Network Identity and the Liberty Alliance Project

Andrew Shikiar
Group Manager, Sun ONE Business Alliances
Sun Microsystems, Inc.
Overview of Network Identity

- Needs and benefits of a federated network identity standard
- Conceptual Demo

Liberty Alliance Project

- Goals & Principles
- Status / update
The set of attributes that describe profile(s) of an individual.

- Customer Name: John Smith
- Email alias: jsmith2@freemail.com
- PIN: js@eng.sun.com
- Credit card number
- Social security number
- Drivers license
- Passport
- Retinal Scan
- DNA
- Entertainment preferences
- Notification preferences
- Employee Authorization
- Business Calendar
- Dinning preferences
- Affinity program
- Friends and associates
- Education History
- Medical History
- Financial Assets...
Without identity, you can’t have an enduring relationship with your customers.

Knowing your customers better than your competitors is a huge advantage.
• Scattered data and personal information
• Consumers can't easily update and/or view identity profiles.
• Incompatible identity “standards”
• Isolated applications, Web sites, and Services make it cost prohibitive for technologies to work together
• There currently is limited development of empowering, productive, and exciting real-world products and services.
An open standard for identity, authentication and authorization will lower costs, accelerate commercial opportunities, and increase customer satisfaction.

A federated standard that will enable every business to:

- Maintain their own customer/employee/device data
- Tie data to an individual’s identity
- Share data with partners according to its business objectives, and the customer’s preferences
What Are the Possible Solutions?

- Single Identity Operator
- Operator
- Financial Svcs
- Customer
- Community
- Online Community
- Telecommunication Community
- Entertainment Community
- Travel Community
- Wireless Community
- Retail Community

Centralized Model

Open Federated Model
1. Distributed data stays with “rightful” owner

2. Multiple authenticators
   ➥ Competition for consumer trust

3. Delineation between authentication and authorization
   ➥ Merchant retains control of transaction requirements
   ➥ Gradient levels of authentication within network

4. Consumer is in control of who can access information
   ➥ Multiple modes: Always, Within group, per transaction, …
Comfort & Ease of Use
- Single ID and Password for all applications
- Seamless interaction of multiple devices
- Ubiquitous updates of personal information

Control of personal information
- Definition of what data is shared
- Definition of recipients of data

Protection of their identity
- Policies and standards around data usage and sharing
- Security and Safety

Enhanced abilities and functionality
- Defines the core infrastructure to allow integrated services
Reduced authentication system support costs

- Ability to leverage external identity mgmt systems and services
- Reduction in need for internal single sign-on application
- Reduced internal and external system integration costs

**Increased Revenue**

- Introduce new direct and indirect services

**Reduced fraud for on-line transactions**

- Support of framework for identifying users during a financial transaction

**Increased customer satisfaction**

- Framework for providing integrated functionality and features
- Support of single ID and Password at all sites

**Identification of new business partnership opportunities**

- Enablement of integrated services across partners
**Core Profile**
- Name
- Email
- PW

**Extended**
- Address
- Birth date

**Bank:**

**Merchant #1:**
Global Studios Inc. Movie Premiere

**ISP**
Calendar
- Access to friend’s calendar

**Financial Institution**
Credit card

**Supplemental Profile**
- Background
- Preferences (Entertainment)
- History
- Access
- Privacy
- Policy
- Authorization
- Other...

**Agent:** Recommend movie, determine optimal date, time and location to see movie with a friend, charge to credit card, reward affinity program account.
One Network Identity, Multiple Profiles

**Primary Trust Authority**
- (my company)
- Accts Payable App
- Calendar
- Supply Chain Aggregator
- Supply

**Secondary Trust Authority**
- (e.g., my airline)
- NI Enabled Merchants
- NI Service Aggregator
- NI Enabled Services
- Friends & Family Notification
- External Services
- News Source
- External Services

**Employee Circle of Trust**

**Consumer Circle of Trust**
B2C NI for Trusted Consumer Relationships

- Customer Relationships build on trust

B2E NI for Employees Productivity

- Employee productivity and effectiveness based on trusted security

B2B NI for Business Services

- Trusted Commerce with support for asynchronous transactions, non-repudiation, contract, signature...
In the B2B realm, Identity underpins not just “sessional” concepts but some key “transactional” concepts:

- Contract
- Signature
- Asynchronous communications
- Recourse
- Non repudiation
- Document origination
- Payment

B2B business demands simplicity - a single concept of identity should be capable of underpinning sessional and transactional concepts.
Real Trade Demands a Community Network Identities to Interact

Buyer

Seller

Consulate

Import Agent

Financial Institution

Financial Institution

Financial Institution

Financial Institution

Intermediary Financial Institution

Financing Financial Institution

Buyer

Seller

Insurance Company Broker

Buyer

Dispute Resolution Services

Shipper

Exporter

Inspection Agency

Lawyer
A multi-industry business alliance that is defining and driving a widely accepted, interoperable standard for:

- **Network Identity** - on anything attached to the Internet
- **Network authentication** - from simply identifying to secure transactions
- **Network authorization** - on any service platform

Providing a standard which will:

- Simplify business partnerships on the internet.
- Increase a user's consumption of network services.
- Allow businesses and consumers to better manage their data.
>1.5 Billion Network Identities

And growing…
1. **Interoperability** is the focus

2. Respects that other private and public identity systems will exist

3. Sun is one of many founders with **no** unique privileges

4. Technology neutral, needs to support many different devices and systems

5. Nimble governance model

6. **Commercial deployment** is measure of success
How Is Liberty Organized?

- Determines market requirements and use case focus for alliance.
- Drives positioning, promotion, branding, adoption and deployment.

Governance

- Defines mission/scope
- Drives execution timetable

Marketing

- Determines market requirements and use case focus for alliance.
- Drives positioning, promotion, branding, adoption and deployment.

Technology

- Understands current standards, drives convergence, evolution of technology
- **Delivers a spec.**

Policy

- Understands policy/regulatory environment
- Eventually describes and audits compliance
Network Identity Value Chain

Creation
- APIs
- Schema
- SW Platform
- Device Specific
- Security
- Best Practices
- Tools

Promotion
- Hosting
- Portal
- Ingredient Branding
- Adoption
- Cross-promotion
- Alliance “Circle-of-Trust”

Content & Delivery
- Entertainment
- Financial Services
- Wireless Services
- Business Services
- Retail Services
- Maintenance/Replenishment services
- Foundation Network Identity Services (e.g. Alerts, location)
- Supply Chain Services
- Aggregation
- Communication
- Notification…

Service Management
- Authentication
- Preferences
- Profile
- History
- Access
- Rewards

Business Factors
- Authorization
- Billing
- Usage
- Discounts
- Payments
- Affinity Program
- Standardized single sign on within an enterprise
- The ability to receive pre-authenticated users from business partner’s sites.
- The ability to retain users within a site, providing authenticated services from business partners
- Being able to navigate the web with customers -- wherever they may go -- to deliver services on demand.
- Interoperability with major identity systems
- Commercial adoption and deployment
Alliance Formation Timeline

Founders Sign Bylaws
Membership Bylaws Completed
2nd Founders Meeting

3rd Founders Meetings

Membership Contract Application Distributed

4th Liberty Membership Meeting

Associate Membership Opens

Liberty Final Spec Q2
Liberty Deployment Q3

November December January
Proposed Liberty Phases

I. Single Sign On for eWallet Applications
   - Context sensitive Cookies
   - Multi-authenticator system

II. Federated Data Exchange
   - Extensible schema with mappings
   - PKI or strong crypto between providers and merchants
   - Endpoints migrate to web services

III. B2B Transactional Support
   - Asynchronous communication
   - Non repudiation, signature binding…

IV. Web services as endpoints
   - Evaluation of mixes, crowds for anonymity
   - Distributed redundant data for identity theft protection