



**The State of California**

**Federated Identity Management  
*Standards***

January 31, 2007

California Enterprise Architecture Program

# Federated Identity

- “Federation refers to the establishment of business agreements, cryptographic trust, and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions.”
- “Key to federated identity management are standardized mechanisms and formats for the communication of identity information between the domains.”

**OASIS**

**SAML**

**Liberty Alliance**

**WS-Federation**

# OASIS

A not for profit global consortium of 600 organizations that drive the development, convergence and adoption of e-business standards

<http://www.oasis-open.org/home/index.php>

# OASIS WS-Security Standards

- ***WS-Security*** (SOAP Messaging Security) - describes enhancements to SOAP messaging to provide quality of protection through *message integrity*, *message confidentiality*, and single *message authentication*. Also provides a general-purpose, but extensible, mechanism for associating security tokens with messages.

“WS-Security is a blueprint, implementation requires protocols and tokens. Liberty Alliance, WS-Federation, and SAML are implementation examples.”

# SAML

Security Access Markup Language – an XML standard for exchanging authentication and authorization data between security domains, that is between an *identity provider* and a *service provider*.

SAML is different from other security approaches because of its expression of security in the form of assertions about subjects.

# SAML is different

- Other approaches use a central certificate authority to issue certificates that guarantee secure communications from one point to another within a network.
- With SAML, any point in the network can assert that it knows the identity of a user or data. It is up to the receiving application to accept if it trusts the assertion.

# SAML

- “Think locally, act globally”
  - Users authenticate to their identity provider (“thinking locally”)
  - They are then able to access resources at one or many service providers (“acting globally”)
- SAML is defined in terms of *assertions*, *protocols*, *bindings*, and *profiles*.

# SAML *Assertions*

An *assertion* is a package of information that supplies one or more statements made by a SAML authority. SAML defines three different kinds of assertion statements.

- ***Authentication*** – The subject was authenticated by a particular means at a particular time.
- ***Attribute*** – The subject is associated with the supplied attributes.
- ***Authorization*** – A request to allow the subject to access the specified resource has been granted or denied.

# SAML *Protocols*

SAML defines a number of request/response protocols that allow service providers to:

- Request from a SAML authority one or more assertions including a query that meets a particular criteria.
- Request that an identity provider authenticate a principal and return the corresponding assertion.
- Request that a name identifier be registered.

# SAML *Protocols*

- Request that the use of an identifier be terminated.
- Retrieve a protocol message that has been requested by means of an artifact (used when authorization request is too long for an HTTP redirect).
- Request a near-simultaneous logout of a collection of related sessions (“single logout”). [*message threading*]
- Request a name identifier mapping.

# SAML *Bindings*

- Mappings from SAML request-response message exchanges into standard messaging or communication protocols are called SAML protocol *bindings*.
- SAML SOAP Binding defines how SAML protocol messages can be communicated within SOAP messages.
- SAML HTTP Redirect Binding defines how to pass protocol messages through HTTP redirection.

# SAML Profiles

- Defines constraints and/or extensions in support of the usage of SAML for a particular application.
- *Web Browser SSO Profile* specifies how SAML authentication assertions are communicated between an identity provider and service provider to enable single sign-on.
- SAML defines a series of *attribute profiles* to provide specific rules for interpretation of attributes in SAML attribute assertions.
  - X.500/LDAP, X.509, UUIDs, XACML (XML Access Control language)

# SAML Advantages

- ***Platform neutrality*** – SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of SOA.
- ***Loose coupling of directories*** – SAML does not require user information to be maintained and synchronized between directories.

# SAML Advantages

- *Improved online experience for end users*
  - SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication. In addition, identity federation (linking multiple identities) with SAML allows for a better customized user experience at each service while promoting privacy.

# SAML Advantages

- ***Reduced administration costs for service providers*** – Using SAML to “reuse” a single act of authentication (such as logging in with a username/password multiple times across multiple services) can reduce the cost of maintaining account information. This burden is transferred to the identity provider.

# SAML Advantages

- ***Risk transference*** – SAML can act to push responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

# SAML Features

- ***Attribute-Based Authorization*** – identity information may be some characteristic of the subject (such as a person’s role) rather than, or in addition to, information about when and how the person was authenticated.

This feature is important when the individual’s particular identity is either not important, should not be shared for privacy reasons, or is insufficient on its own.

For example, is the user a member of a role?

# SAML Features

- ***Securing Web Services*** – SAML assertions can be used within SOAP messages to convey security and identity information between web service interactions.

The SAML token Profile (OASIS WS-Security) specifies how SAML assertions should be used for this purpose within the WS-Security framework.

WS-Trust proposes protocols for the exchange and validation of security tokens described in WS-Security. SAML assertions are one such security token format.

# SAML Features

- *Pseudonyms* – SAML 2.0 defines how an identifier (for example, a computer generated ID) can be used between providers to represent Principals. Pseudonyms are a key privacy-enabling technology because they inhibit collusion between multiple providers (as would be possible with a global identifier such as an email address).

Pseudonyms were incorporated from Liberty Alliance (opaque identifiers).

# SAML Features

- *Encryption* – SAML 2.0 permits attribute statements, name identifiers, or entire assertions to be encrypted.

This ensures end-to-end confidentiality.

**Liberty Alliance**  
**(Federated Identity for Web Services)**  
<http://www.projectliberty.org/>

# Who is Liberty Alliance

- The Liberty Alliance was formed in 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for federated identity management.
- Released Liberty Federation in 2002
- Released Liberty Web Services Framework in 2003
- 170 members today including global technology vendors, consumer-facing companies, educational organizations and governments from around the world.

# Liberty Alliance

- Three major components
  - ID-FF (Federated Framework)
  - ID-WSF (Web Services Framework)
  - ID-SIS (Service Interface Specifications)

# ID-FF (Federated Framework)

- ***Principal*** – the customer (constituent)
- ***Identity Provider (IdP)*** – creates, maintains, and manages identity information for Principals, and authenticates and vouches for the Principal to other Service Providers.

“A Principal has an account with an IdP”

- ***Service Provider (SP)*** – provides the services to the customer. May also be an identity provider.

# ID-FF (Framework)

- ***Attribute Provider (AP)*** – provides attribute data regarding the Principal to Service Providers based on its own policies and the Principal’s usage directives.

“Identity attributes may come from multiple APs, and they may have different usage policies”

- ***Personally Identifiable Information (PII)***  
– any data that identifies or locates a particular person, consisting primarily of name, address, telephone number, e-mail address, bank account, SSN number, drivers license number, etc.

# Circles of Trust

- **A contractual relationship between service and identity providers**
  - What type of information will be shared
  - How and when it will be shared
  - How it will be treated
  - What security procedures will be used to maintain confidentiality
  - How participants may join or leave the COT
  - How the COT will be administered

# ID-FF

- ***Interaction Service*** – provides a means for an Attribute Provider to request that a Service Provider obtain consent from a Principal.
- ***Consent Header*** – carries an indication of whether consent has been obtained from the Principal.
- ***Usage Directives*** – attributes may be coupled with usage directives, which provide permissions to the AP for the use and sharing of that attribute.
  - Identity and reference a rights expression language (REL)
  - Provide audit and log capability

# ID-WSF (Web Services Framework)



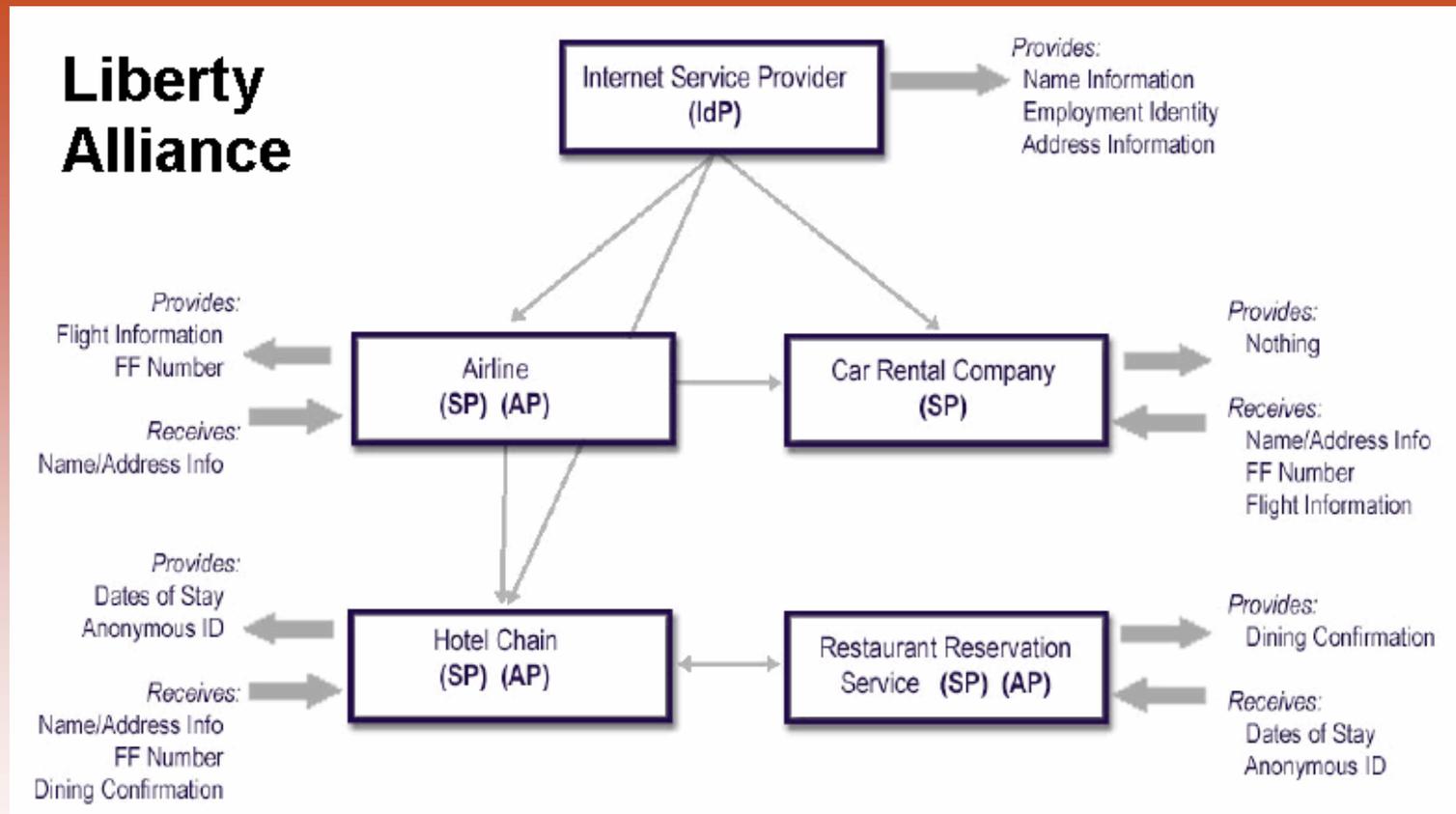
- ***Authentication*** –
  - Federated Name Identifier
  - Name identifier encryption
  - Opaque identifiers (pseudonyms)
- ***Message Protection***
  - SOAP binding and message threading (key federation principle)
- ***Discovery Service (DS)***
  - Discover services belonging to a particular user
  - Uses privacy-protected name and resource identifiers
  - Decentralized attributes (multiple providers)
- ***Policy***
  - Usage directives (determines how and where attributes can be used)
- ***Common data access protocols***

# ID-SIS (Service Interface Specs)

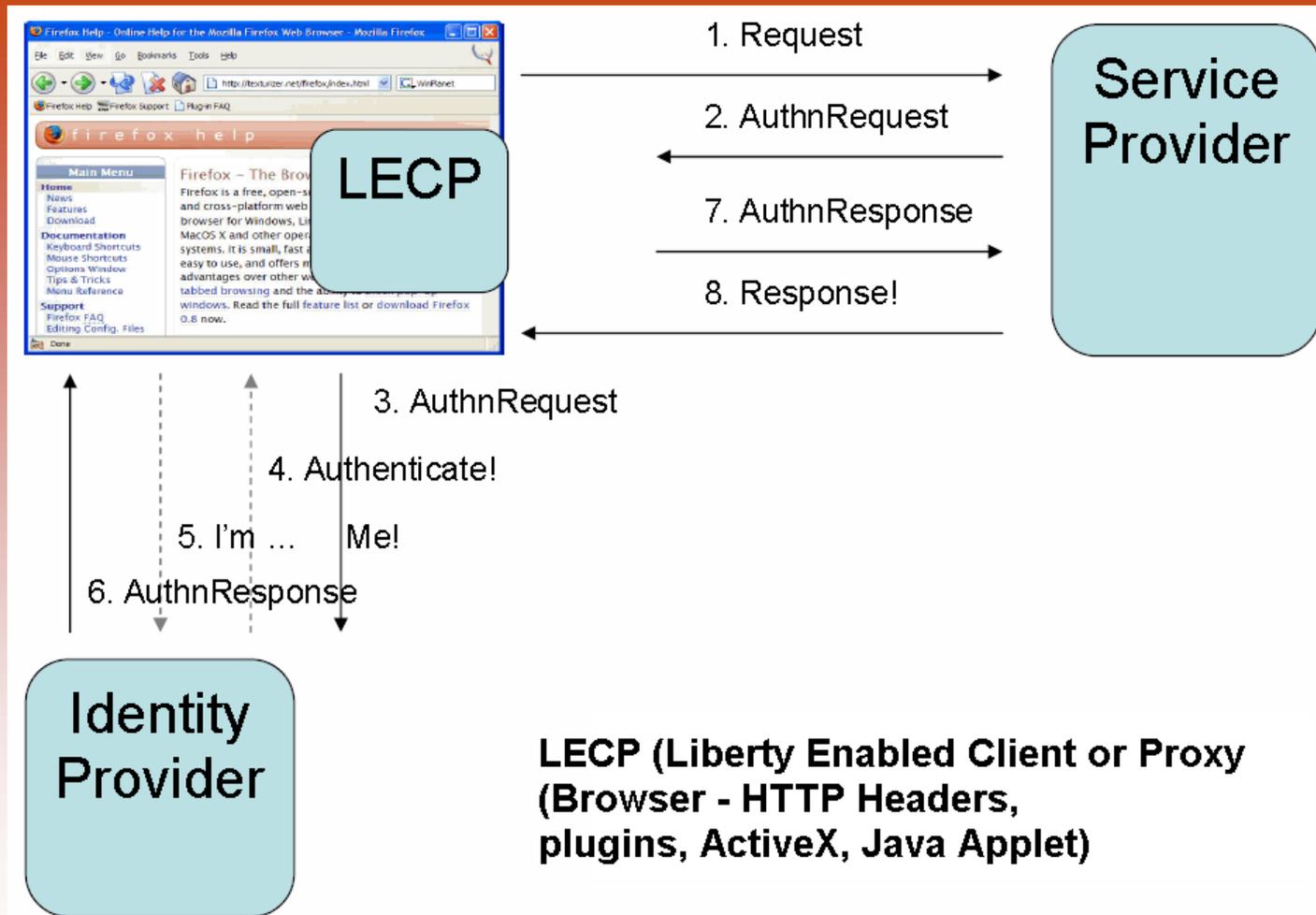


- ***Personal Profile Service***
  - Informal Name, Common Name, Legal Name, Employment Name, Address Card, Message Contact, Façade (photo, web site), Emergency Contact, Extensions.
- ***Employee Profile Service***
- ***Geolocation Service*** - Specifies a web service offering geolocation information associated with a Principal.
- ***Presence Service*** - Specifies a web service offering presence information associated with a Principal.

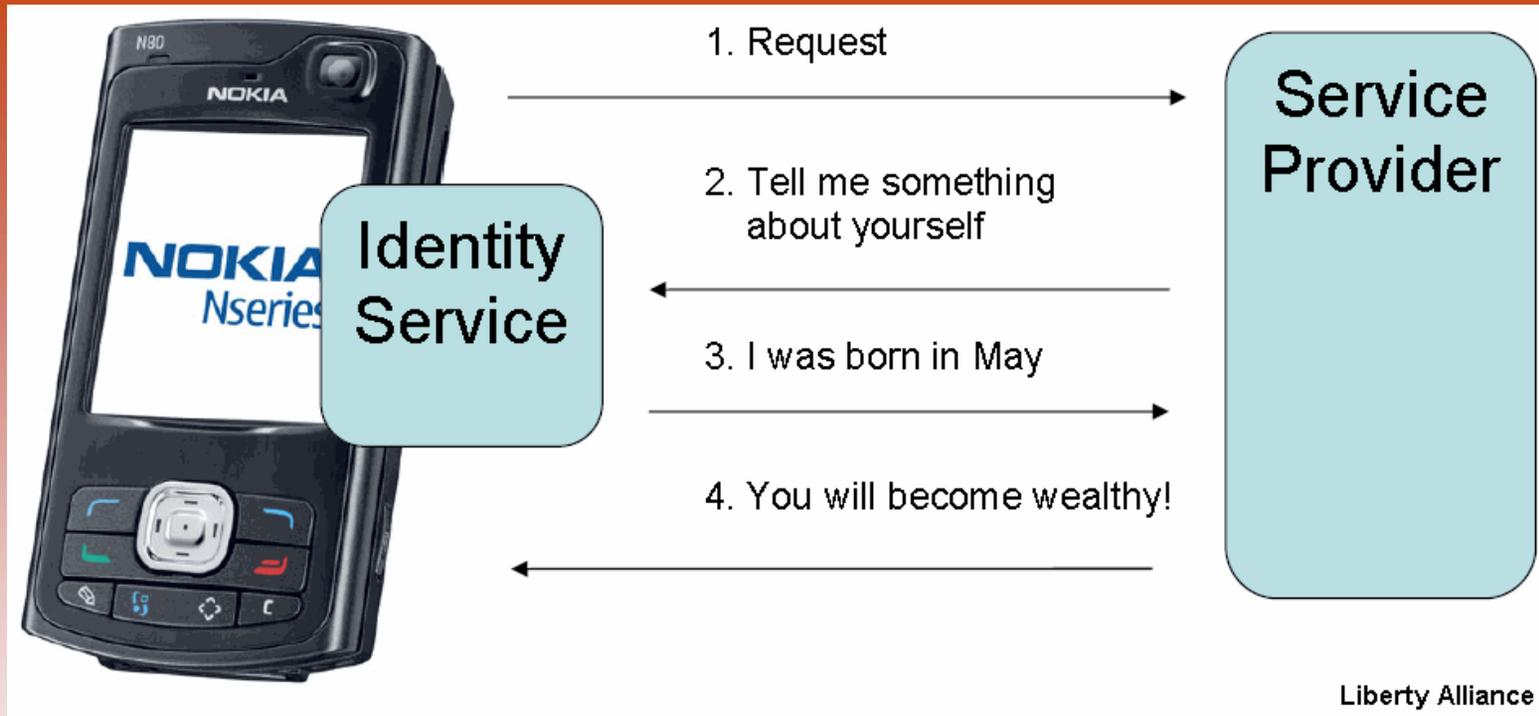
# Example Business Model



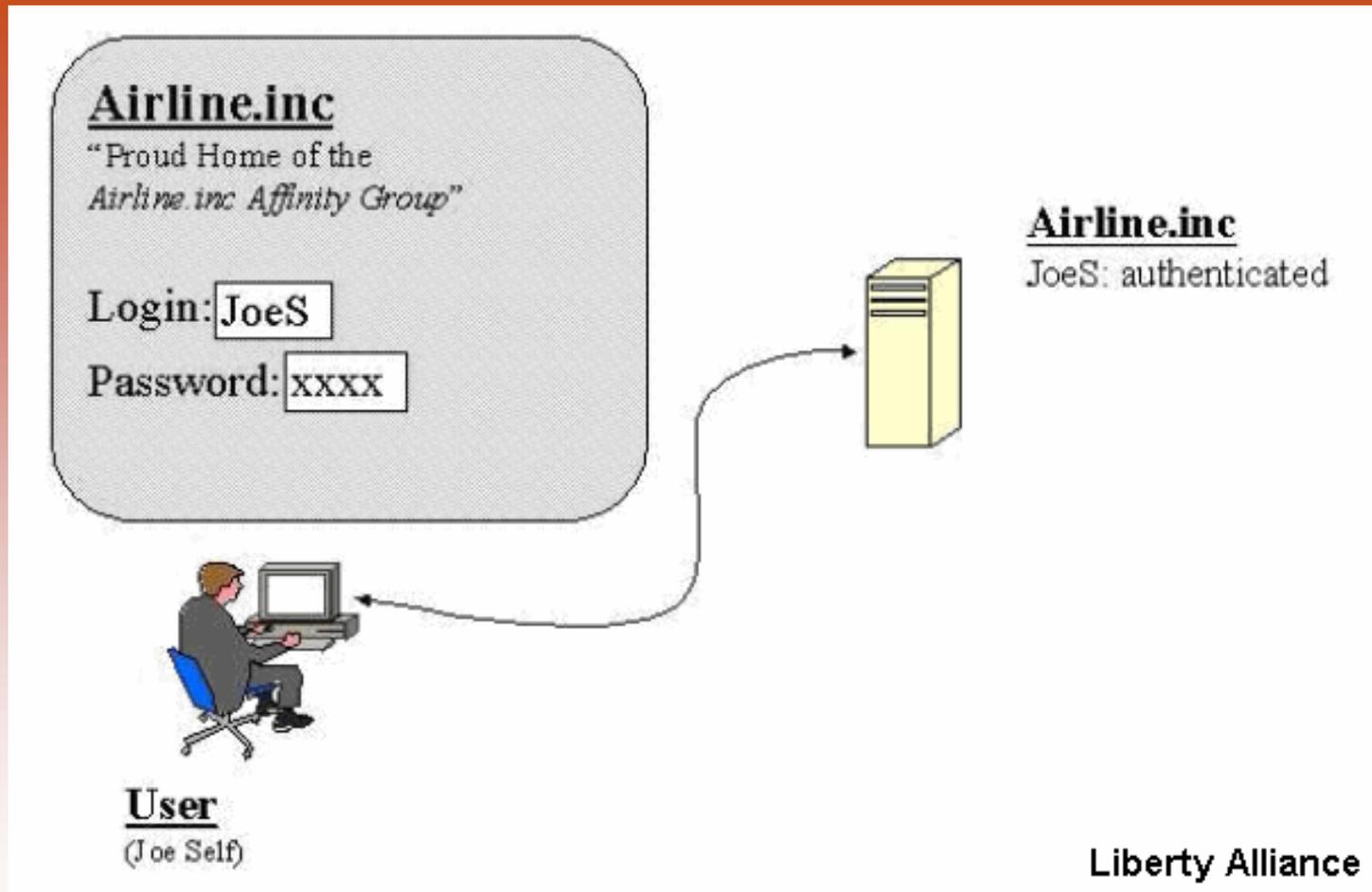
# Separate Identity Provider



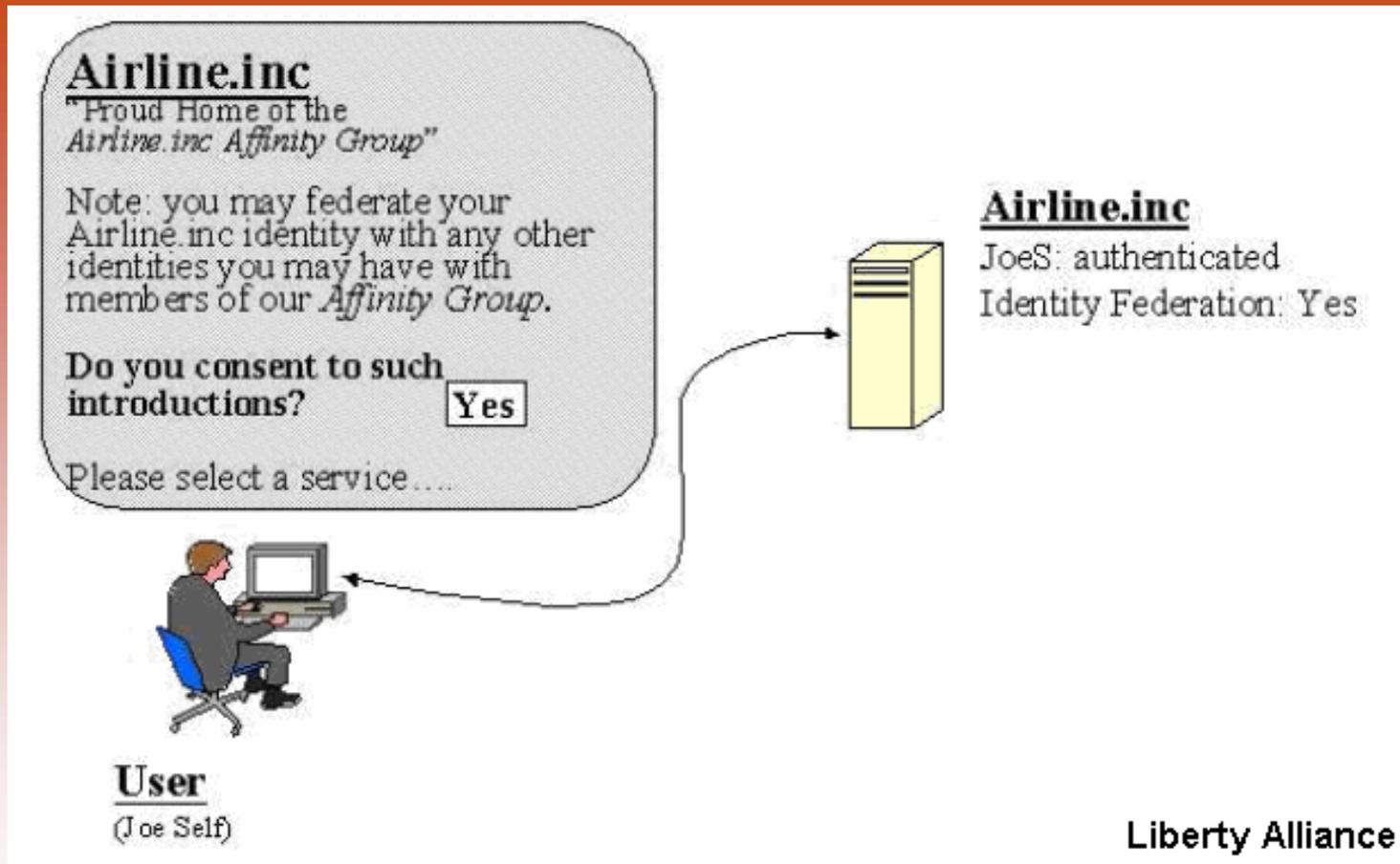
# Personal Identity Provider



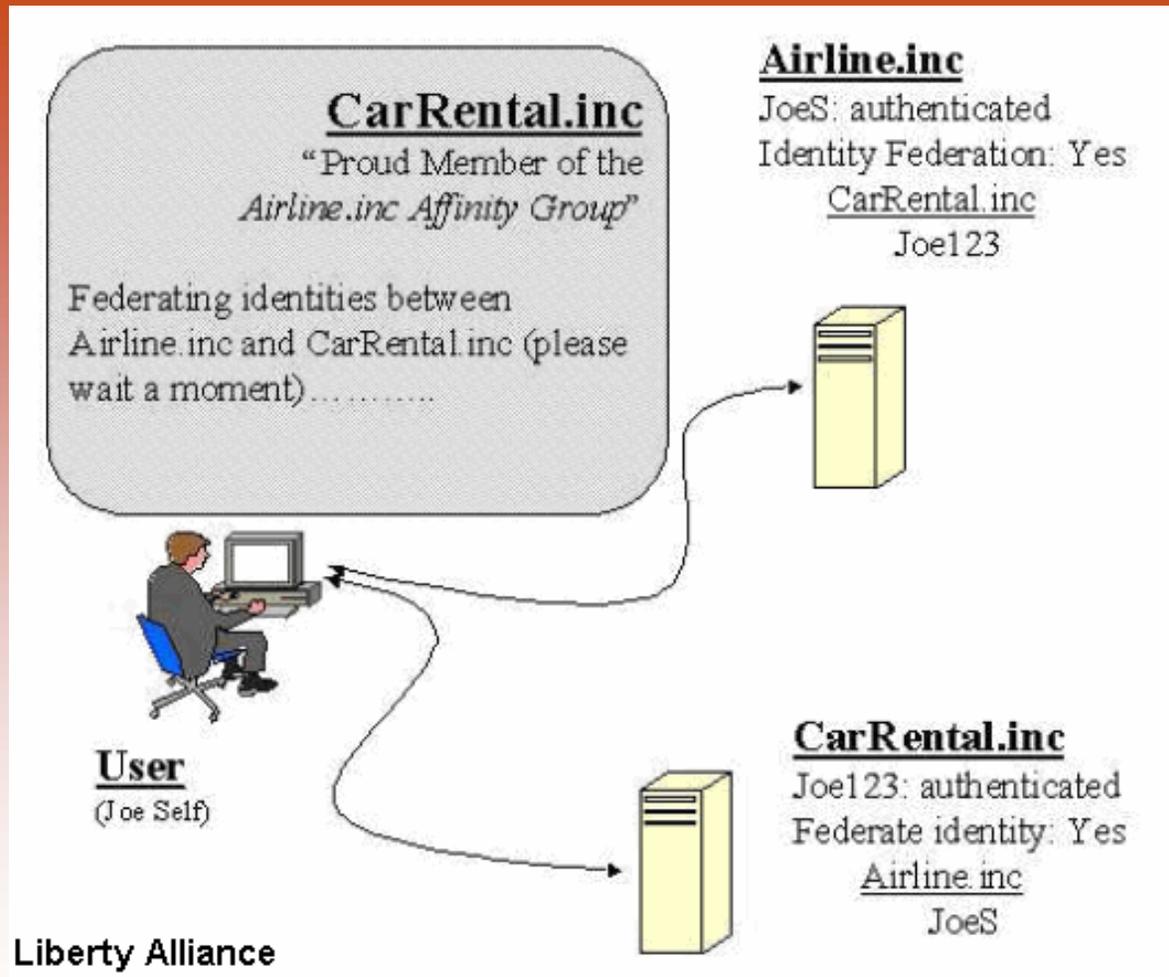
# Example Federation



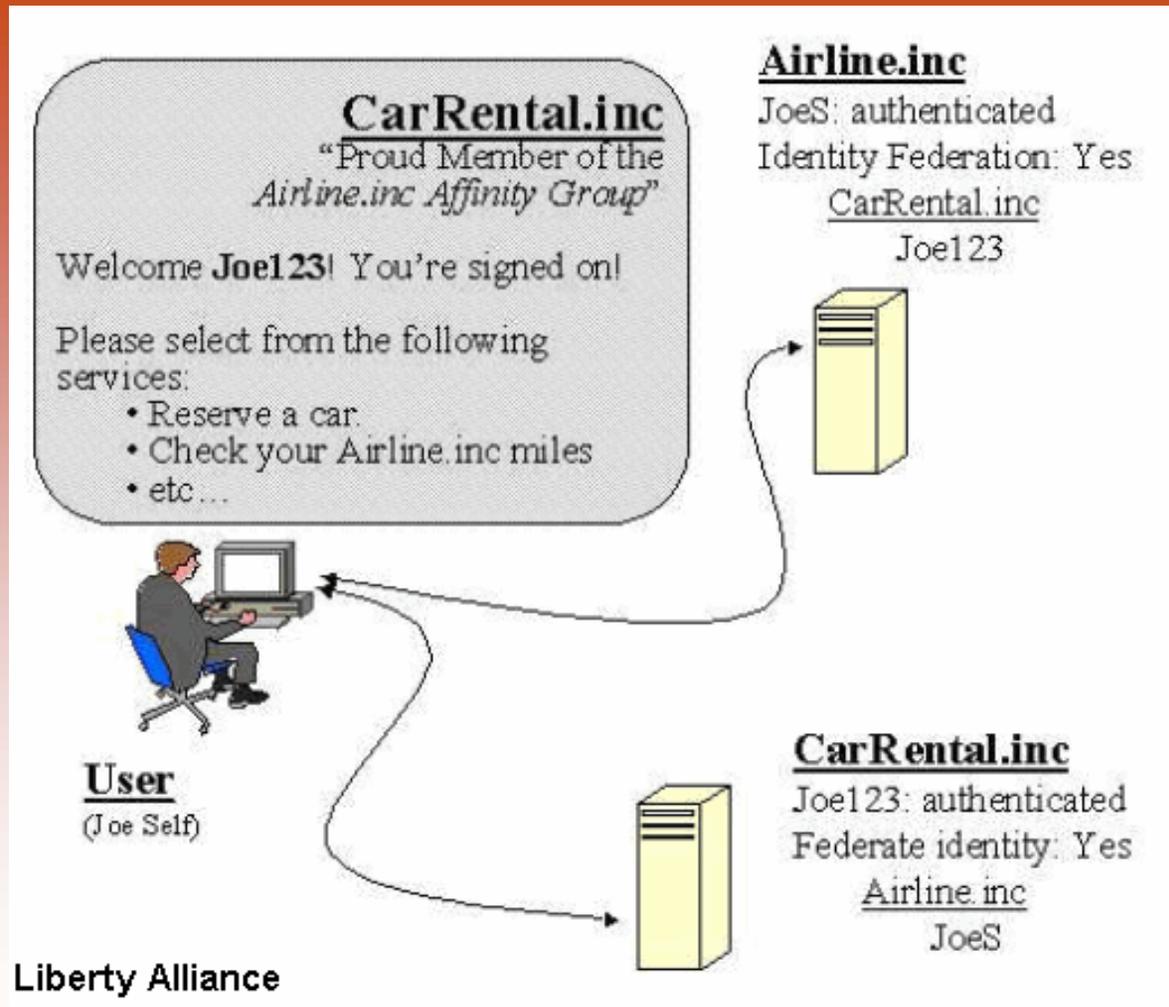
# Example Federation



# Example Federation



# Example Federation



# Entrust Example - SSO

## User Experience



### Step 1: Federate (link) Accounts

Airlines, Inc.

Please Login

Mileage Account #  
4215-2212

Password  
\*\*\*\*\*

Login

Airlines, Inc.

Welcome

Link this account with your car rental account?

Yes No

Rental Car Co.

Please Login

Account #  
624159

Password  
\*\*\*\*\*

Login

Rental Car Co.

Welcome

Link this account with your airline account?

Yup Nope

### Step 2: Single sign-on

Airlines, Inc.

Please Login

Mileage Account #  
4215-2212

Password  
\*\*\*\*\*

Login

Airlines, Inc.

Welcome back Mr. Madsen

Book a flight

Rent a Car

Rental Car Co.

Welcome back Mr. Madsen

Your Status: Gold  
Preferences: Mid-Sized Sedan



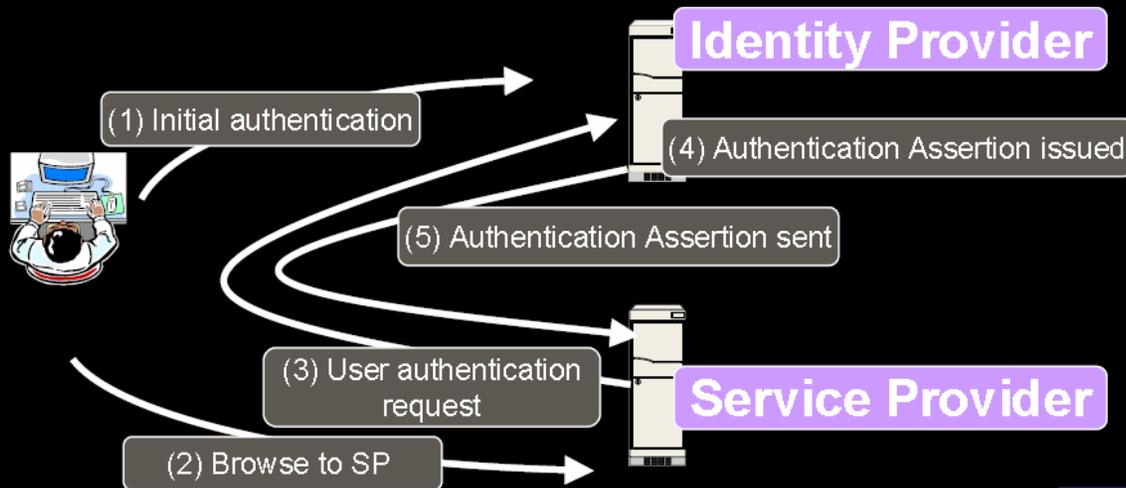
# Entrust Example – SSO Flow



## Liberty SSO Protocol Flow



- ➔ **Instead of the SP directly authenticating the user the SP queries the IdP and the IdP issues an authentication assertion**
- ➔ **SP must 'trust' the IDP**

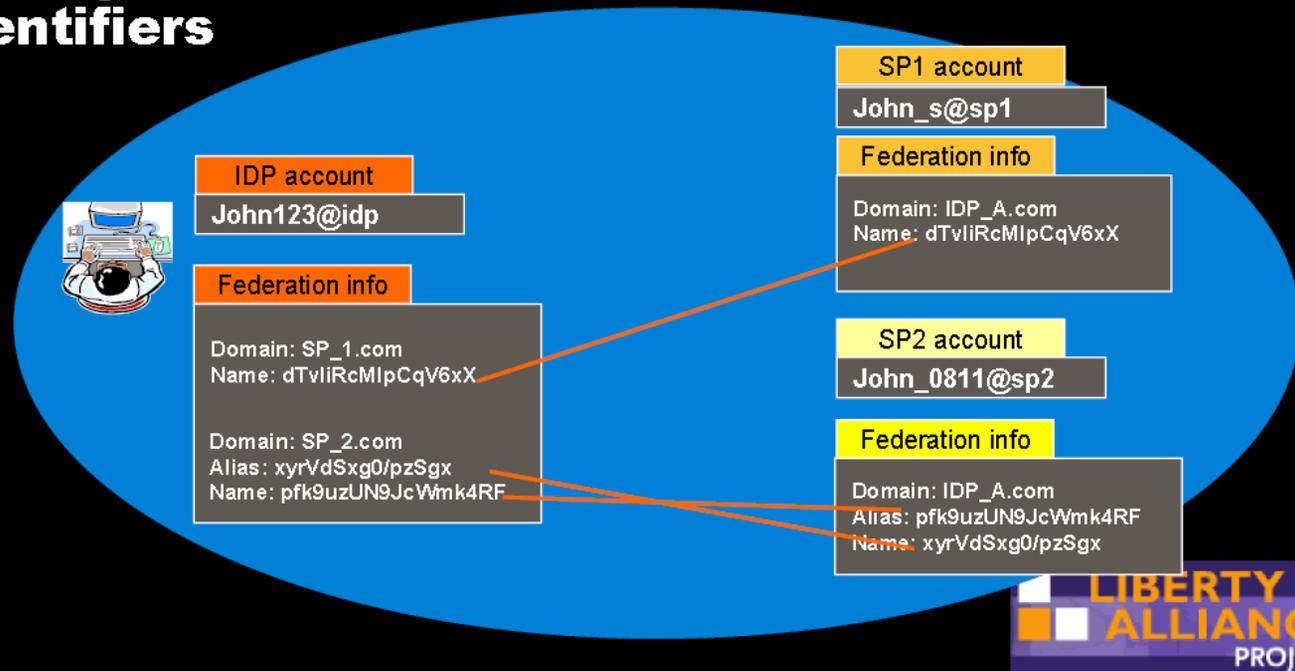


© Copyright 2003 Entrust. All rights reserved.

# Entrust Example - Pseudonyms

## Pseudonyms

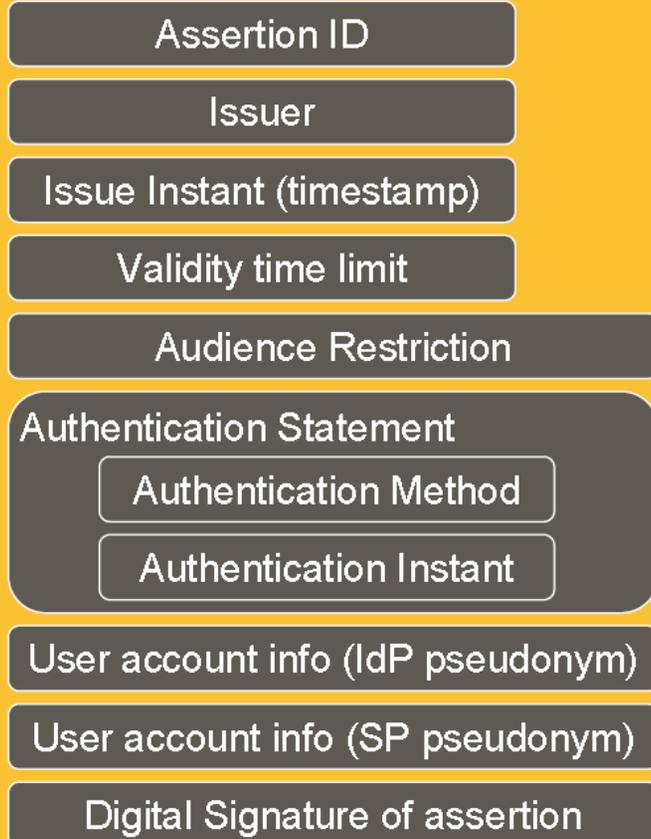
- ➔ SSO requires that sites *talk* about the User
- ➔ Privacy concerns rule out a global identifier
- ➔ Liberty defines mechanism for opaque identifiers



# Entrust Example - Assertion



## Authentication Assertion



# WS-Federation (IBM, Microsoft, BEA, Verisign, RSA Security)

<http://www-128.ibm.com/developerworks/library/specification/ws-fed/>

<http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf>

# WS\* - Identity Standards

- WS-Federation (similar to Liberty ID-FF)
- WS-Trust
  - Secure Token Service
- WS-SecurityPolicy
- WS-SecureConversation
- Token Profiles
  - SAML (1.x)
  - Kerberos Tickets
  - X.509 Certificates
  - Username/Password
  - REL (Rights Expression Language)

# Web Single Sign-On Metadata Exchange Protocol



## Microsoft & Sun

"When a client desires identity-based communication with a service, there is a need to establish a common protocol that is supported by both parties. There are several different models which can be employed — specifically the identity provider can support multiple protocols or the target service can support multiple protocols."

“When an identity provider supports multiple protocols the target service simply uses its preferred protocol suite to communicate with the identity provider and the identity provider responds correctly.”

# Web Single Sign-On Interoperability Profile



## Microsoft & Sun

“Defines an interoperability profile of the web single sign-on metadata exchange protocol that allows using either Liberty Identity Federation or WS-Federation based Identity Providers to interact with a service.”

# Reference Documents

- [Liberty Deployment Guidelines for Policy Decision Makers](#)
- [Liberty Privacy and Security Best Practices](#)
- [SAML v2.0 Executive Overview](#)
- [Liberty ID-FF](#) (technical)
- [Liberty ID-WSF](#) (technical)
- [Liberty ID-SIS](#) (technical)

# Questions



[Lee.Macklin@dts.ca.gov](mailto:Lee.Macklin@dts.ca.gov)

**916-739-7637**