
Driving Federated Identity to promote Web Services Security Liberty – SAML Update

Jim Cowing
Digital Resources Group
www.drgsf.com
Global Concepts Meeting – St. Louis
June 25, 2003

Agenda

- Background & History – Network Identity
- Identity for Financial Institutions
- SAML
- Liberty Alliance
- FSTC Specifications Review
- Emerging Issues and Conclusion

My Disclaimer

- Views expressed in this presentation do not represent the Liberty Alliance, OASIS, or any other standards bodies or organization.
- Digital Resources Group (DRG) is a consulting firm that works with financial services industry to understand and define and promote Strategic Technology initiatives.
- DRG is a member of FSTC and Jim Cowing is co-chair of the FSTC Security SCOM. DRG currently participates in a Liberty/SAML analysis project to assess how evolving Network Identity specifications may impact the Financial Services industry.

What is Network Identity?

A Network Identity is
a user's overall global set of attributes
 constituting their various accounts

- When users interact with services on the Internet they often tailor them in some way for their personal use

- Users establish accounts with user names and passwords, and/or set some preferences for what information they want displayed and how they want it displayed

- Today, users' accounts and personal information are scattered across isolated Internet sites



Federation vs. Centralization

Centralized Model

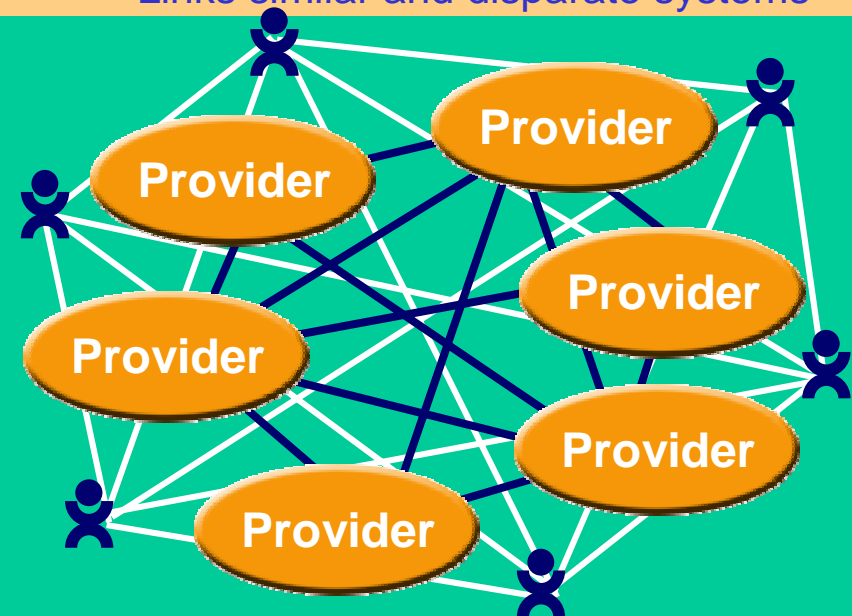
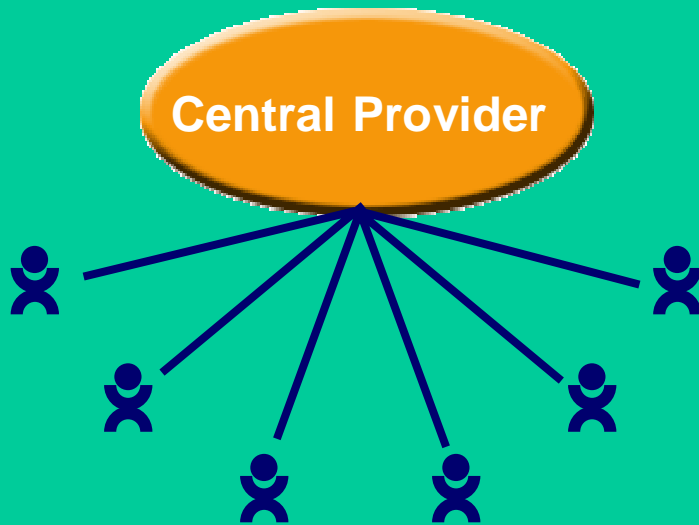
(Microsoft Passport)

- Network identity and user information in single repository
- Centralized, proprietary control
- Single point of failure
- Links similar systems

Open Federated Model

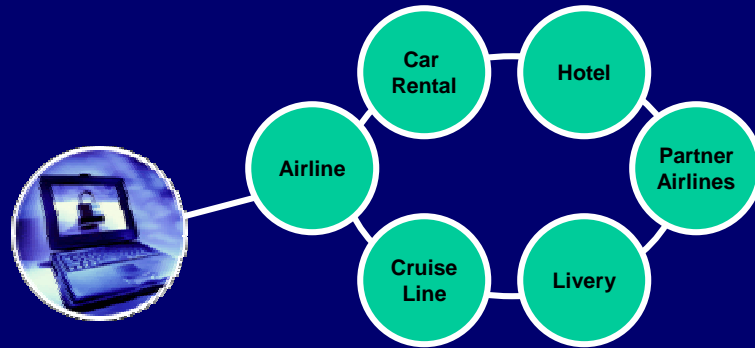
(Liberty Model)

- Network identity and user information in various locations
- Open architecture
- No centralized control
- No single point of failure
- Links similar and disparate systems

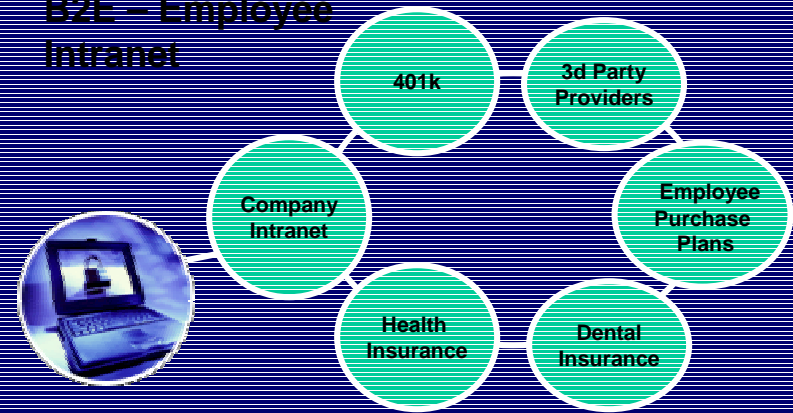


Trust Domains Exist Today

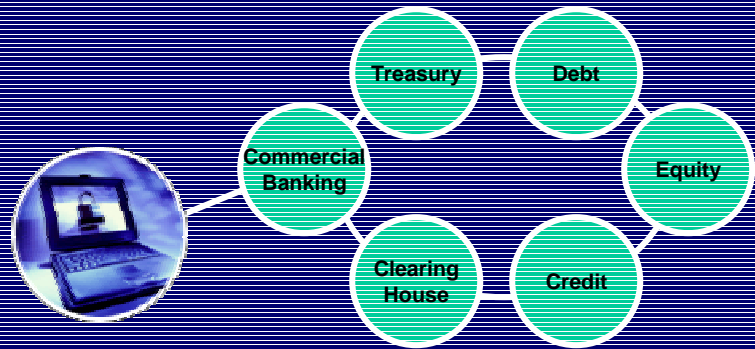
B2C – Travel Industry



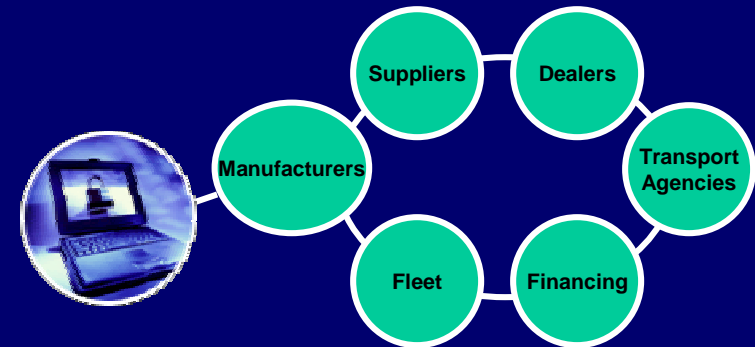
B2E – Employee Intranet



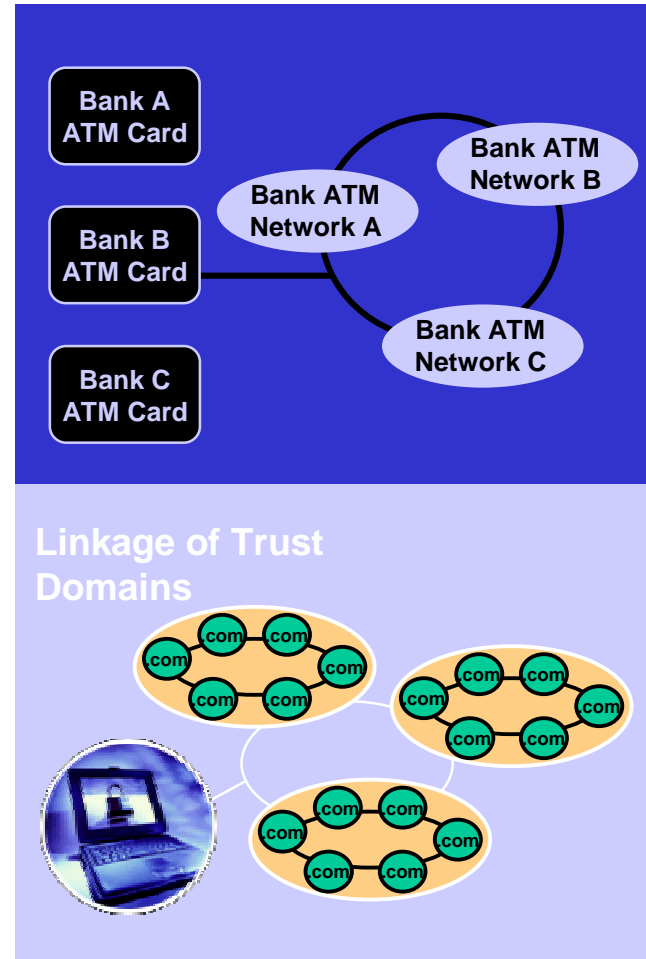
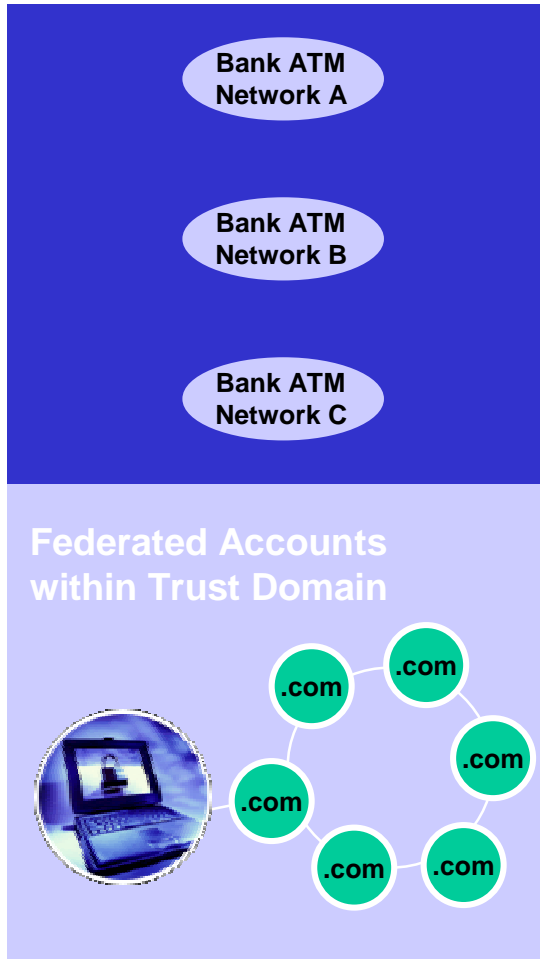
B2B – Financial Services



B2B - Automotive



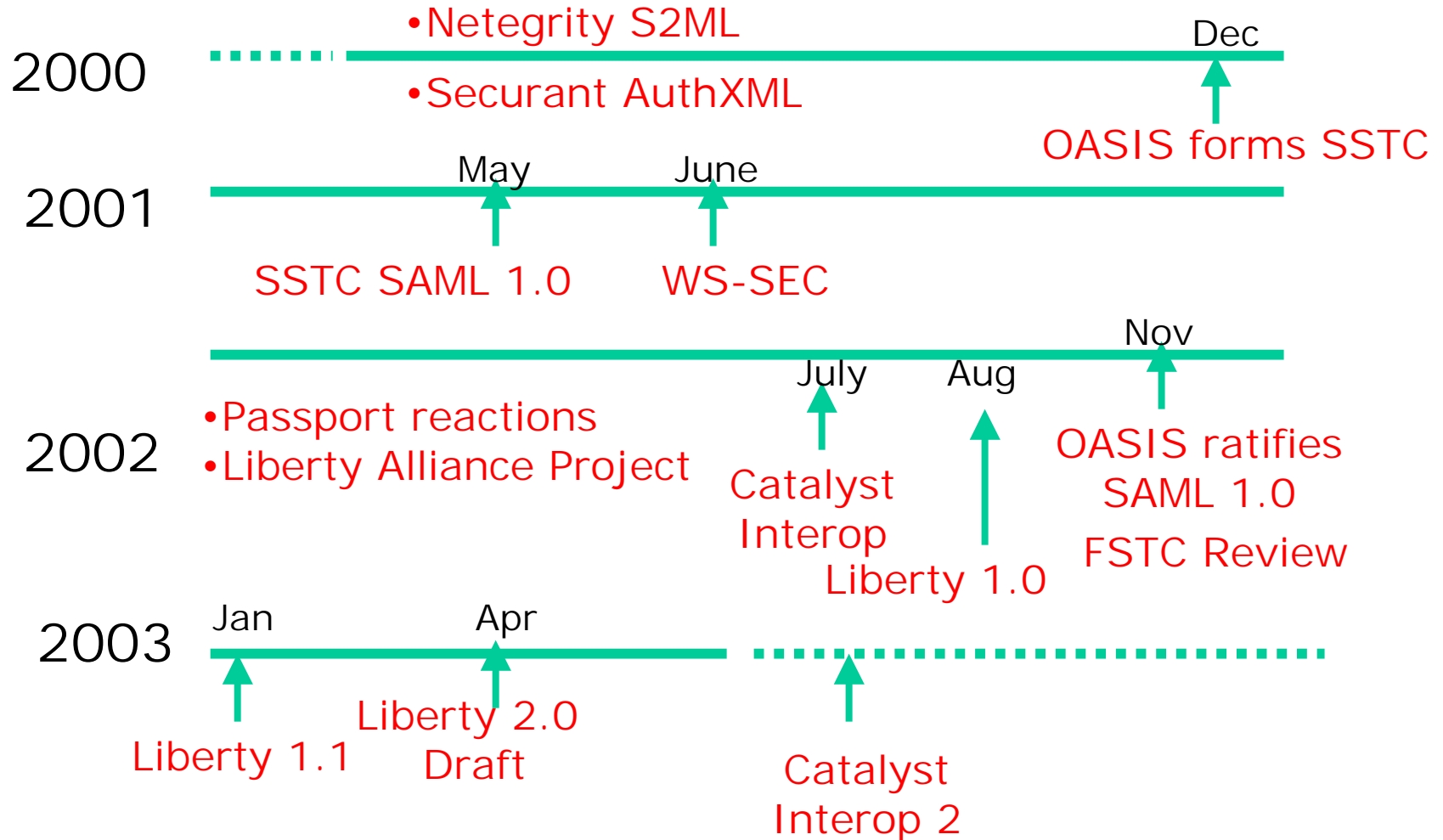
Linking Federated Trust Domains



Importance of Identity for FIs

- Enrollment – Know Your Customer
- Fraud – Identity Theft
- Privacy - GLB
- Multi-channel delivery – “Know Me Everywhere”
- Security – We are Under Attack
- Outsourcing – Partners and Third Parties
- Bank Alliances & Consortia
 - Identrus, Spectrum
- Regulatory Requirements
 - OCC 2001-8, Patriot Act, Homeland Security Act

Identity Standards Timeline



SAML

SAML

- Security Assertion Markup Language.
- XML framework or vocabulary to convey trustworthy, digitally signed authentication and user information tokens between applications or domains, independently from actual authentication mechanisms, user directories, or security policies.

What is SAML used for?

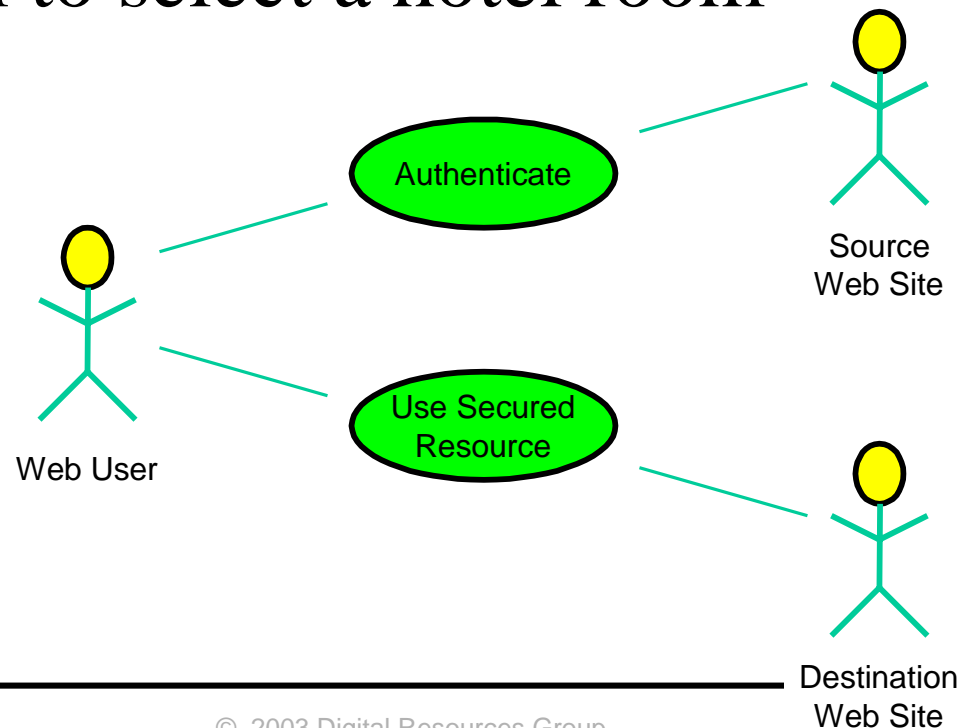
- Distributed Authorization
- Federated Identity Management
- Multi-vendor Portals
- Web Services Access Control

SAML Use Cases

- SAML developed three “use cases” to drive its requirements and design:
 1. Single sign-on (SSO)
 2. Distributed transaction
 3. Authorization service
- Each use case has one or more “scenarios” that provide a more detailed roadmap of interaction

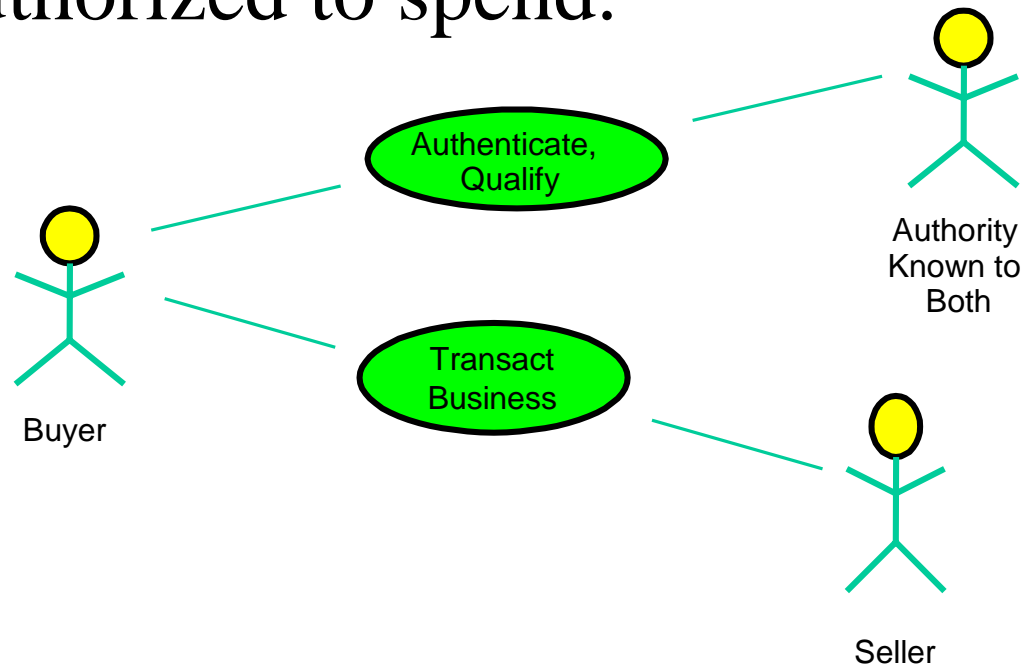
#1: Single sign-on (SSO)

- Logged-in users of Hilton.com website are allowed access to a sister site, Hampton Inn.com to select a hotel room



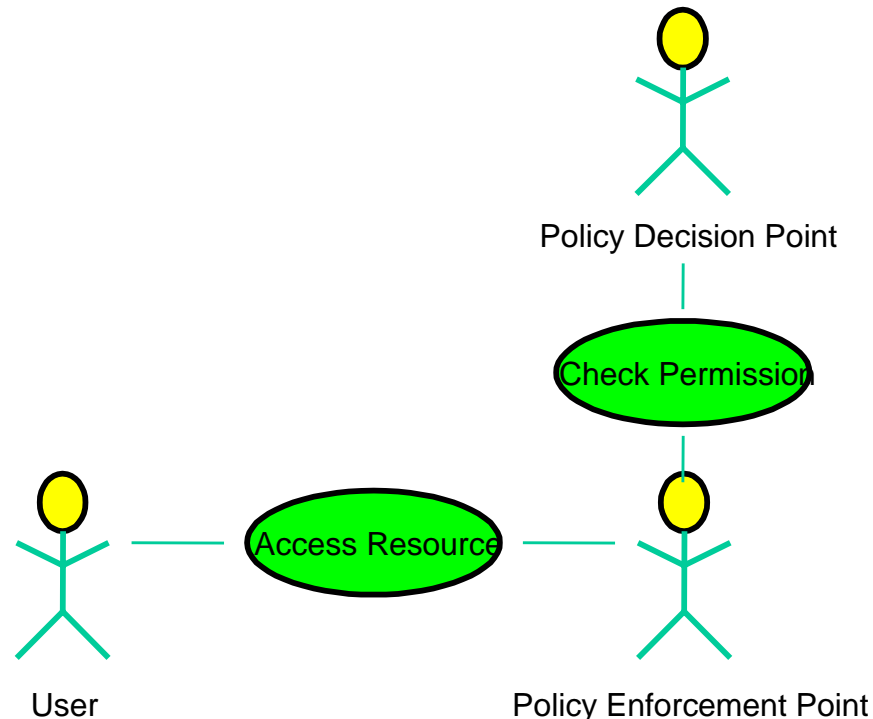
#2: Distributed transaction

- Employees are allowed to order office supplies from suppliers if they are authorized to spend.



#3: Authorization service

- Employees at YourCo order office supplies directly from OfficeSupplies, which performs its own authorization



SAML assertions

- Assertions are declarations of fact, according to someone
- SAML assertions are compounds of one or more of three kinds of “statement” about “subject” (human or system):
 - Authentication
 - Attribute
 - Authorization decision
- SAML may be extended to make new kinds of assertions and statements
- Assertions can also be digitally signed (PKI)

SAML - Future

- SAML was intended to provide heterogeneous Single Sign-On for two portal models.
 - Browser profile gaining strong industry support and acceptance.
 - Supporting companies include RSA Security, Netegrity, Oblix, Novell Networks, Sun Microsystems, and IBM's Tivoli (all of which are members of the Liberty Alliance).
- SOAP profile pulled, in process by WS-Security.
- SAML does not solve overall identity problem.
- Microsoft says it will deliver SAML support with its Server 2003 operating system
- OASIS voted to accept Liberty v1.1 contribution in preparation for its next update -SAML version 2.0.

Liberty Alliance

Liberty Alliance - Mission



Establish an open standard for federated network identity through open technical specifications that will:

- Support a broad range of identity-based products and services
- Allow for consumer choice of identity provider(s), the ability to link accounts through account federation, and the convenience of single sign-on, when using any network of connected services and devices
- Enable commercial and non-commercial organizations to realize new revenue and cost saving opportunities that economically leverage their relationships with customers, business partners, and employees
- Improve ease of use for e-commerce consumers

•Source: Liberty Alliance

Liberty Refresher

Membership Update

- 150 + members (with 1Billion plus customers worldwide)
- Members represent a wide range of industries, including:
 - Transportation
 - Financial services
 - Mobile phone and wireless service providers
 - Internet service providers
 - Hardware and software suppliers
 - Security and web services companies
- Privacy Focus - Key Goal of Alliance – User Controls Identity
- Interoperability - Additional Key Goal of Alliance
 - Business –
 - Define business needs for network identity; Develop business frameworks, guidelines and best practices.
 - Technical -
 - Open technical specifications
 - Drive interoperability and convergence of
 - Demonstrate and prove interoperability



Key Objectives

- **Simplified Sign-On:** Provide an open simplified sign-on specification that includes federated authentication from multiple providers operating independently, simplified access across multiple accounts within a trust community, and portable on-line identity
- **Enhance Constituent Relationships:** Enable commercial and non-commercial organizations to control, maintain and enhance relationships with constituents
- **Support All Devices:** Create a network identity infrastructure that supports all current and emerging network access devices
- **Enable Consumer Privacy:** Enable commercial and non-commercial organizations to protect consumer privacy
- **Support Interoperability:** Provide a mechanism supporting interoperability with existing systems, standards, and protocols

Source: Liberty Alliance

New Membership Tiers Added

Sponsors

- Full participation and voting in any or all Expert Groups
- Can run to fill Management Board vacancies
- Representatives can be officers in Expert Groups

Membership Fee: based upon size of firm
120,000/year maximum

Associates

- Can view and comment on draft specifications prior to public release
- Access to alliance member web site
- Can attend semi-annual “All Participants” meetings

Membership Fee:
\$1,000/year maximum

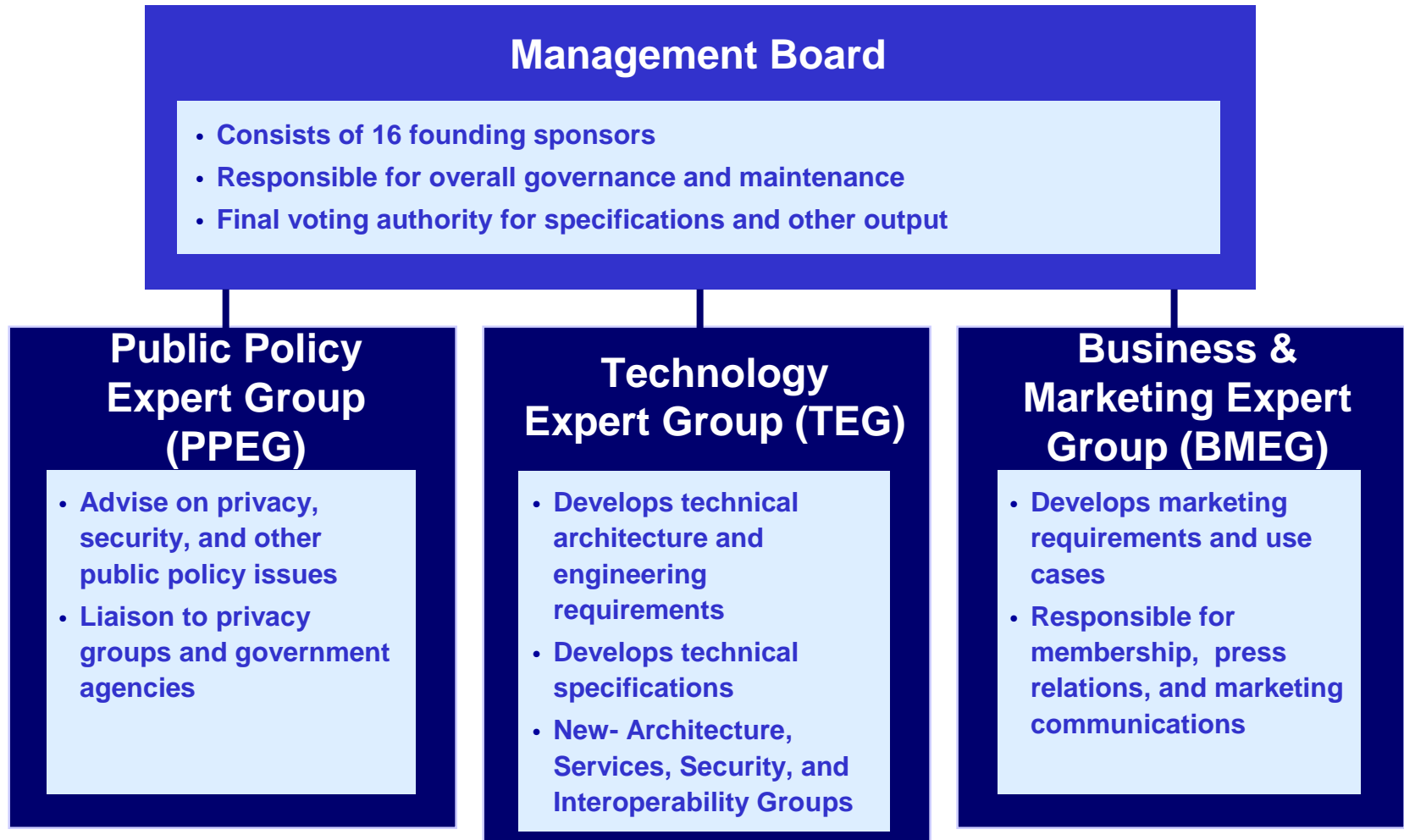
Affiliates

- For government agencies, educational institutions, and non-profit organizations only
- Have same privileges as Associate members

Membership Fee:
None

•Source: Liberty Alliance

Current Liberty Structure



Version 1.0 Specifications - Functionality

- Opt-in account linking – **Users can link their accounts with different service providers within “circles of trust”**
- Simplified sign-on for linked accounts – **Once users’ accounts are federated, they log-in, authenticate at one linked account and navigate to another linked account, without having to log-in again**
- Authentication context – **Companies linking accounts communicate the type of authentication that should be used when the user logs-in**
- Global log-out – **Once users log-out of the site where they initially logged in, the users can be automatically logged-out of all of the other sites to which they were linked**
- Liberty Alliance client feature – **Implemented on client solutions in fixed and wireless devices to facilitate use of Liberty version 1.0 specification**

Source: Liberty Alliance

Liberty Evolution - Phase 1 vs. Phase 2

- Liberty Phase 1

Liberty Version 1.1

- Account linkage, simplified sign on, simple session mgt, etc.

Enables



- Liberty Phase 2

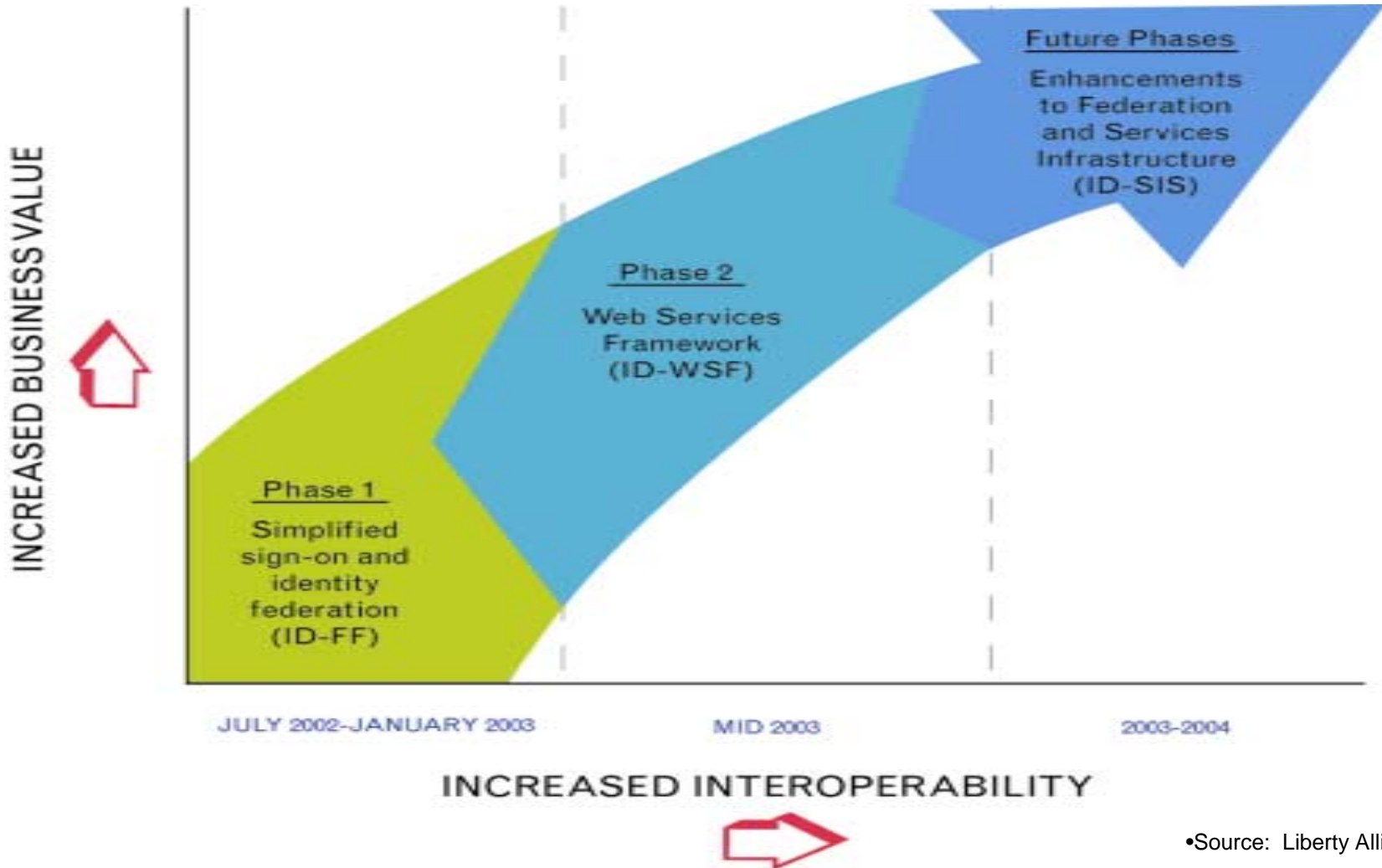
Liberty Version 2.0

- Permission based attribute sharing, service discovery and invocation, data oriented service abstraction, etc.

Enables



Phases to Interoperable Federated Identity



•Source: Liberty Alliance

Recent Architectural Roadmap

Apr 2003 - Liberty publicly announces next generation architectural roadmap with new terminology to define next generation of open standards-based independent modules for their Identity 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)

The schema, and instantiation of the technical implementation as defined by ID-WSF, to provide for 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)

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



•Source: Liberty Alliance

Phase 2 Direction

Caveats on Next Phase

- Liberty version (phase) 2.0 is *not an incremental build* on top of Liberty version 1.1, but more of an orthogonal set of specifications.
- Liberty anticipates certain companies will only want to implement Liberty version 1.1 and not 2.0.(and potentially vice-versa).
 - Note: This could lead to a false perception by their customers that they are not implementing the latest Liberty version or the complete specification

RSA Public Interoperability Event

- April 2003 - First public Liberty IOP event
- 20 companies demonstrate Liberty interoperability
- Four different scenarios demonstrated
 - Business to Business (B2B)
 - Business to Employee (B2E)
 - Business to Consumer Mobile (B2C)
 - Business to Consumer Broadband (B2C)
- Strong commitment for Phase 2 deployment

Financial Industry Impact FSTC Study



FSTC Introduction

- Consortium of leading North American based financial institutions (FI), technology vendors, independent research organizations, and government agencies.
- Sponsors collaborative technology by development pilots, proofs of concept, tests, and demonstrations – supported by member FIs and technology companies.
- Mission: bring forward interoperable, open-standard technologies that provide critical infrastructures for the financial services industry.
- In November 2002, FSTC began the SAML and Liberty Alliance specifications review project.



FSTC Review of SAML/Liberty

- FSTC Members requesting guidance on use and application of web services security – specifically SAML, Liberty, Passport (.Net), WS-Security to financial services industry
- Security Committee organized a funded review and analysis of the SAML and Liberty Alliance specifications
- Project team: FIs and technology vendors (next page)
- Deliverable: Report comparing specifications; analyzing key business and technical questions related to implementations; providing recommendations to FIs, and Standards Bodies, such as OASIS, Liberty and BITS.
- Status: Report to be released at Burton Catalyst Conference in San Francisco during week of July 9th.



Project Participants

- **Sponsoring Institutions**
 - Bank of America, Fidelity, JPMorganChase, Wells Fargo
- **Other participating Financial Institutions**
 - CitiGroup, Glenview, National City, University
- **Technology Partners**
 - HP, SUN, DRG, Yodlee, eOne Global
 - Niteo Partners (NEC), Top Layer, Glenbrook Partners

Questions FSTC Asked

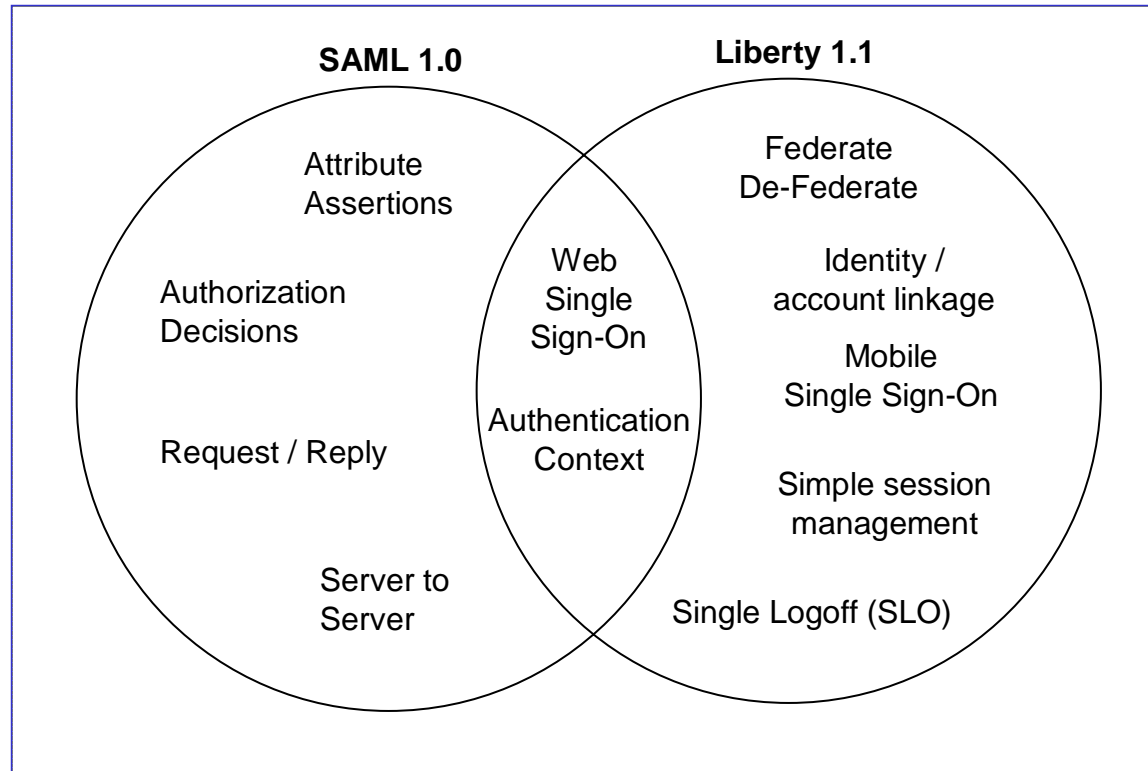
1. Do these specifications meet FI-specific requirements for customer interactions?
2. Are they applicable to B2B as well as B2C?
3. How do these specifications compare with traditional models for identity management between FIs (e.g. SSO, and aggregation)?
4. Will the security and privacy models provided by SAML and LA meet the needs of the financial industry?
5. What about performance and scalability?
6. Are there additional considerations beyond the technical aspects that FIs should consider when evaluating or implementing the specifications?
7. Are there compelling business opportunities that would support or leverage the capabilities inherent in these specifications?



Overview Use Cases

- **Use Case 1 – B2B:**
 - Business exchange portals securely incorporate supplier content in customer presentation and customer content in supplier presentation. End to end supply chain automation
 - Banks uniquely positioned to benefit via payments
- **Use Case 2 - B2E:**
 - Single Sign-On experiences with outsource services. Travel; 401K
- **Use Case 3 – Securing Aggregation Services (B2C):**
 - Eliminate need for consumers to share online banking credentials with aggregators
 - Evolve data feeds from screen scraped HTML to web services
 - Evolve delegated aggregator authentication to SAML identity assertion (for XML data feeds)

SAML and Liberty Context



- SAML and Liberty specifications do not compete with one another.
- Liberty technical specification includes SAML as a key foundation element, leveraging both the Web browser and Web service profiles.
- Beyond SAML, Liberty adds incremental network identity elements that were outside SAML's scope.
- Liberty not only provides additional capabilities beyond the core SAML specification, but it also provides further constraints.



Partial List of Specific Findings

- SAML compliance does not guarantee interoperability
- Name space ambiguities left to implementers to resolve
- Session keep-alive across multiple sites required
- SAML doesn't provide additional assertions for wide range of applications beyond SSO
- Need SAML assertion schema for account delegations (potential role for FSTC?)
- Need server-server protocol model (Liberty 2.0)
- Need “official” SAML-SOAP binding (WS-Security)
- Need OFX & IFX web service bindings (nascent)



Comparative Analysis

SAML benefits

- Passes security context between apps
- Highly Extensible
- Supports industry-standard transport and messaging bindings – browsers, HTTP Post, MIME, SOAP, ebXML

SAML drawbacks

- Interoperability not assured
- Single log out not provided in SAML
- No ability to federate identity
- No ability to opt-out

Liberty benefits

- Well-suited for B2C and B2E SSO and sign-out.
- Uses SAML to provide SSO.
- Provides single log-out
- Authentication context provided

Liberty drawbacks

- Bulk federation not provided
- Does not define support mapping for customer service
- Server to server interactions are beyond scope of Liberty 1.1
- Inadequate ability to determine strength of authentication (I.e. strong authentication)



Report Recommendations

- Value proposition for online identity standards is compelling for Financial Services industry
 - Adoption is really underway, not always obvious
- Non-technical aspects of solution need attention
 - Liability model, bilateral agreements, privacy, non-repudiation, marketing
- Technical standards finally (almost) ripe
 - SAML provides sound foundation, Liberty broadens
 - WS-SECURITY emerging as key piece of solution
 - OFX / IFX need to adopt SAML security or SOAP



Clouds on the Horizon



- Competing Standards
- Liability & Repudiation
 - Assumptions untested
- Privacy
 - Opt-in versus Opt-out
 - GLBA, EU
- When is a standard a standard?
 - “Liberty Alliance not a standards body”
- Microsoft Passport
- Federations versus centralization
 - Liberty Circles of Trust
- Web services
 - WS-security SAML binding
 - OFX, IFX SOAP bindings
- SAML may change

References

- **Liberty Alliance** - www.projectliberty.org
 - Best Practices Whitepaper – Security and Privacy
https://www.projectliberty.org/specs/Project_Liberty_Best_Practices4.14.03.pdf
- **OASIS** – www.oasis-open.org
 - Security Services Technical Committee (SSTC)
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- **W3C** – www.w3.org (SOAP work)
- **FSTC** – <http://www.fstc.org/projects/liberty/index.cfm>
- **DRG** – www.drgsf.com