

SF ISACA – Fall 2002 eXciting Seminar

# Web Services Security Overview

Jim Cowing  
Digital Resources Group  
[www.drgsf.com](http://www.drgsf.com)

October 18, 2002

# Agenda

*Introduction to Web Services Overview*

*Types of Web Services, Terminology, & Standards*

*Security of Web Services*

*Requirements for Web Security ?*

*Web Services Security Standards Efforts*

*XML Security Standards*

*SAML*

*Liberty Alliance*

*WS Security*

*- Security and Authentication Implications: How Web Services Impact IM and Single Sign On*

# Digital Resources Group (DRG)

- ❖ *Leading Internet Security Company since '97.*
- ❖ Focus: Security Strategy, New Technologies and Assessment Services
- ❖ Industry Focus: Financial Services
- ❖ Headquartered in Redwood Shores, CA
- ❖ Independent Security expertise

# Disclaimer

- ❖ *No affiliation with any of these vendors. DRG has no vested interest in any particular vendor technologies (i.e. no affiliation with Microsoft, IBM, Sun or others in this space).*
- ❖ *We are not Developers, nor are we Web Services Experts – we do not code.*
- ❖ Our expertise is in Security – concern for clients web-based transaction security.
- ❖ The views expressed here are only my opinions based on what we've heard so far.

# What Are Web Services?

# Web Services enables

- ❖ a new model for using the Web to:
  - ❖ Automate initiation of web processes using programs
  - ❖ Method for describing, publishing, promoting, registering, & initiating processes dynamically in a distributed environment
  - ❖ New ways of using the web, including intelligent agents, marketplaces & auctions
  - ❖ And... Not necessarily using a Web browser!
  
- ❖ All done using XML standards.

# Web Services Hype

- ❖ XML Adoption rapidly Accelerating
- ❖ Web Services represents the Next Generation of Internet Development
- ❖ New model for Services and Content Delivery enabling Distributed eBusiness Applications
- ❖ Multi-Vendor – Promotes **Interoperability**
- ❖ Standards are Evolving
  - ❖ XML, SOAP, WSDL, UDDI
- ❖ Lack of End-to-End Security Solutions
  - ❖ Use of SSL and proprietary solutions Today
  - ❖ No shortage of Security Efforts

# Web Services enable

- ❖ Application to application requests and responses over the web stack
  - ❖ SSL
  - ❖ HTTP/SMTP/...
  - ❖ XML
  - ❖ SOAP
  - ❖ UDDI
- ❖ Registry
- ❖ RPC and Business Messaging
- ❖ all loosely coupled...

# Characteristics of Web Services

- **Reliable & Transparent Interconnectivity**
  - Web Protocols
- **Structured Information**
  - XML Schemas & validation
- **Application Interface Standards**
  - UDDI, WSDL, SOAP
- **Consistent Definitions**
  - Profiles, Test Suites & Scenarios
- **Business Process Interface Standards**
  - ebXML, BTP, BPEL4WS, etc.
- **Security / Infrastructure Standards**
  - SAML, XACML, etc. (Eventually !!!)

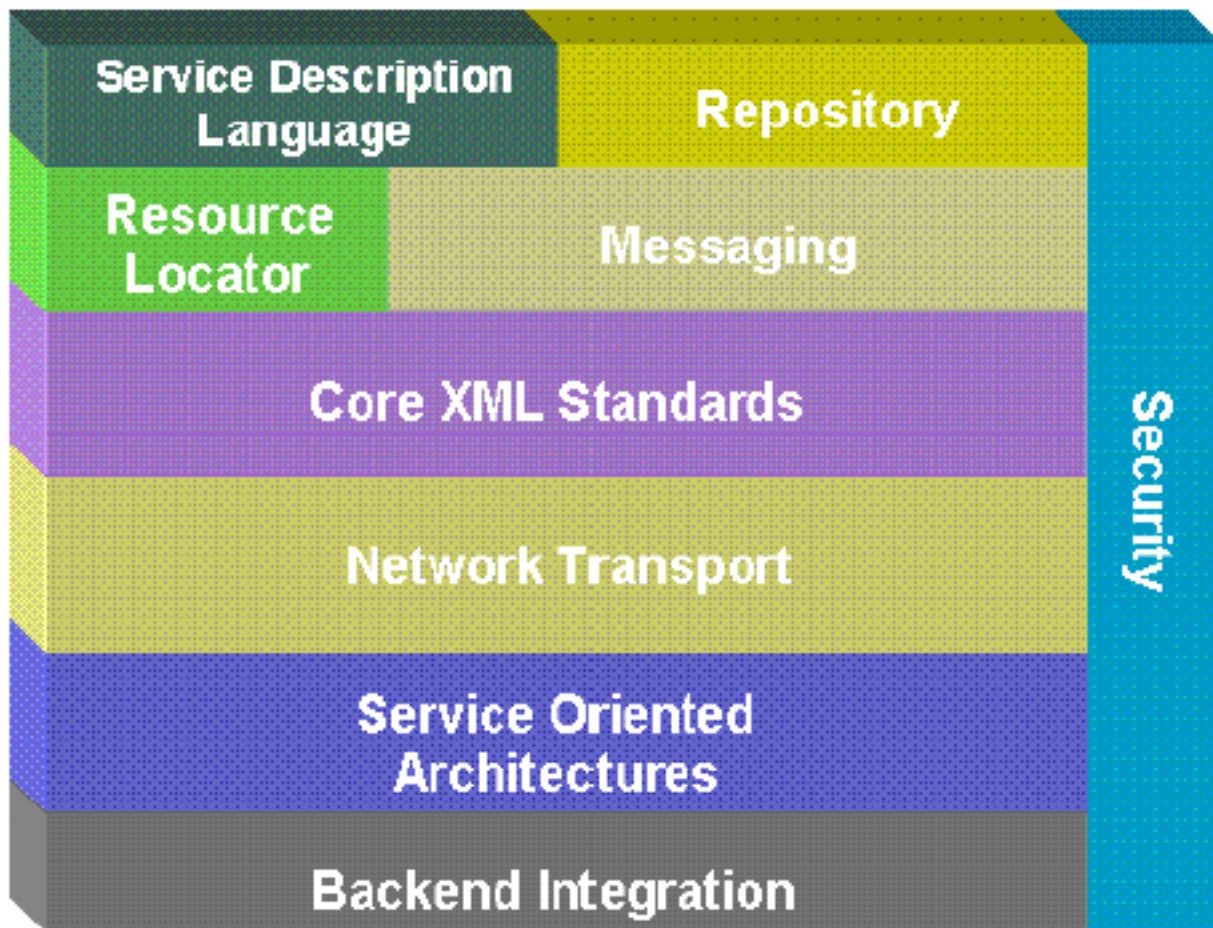
The fundamental characteristics of Web Services are interoperability & consistency across platforms, applications & programming languages.

Checkpoint:

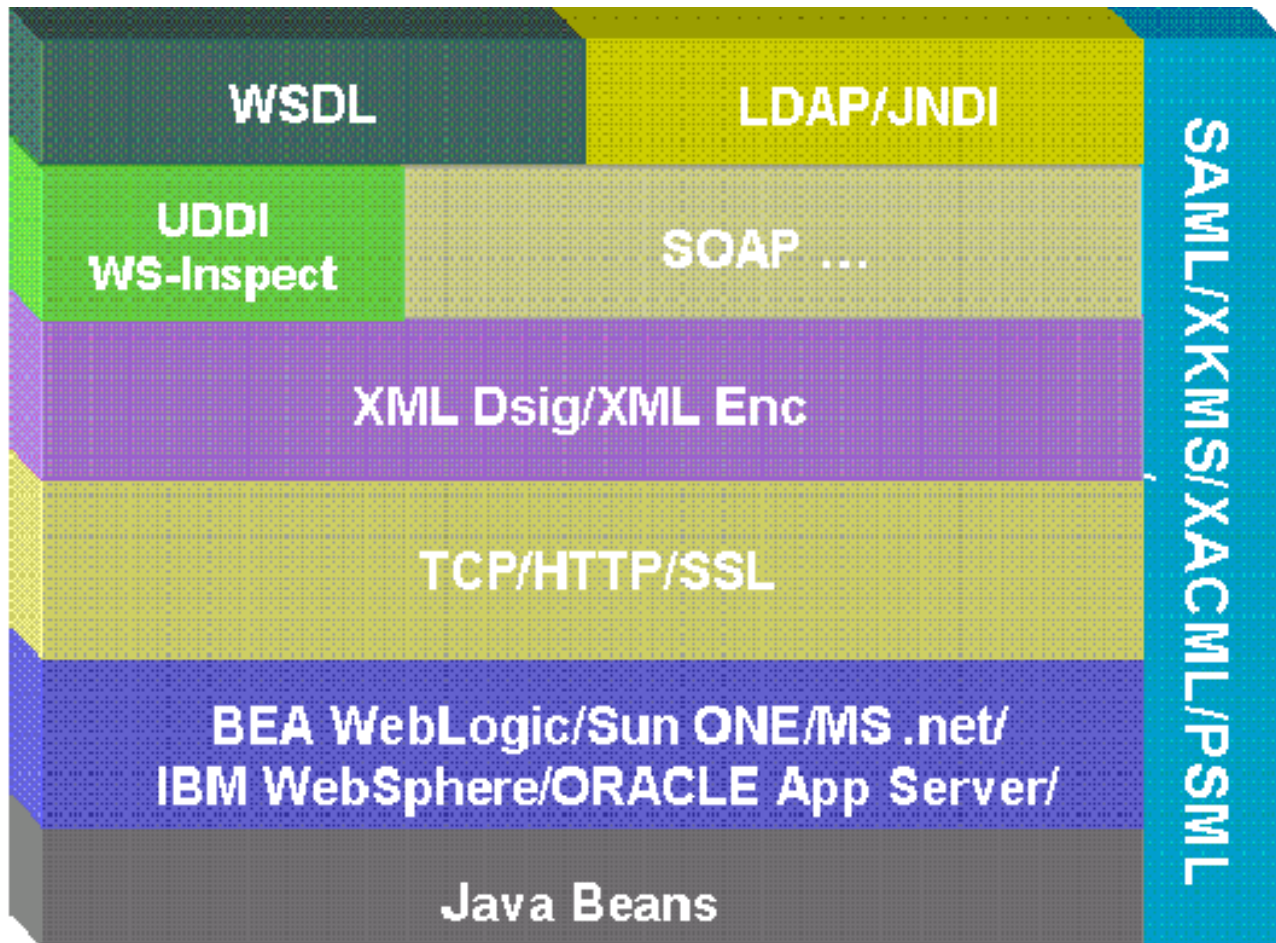
**Why are Web Services  
relevant to IS Auditors ?**

**What applications are your  
customers building in Web Services?**

# Web Services Core Architecture



# Web Services Core Specifications



# Web Services Component Standards

- ❖ eXtensible Markup Language (XML) – W3C
  - ❖ Data format description language
- ❖ Small Object Access Protocol (SOAP)
  - ❖ W3C XML Protocol WG – SOAP v1.2
  - ❖ Still in process
- ❖ Web Services Description Language (WSDL)
  - ❖ W3C WS Description WG started Jan. 2002
- ❖ Universal Description, Discovery & Integration (UDDI)
  - ❖ OASIS Member Section August 2002
    - ❖ First TC meeting 9/13

# What is WSDL?

- ❖ Web Services Description Language (WSDL)
  - ❖ XML Format for describing Web Services as end points acting on messages containing either documents or procedural calls (Port Types)
  - ❖ Describes service; who operates it, where it is located, and how to access
  - ❖ WSDL v1.1 (IBM & MS) W3C Note Mar. 2001
  - ❖ W3C WS Description WG started Jan. 2002

# What is UDDI ?

## ❖ Universal Description, Discovery & Integration (UDDI)

- ❖ Facilitates Describing/Discovering Services & Business
- ❖ Registration of Business Identity Information
- ❖ UDDI.org v3.0 specification August 2002
- ❖ OASIS Member Section August 2002
  - ❖ First TC meeting 9/13
- ❖ Sometimes referred to as the Web Services Yellow Pages.

# SOAP Messages

- ❖ XML-based protocol defines a vocabulary for electronic message exchange -- "envelope"
- ❖ Message itself is encoded in another specific vocabulary – HTTP, JMS, etc.
- ❖ Uses XML structure to create request-response messages
- ❖ Still being developed to address more complex business requirements
- ❖ Hides application technology from users / other services
- ❖ Does NOT define a security mechanism.
- ❖ **Today – we see SSL as primary security mode.**

# SOAP Example

## SOAP Message embedded in an HTTP Request

```
POST /StockQuote HTTP/1.1
Host: www.stockquoteserver.com
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "Some-URI"
```

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  <SOAP-ENV:Body>
```

## SOAP Header

```
<SOAP-ENV:Header>
  <t:Transaction
    xmlns:t="some-URI" SOAP-
    ENV:mustUnderstand="1">
    5
  </t:Transaction>
</SOAP-ENV:Header>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
</SO
```

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <m:GetLastTradePriceResponse xmlns:m="Some-URI">
      <Price>34.5</Price>
    </m:GetLastTradePriceResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

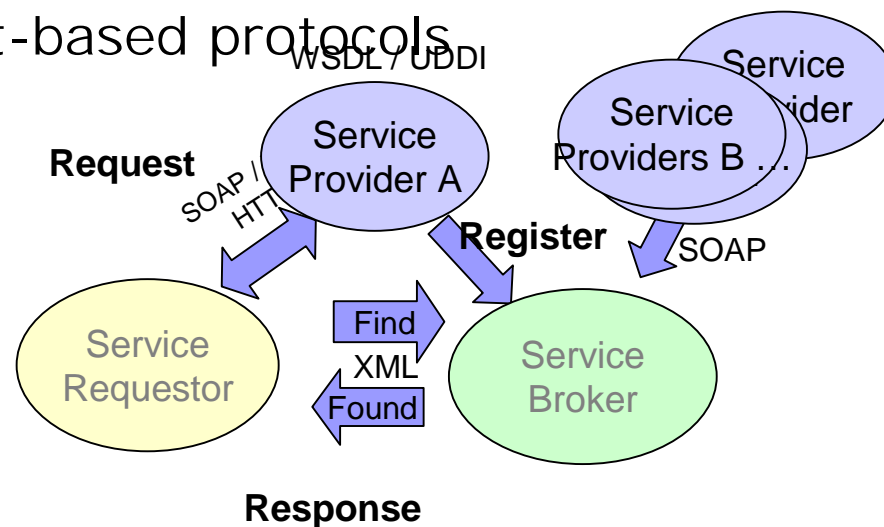
## SOAP Message embedded in an HTTP Response

# Two Types of Web Services

1. Remote Procedure Call (RPC) Based
  - ❖ Supports simple Web Services
2. Conversational Based
  - ❖ Message-based, supporting loosely coupled asynchronous models
  - ❖ A key requirement for Enterprise-class Web Services
  - ❖ Essential for complex Web Services

# RPC-based Web Services

- ❖ Components that provide a service to a user
  - ❖ Human or computer based users
  - ❖ Can be located anywhere
  - ❖ Appears as a remote object to the client application
  - ❖ Tightly coupled and resemble traditional distributed object paradigms, such as RMI or DCOM
  - ❖ Can be implemented in many programming languages
  - ❖ Access is done through Internet-based protocols
  - ❖ Synchronous
    - ❖ Waits for a response
  - ❖ Does not address business processes



# Conversational Web Services

- ❖ Message-based Conversational Web Services
  - ❖ *Loosely coupled, asynchronous* & document-driven
  - ❖ Client invokes a message-based Web Service by sending entire document, such as a purchase order, rather than a discrete set of parameters
  - ❖ Web Service accepts the entire document, processes it, & may or may not return a result message
  - ❖ Promotes a looser coupling between client & server & provides additional benefits beyond RPC-based Web Services
  - ❖ More transactions oriented; offering non-repudiation capabilities

# Business Drivers

- ❖ LOTS of momentum behind Web Services
  - ❖ Business needs a secure mechanism for service-service, client-service, and mobile-service messaging
  - ❖ Early consumer-oriented services based on proprietary solutions, such as Microsoft's Passport
  - ❖ Web services development tools now available from Microsoft, IBM, Sun and other Java tool vendors
  - ❖ Yet...Enterprise concerns around security and interoperable standards threaten to this Web services momentum:
    - ❖ According to Burton, Security is cited as biggest implementation obstacle by 45% of IT development managers in recent survey

# Business Requirements

## ❖ Security considerations

- ❖ Authentication of service provider/responder
  - ❖ Prevents spoofing and exposure of private information
- ❖ Authentication of service requestor
  - ❖ For all the traditional reasons, and as an essential element in support of authorization, auditing, and liability for the service
- ❖ Transactional integrity
  - ❖ To ensure that transactions cannot be modified, once initiated
- ❖ Confidentiality
  - ❖ To protect the privacy of both the service requestor and any information being provided as a result of the transaction
- ❖ Nonrepudiation and auditability of the transaction

# Elements of Security



Element	Description
Identification	Who are you?
Authentication	How do I know you are who you say you are?
Authorization	Are you permitted to do that ?
Integrity	Is the data sent the same as that data received ?
Confidentiality	How we ensure no one has read the data sent
Auditing	Record of transactions
Non-repudiation	Can you prove that both ends received the same identical transaction

# Web Services Security Standards Players

- ❖ Microsoft – Passport .NET
- ❖ W3C – *XML Security Specifications*
- ❖ OASIS – *Assertions – SAML v.1*
- ❖ Liberty Alliance – *Federated Identity*
- ❖ WS-Security - *SOAP extensions*
  - ❖ IBM, Verisign & Microsoft advanced
  - ❖ now OASIS TC

# XML Security Standards

## W3C

### XML DSIG

-  XML Digital Signature – Authenticate message /Integrity -- Recommendation W3C

### XML Encryption

-  XML Message Privacy -- -Working Draft W3C -

### XML Key Management Services

-  Public key registration & Vallidation -- 2.0 Working Draft W3C

## Security-Related OASIS Standards:

### XCBF Biometric Security Data

### XrML Rights Management (DRM) – requirements

### XSPML Service Provisioning Markup Language

### XACML Access Control Markup Language

-  Community draft- OASIS

# Competing Web Services Security

- ❖ SAML – ver 1.0 Open Standard
  - ❖ XML authentication & authorization
  - ❖ July 15 – Burton Interoperability Demo & initial specification released
- ❖ Liberty Alliance spec – ver 1.0 Membership limited
  - ❖ Federated identity advanced
  - ❖ Specification Publicly available – July 15
- ❖ WS- Security
  - ❖ Defines SOAP message headers for confidentiality and integrity
  - ❖ IBM, Verisign & Microsoft advanced
  - ❖ OASIS TC formed for WS-Security – July 23

# SAML

# Security Assertion Markup Language


- ❖ "SAML" - new XML vocabulary
- ❖ XML-based framework for exchanging certain security information – specifically SAML describes authentication & authorization
- ❖ XML-encoded security "assertions"
- ❖ SAML was intended to provide heterogeneous Single Signon for both portal models
  - ❖ Browser profile gaining wide acceptance
  - ❖ SOAP profile pulled, awaiting ws-security
- ❖ SAML does not solve overall identity problem

# Anticipated SAML Use Cases


## Single Sign-On

-  classic case of web user authenticates at one site; then accesses another without re-authentication

## Authorization Services

-  User attempts to access a resource or service. The users authorization privileges are validated against rights database.

## Attribute Service

-  User move between website – loyalty or context is passed to simplify user experience as part of a federated info service.

# SAML Evolution

- ❖ Originally S2ML (Security Services Markup Language) pioneered by Netegrity with its partners:
  - ❖ Sun, webMethods, VeriSign, Oracle, Commerce One, TIBCO, PriceWaterhouseCoopers
- ❖ OASIS started Security Services Technical Committee (SSTC) in December 2000
- ❖ SAML 1.0 specification draft was presented to the OASIS Board for endorsement on May 28, 2002
- ❖ SAML reference implementation interoperability bake-off at Burton Group Catalyst conference on July 15, 2002
- ❖ SAML is technical foundation of Liberty Alliance spec

# Liberty Alliance

# Liberty Alliance

**Goal – to establish an Open Standard for Federated Network Identity through Open Technical Specifications that will:**

- Supporting 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 July 2002*

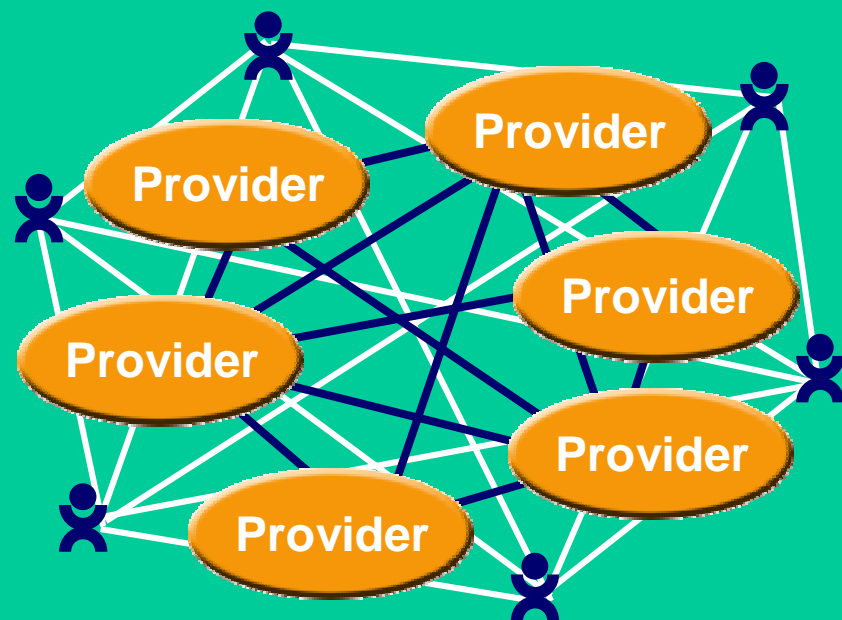
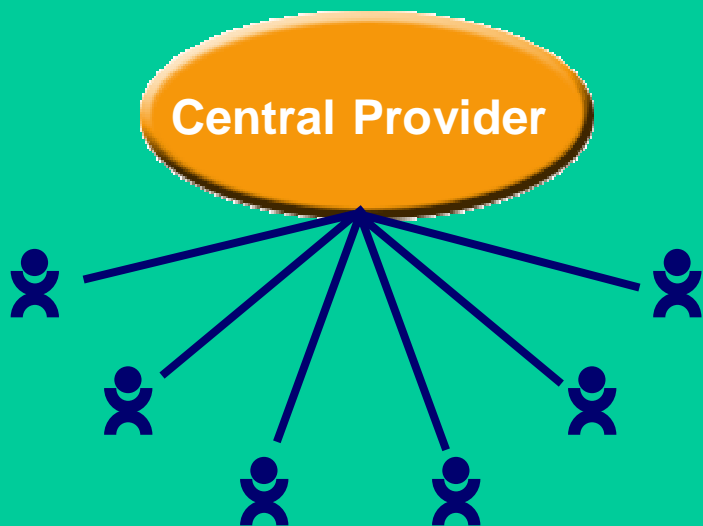
# What is Federated Identity ?

## Centralized Model

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

## Open Federated Model

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



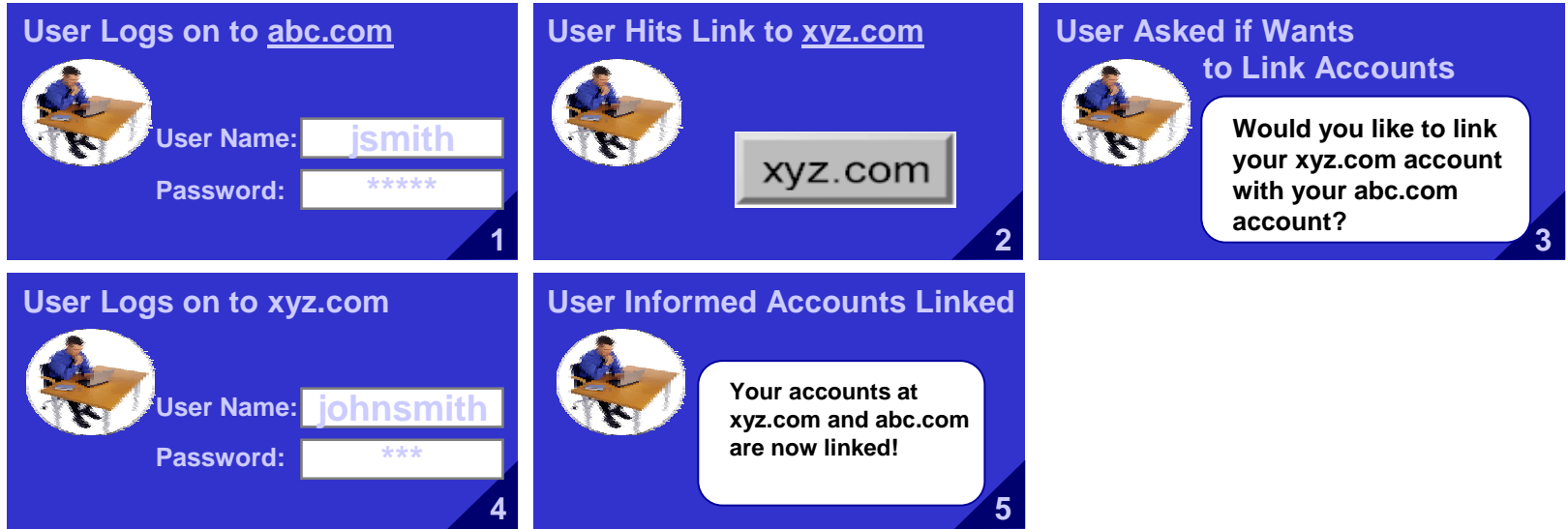
# Key Objectives of the Liberty Alliance

- **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 July 2002*

# User Experience - Version 1.0

## Account Federation



## Federated Simplified Sign-On



Source : Liberty Alliance July 2002

# Liberty Specifications: A Phased Approach

## Approach Drivers

- Support rapid acceptance and deployment
- Easy incremental adoption

### Version 1.0

- Federated network identity
- Opt-in account linking and simplified sign-on within an authentication domain created by business agreements
- Security built across all the features and specifications

### Future Versions

- Permissions-based attribute sharing
- Schema/protocols for core identity profile service
- Simplified sign-on across authentication domains created in version 1.0 by business agreements
- Delegation of authority to federate identities/accounts

# Liberty - Membership

- Over 62 active members (over a billion customers worldwide)
- Global coalition of companies.
- 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
- Open alliance that welcomes and encourages participation by all commercial and non-commercial organizations

# Liberty Alliance Project

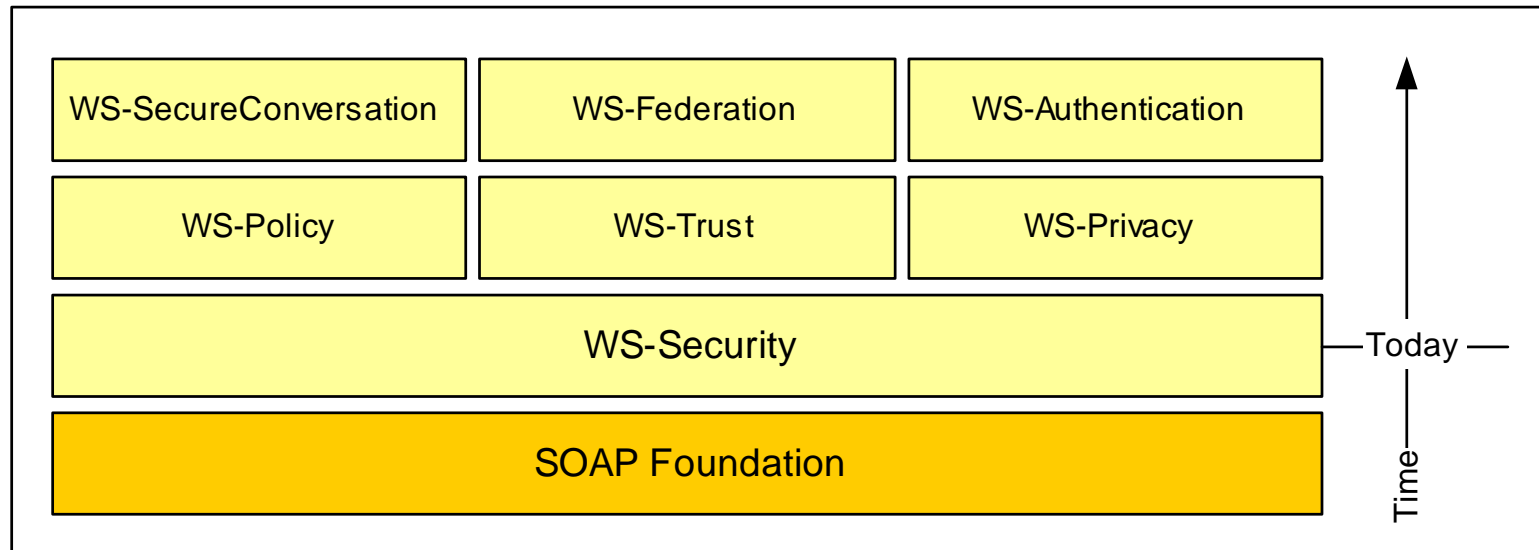
- ❖ A multi-industry, global business alliance
- ❖ Defining a widely accepted, interoperable “standard” for federated identity
  - ❖ Legal: liability model, standard bilateral agreements
  - ❖ Business: business model, branding, marketing
  - ❖ Technical: SAML plus user account linking etc.
- ❖ Sun has been the primary driver
  - ❖ no preferential treatment according to Alliance rules
- ❖ Microsoft supports SAML- not Liberty
  - ❖ Possibly future federation impacts could reshape Passport

# WS - Security

# WS Security

- Original specifications defined by IBM, Microsoft and Verisign.
- WS-Security extends and subsumes previous Web services security specifications published individually and jointly by IBM, Microsoft and Verisign.
- Specification defines foundational set of SOAP extensions used when building secure Web services to implement INTEGRITY and CONFIDENTIALITY.
- Describes how to exchange signed and encrypted messages in a Web services environment.
- Works with multiple security approaches: PKI, Kerberos, SAML, XrML, SSL, etc.
- First specification in a planned series that will help address end-to-end Web services security including federation across security domains.

# Web Services Security Strategy Roadmap



# How Does WS-Security Work?

1. *Messages have security tokens that assert claims*
2. *Web services have policies that describe required claims*
3. *A security token service is just a web service that issues security tokens*

# Security Tokens

Messages have security tokens that assert claims

Unsigned



...

Username

Proof of Possession



Secret Key



Password

Signed

X.509



Kerberos



...

XrML

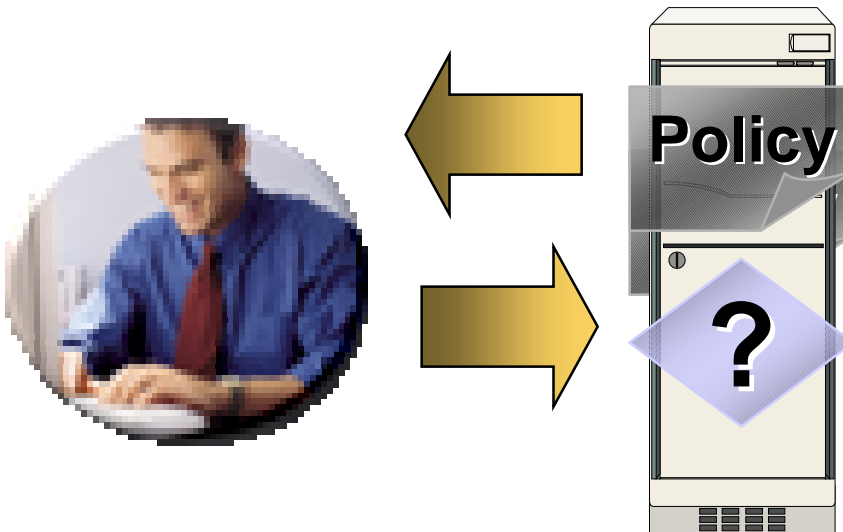


SAML

# Policies

**Web services have policies that describe required claims**

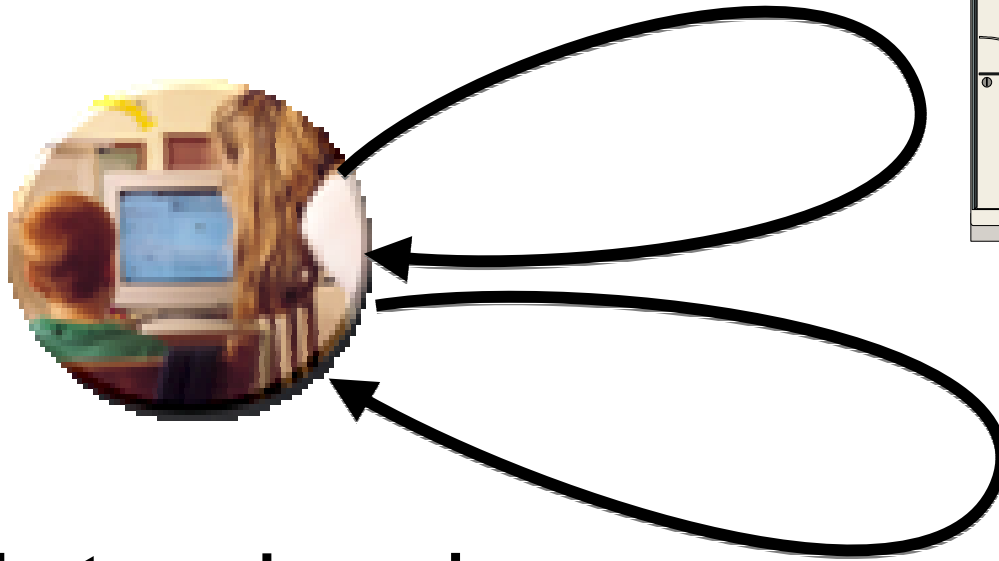
- **Policies can also describe where to get claims**



**Does the request have the correct security tokens?**

# Security Token Service

**A security token service issues security tokens**



- It is just a web service
- A solution may require multiple token services

Checkpoint:

How does all this fit with my business

Security and Identity initiatives

# The Need for Identity Standards

- ❖ Knowing Your Customer
- ❖ Multiple Channel Authentication
- ❖ Outsourced Business Components
- ❖ Business Partners and Alliances
- ❖ Prevent Fraud and potential identity theft
- ❖ Security
- ❖ Regulatory – certain industries

# Summary

- ❖ Web Services are coming quickly, in some cases, they are already here !
- ❖ Web services security is lacking today.
- ❖ End-to-end seamless security is critical for e-business to continue growth.
- ❖ IM and SSO – critical to next generation internet business success.
- ❖ Which technology and security standards will evolve – still open !
- ❖ Will this impact web services growth? – open!

# Resources & References

OASIS and SAML information:

- ❖ <http://www.oasis-open.org>
- ❖ <http://xml.org>
- ❖ <http://www.ebxml.org>
- ❖ <http://www.ws-l.org>

Liberty Alliance

- ❖ <http://www.projectliberty.org>

# DRG Security Consulting

Digital Resources Group LLC  
270 Redwood Shores Pkwy #210  
Redwood Shores, CA 94065  
650-508-8959  
Info@drgsf.com

**[www.drgsf.com](http://www.drgsf.com)**