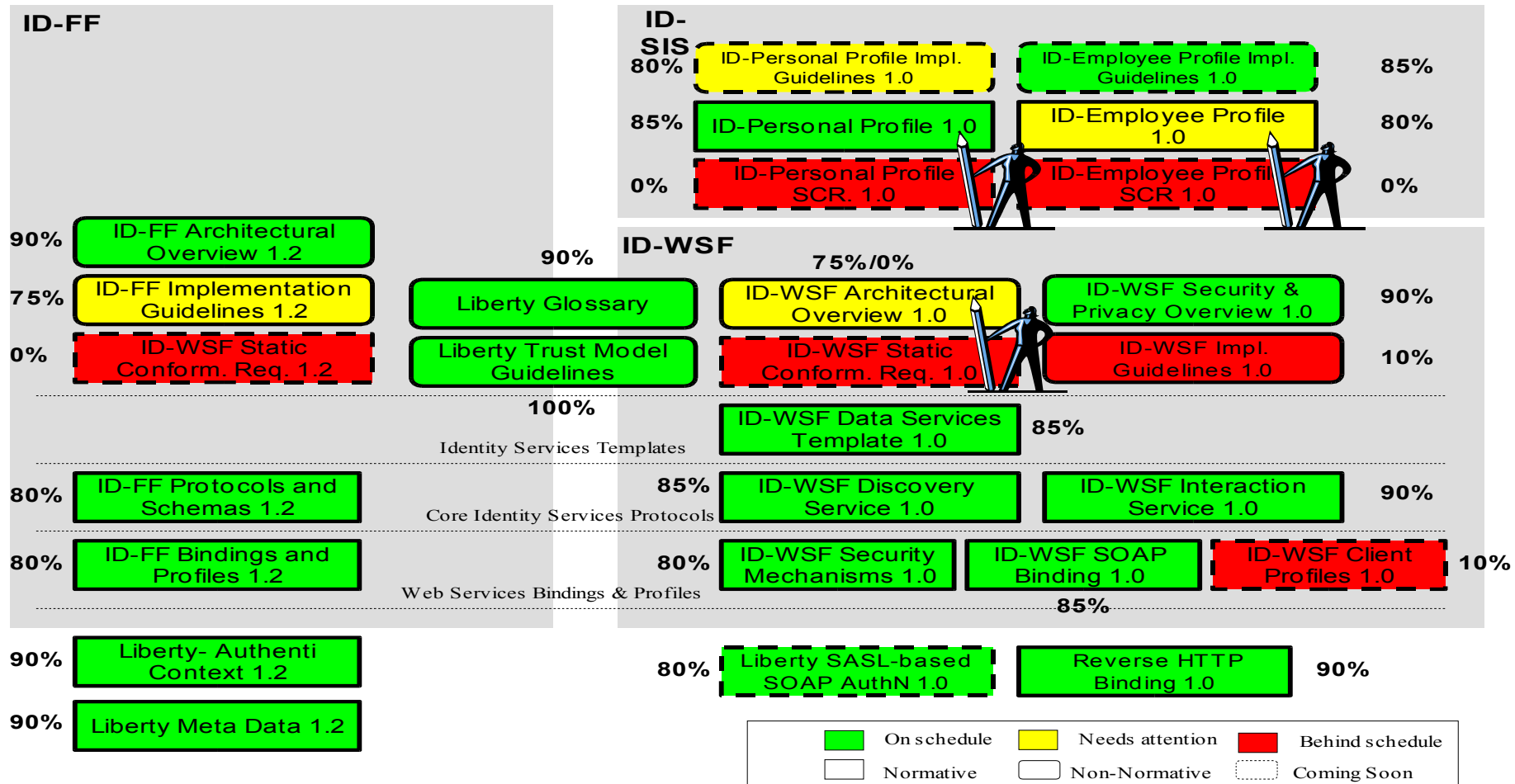
Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards

Phase 2 Final Schedule

| | |
|-----------|--|
| 9/12 | Phase 2 FINAL DRAFTS frozen |
| 9/15-9/19 | TEG vote to release Phase 2 FINAL DRAFTS to All Participants (triggers final IPR review cycle 9/22-11/5) |
| 9/22 | TEG releases Phase 2 FINAL DRAFTS to All Participants |
| 9/22-9/30 | TEG vote to release Phase 2 FINAL DRAFTS to MB |
| 11/6 | Management Board approves Phase 2 FINAL DRAFTS |
| 11/10 | Liberty Alliance Publishes Phase 2 FINAL |

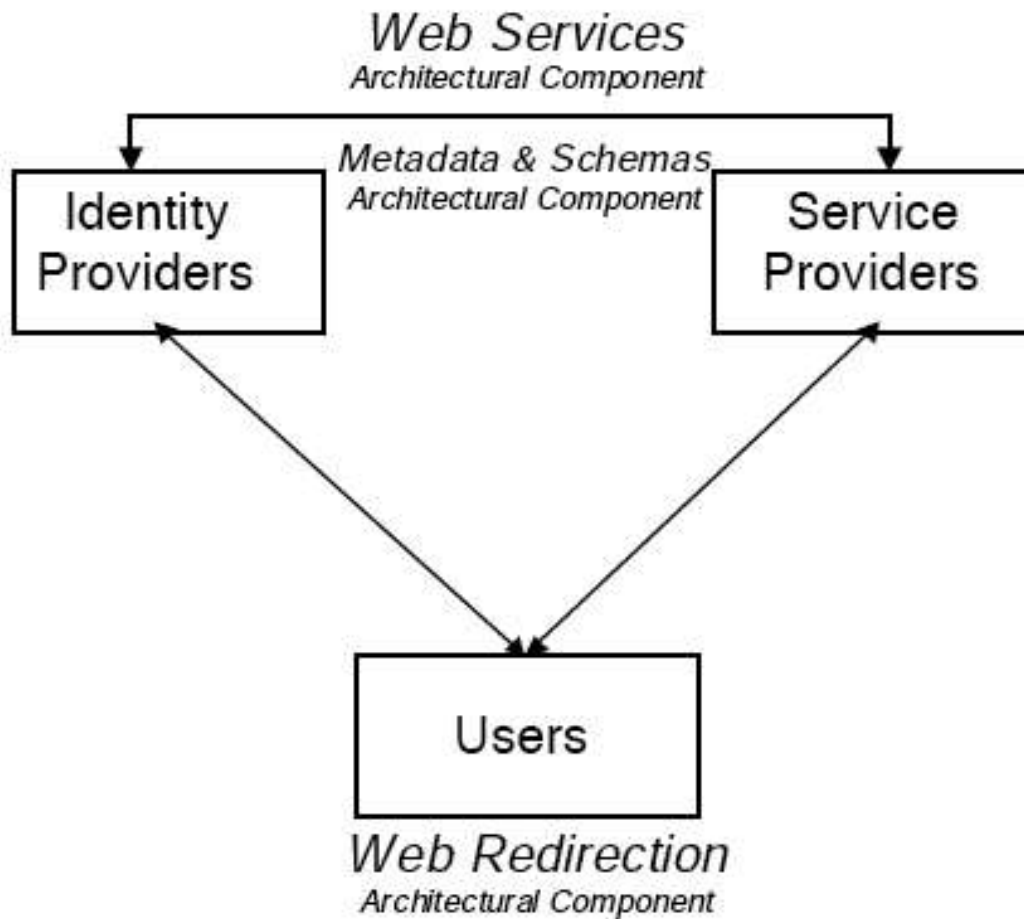
Liberty Specifications (draft for phase 2)



Liberty Alliance vs. SAML

- Liberty defines a standard for federation and SSO
- Liberty uses SAML specifications
 - Bindings
 - Assertions and exchange of assertions
 - SAML profiles
- Liberty defines additional protocols
 - Single logout
 - Provider introduction
 - Federation termination

Basic Architecture



- **Web Redirection**
Enables Liberty-enabled entities to provide services via today's user-agent-installed base.
- **Web Services**
Protocol profiles that enable direct communication between Liberty-enabled entities
- **Metadata and Schemas**
Common set of metadata and formats used by Liberty-enabled sites to communicate various provider-specific and other information

Liberty Platform Requirements

- Trust Relationships
 - Infrastructure entities – Identity Provider (IDP) and Service Provider (SP)
 - Trust Circle (PKI trust root/path)
- Confidentiality and Integrity
 - Secure Back-Channel (TLS, SSL or VPN)
 - XML Signatures
- Peer Authentication and Authorization
 - Server-side Certificates
- Session State Management
 - Common domain cookie

Non-Liberty Platform Requirements

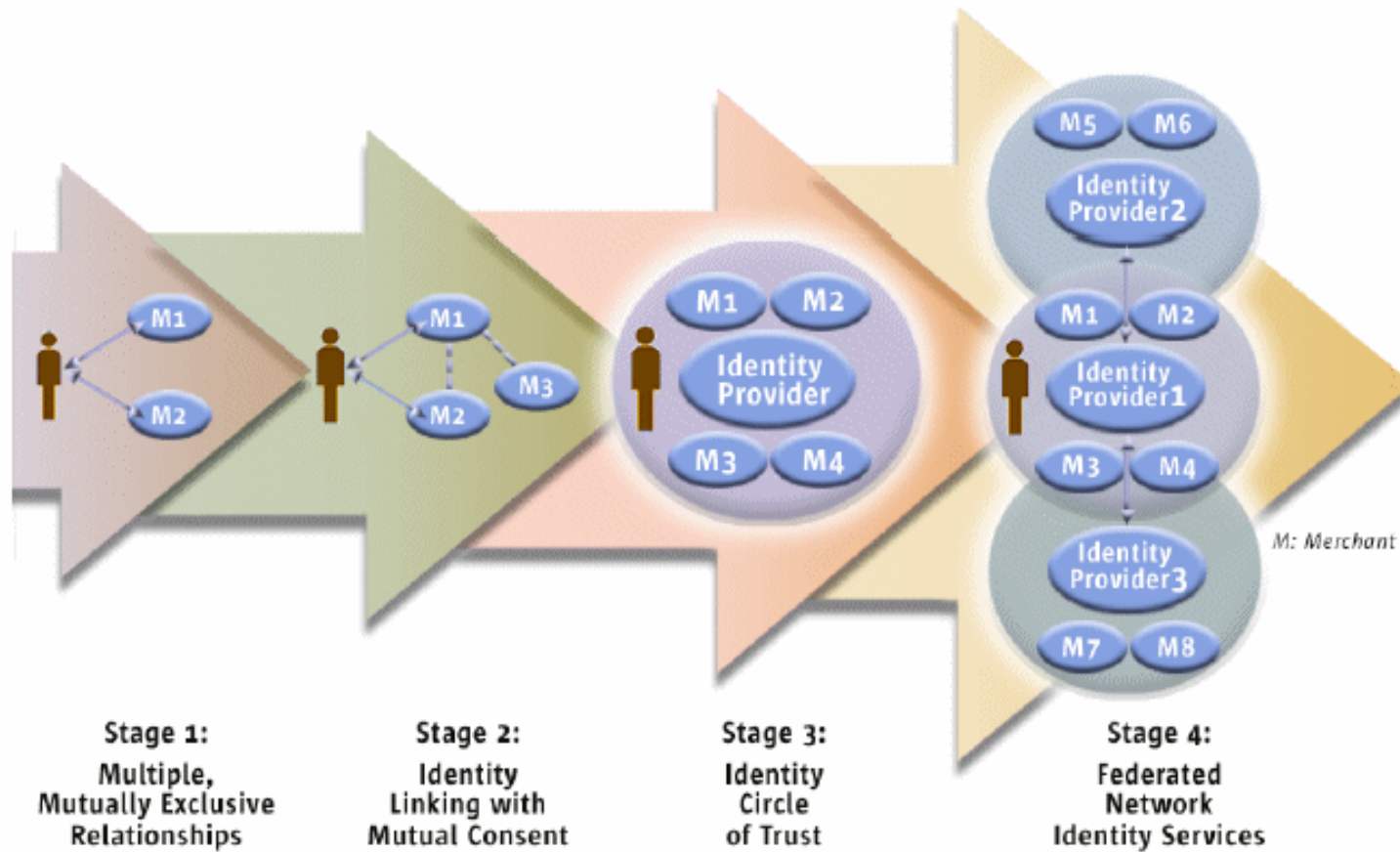
- Identity Management
 - IDPs create, register and manage network identity information in LDAP
- Authentication
 - IDPs have access to authentication service (LDAP, Radius, etc.)
- Meta-directory
 - IDPs and SPs use meta-directories to synchronise identities across federated sites
- Public Key Infrastructure
- Account Provisioning
- Web service interface and metadata exchange
 - Expose Liberty, SAML, SOAP functional interface

Sun ONE IS 6.0 Liberty Implementation

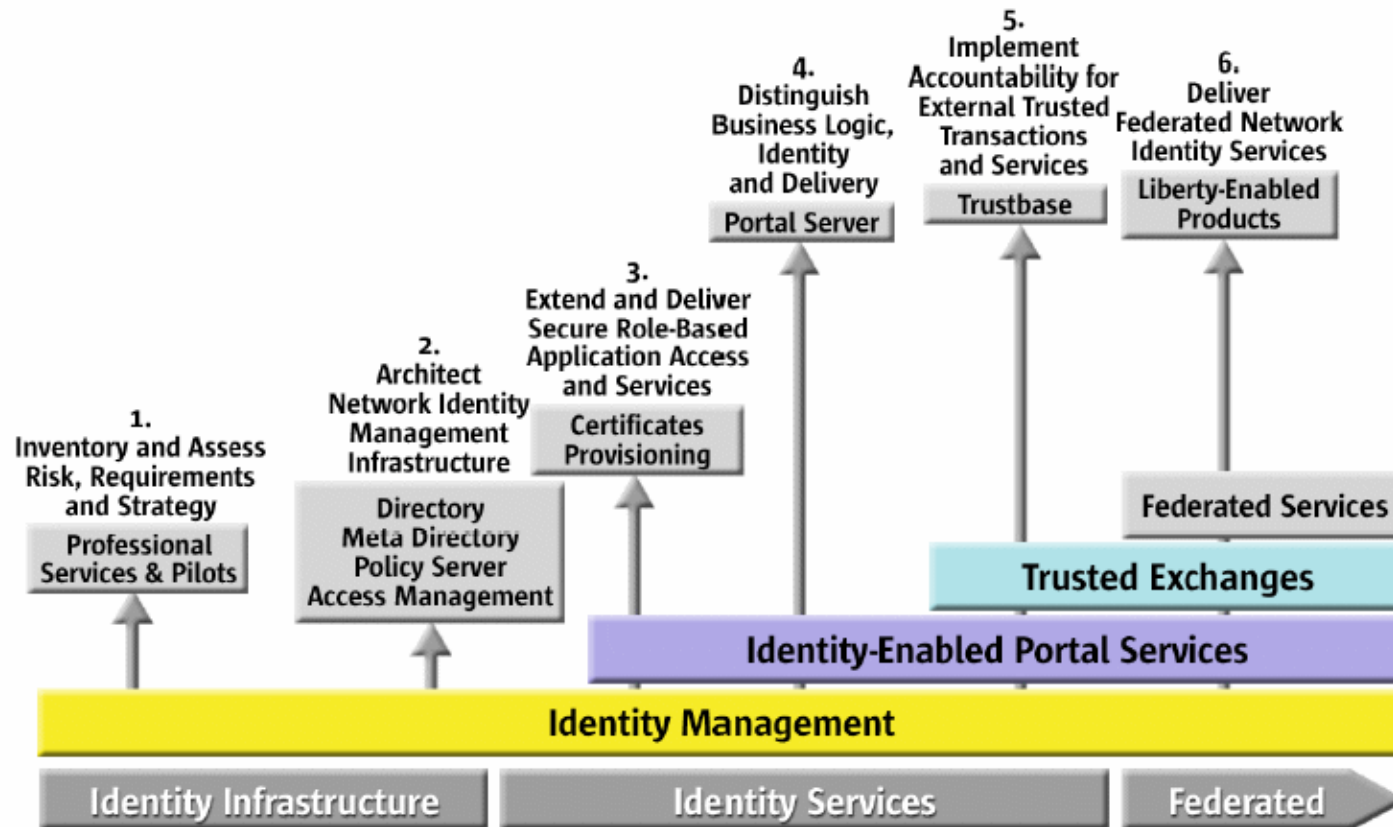
- Liberty Support
 - Liberty Alliance 1.0 Specification => IS 6.0
 - Liberty Alliance 1.1 Specification => IS 6.0 SP1 , IS 6.1 (Orion 1)
 - Liberty Alliance 2.0 Specification => IS 6.2 (Orion Update 1, expected)
- Implements Liberty Alliance 1.0 Protocol Specifications
 - Single Sign-On (Web-SSO)
 - Federation (SAML)
 - Name Registration
 - Federation Termination
 - Single Logout
 - Identity Provider Introduction



Network Identity Evolution



Sun's Network Identity Implementation Approach



Benefits of the Solution

- Increased Security
 - Web SSO ; Certificate Management ; Authentication plug-ins
 - Logging and Auditing ; Identity Federation
- Control over access to resources
 - Centralized policy management ; Multi-level access management
- Lower Administration costs
 - Centralized administration ; Delegated administration
 - End-user self-service
- Reliability Availability Scalability
 - Directory co-existence ; Load Balancing ; Service fail-over
- Flexibility/Open Architecture
 - UI customization for application integration ; Standards support

Sun Professional Services Designs and Delivers Network Identity

- Architecture Workshop Service
- Architecture Roadmap Service
- Quick Start Service for Network Identity
- Security Services
- Identity Management Services
- Sun ONE Implementation Services
- Java Center Services

<http://www.sun.com/service/sunps/architect/ni.html>

Spec Summary ID-FF

- Liberty ID-FF Architecture Overview is a non-normative summary description of the Liberty ID-FF architecture, including policy and security guidance.
- Liberty ID-FF Implementation Guidelines defines the recommended implementation guidelines and checklists for the Liberty architecture focused on deployments for the service-providing entities: service providers, identity providers, and Liberty-enabled clients or proxies (LECPs).
- Liberty ID-FF Protocols & Schema defines the abstract protocols and XML schemas for Liberty.
- Liberty ID-FF Bindings & Profiles defines concrete transport bindings and usage profiles for the abstract Liberty protocols.
- Liberty Authentication Context defines the authentication context schema, which is used to communicate information about an authentication event.
- Liberty Metadata describes metadata, protocols for obtaining metadata, and resolution methods for discovering the location of metadata.

Spec Summary ID-WSF

- Liberty ID-WSF Primer is a non-normative document intended to provide an overview of the features of the Liberty ID-WSF Version 1.0 Specifications.
- Liberty ID-WSF Security & Privacy Guidelines is a non-normative document providing an overview of the security and privacy issues in ID-WSF technology and briefly explaining potential security and privacy ramifications of the technology used in ID-WSF.
- Liberty ID-WSF Static Conformance Requirements
- Liberty ID-WSF Data Services Template provides protocols for the querying and modifying of data attributes when implementing a data service using the Liberty Identity Web Services Framework (ID-WSF).
- Liberty ID-WSF Discovery Service describes protocols and schema for the description and discovery of ID-WSF identity services.
- Liberty ID-WSF Interaction Service specifies an identity service that allows providers to pose simple questions to a Principal.
- Liberty ID-WSF Security Profiles specifies security mechanisms that protect identity services.
- Liberty ID-WSF SOAP Binding defines the Liberty Identity Web Services Framework (ID-WSF) SOAP binding. It specifies simple SOAP message correlation, consent claims, and usage directives.
- Liberty Reverse HTTP Binding for SOAP specifies a binding that enables HTTP clients to expose services using the SOAP protocol, where a SOAP request is bound to an HTTP response, and a SOAP response is bound to an HTTP request.



Fulup@Sun.com

