Federated Identity Management, the Real Story

Anthony Nadalin
Chief Security Architect
IBM Corporation
Agenda

- Web Services Overview
  - Security Roadmap
  - Federation Overview
- Federation Drilldown
Secure, Reliable, Transacted Web Services

BPEL4WS

Service Composition

Composable Service Assurances

Description

Messaging

Transports

Security

Reliable Messaging

Transactions

XSD, WSDL, UDDI, Policy, MetadataExchange

XML, SOAP, Addressing

HTTP, HTTPS, SMTP

Importance of Composition

- Everything works in combination
  - Ex: Transaction context works over a reliable connection
  - Ex: Participants use WS-Security to secure transactions (for all types participants)

- Not "reinventing the wheel" for every stack
  - Code reuse, lower costs, faster time to market
  - Ex: all resources named using WS-Addressing

- The overall system is more stable
  - Changes don't percolate up the stack
  - Ex: By using WS-Security, Federation supports all tokens, including future ones
Composable Headers

Addressing

<wsa:ReplyTo>
</wsa:ReplyTo>
<wsa:To>http://fabrikam123.com/Traffic</wsa:To>

Security

<wssec:BinarySecurityToken
  ValueType="wssec:X509v3"
  EncodingType="wssec:Base64Binary">
  dWJzY3JpYmVyLVBlc…..eFw0wMTEwMTAwMD
</wssec:BinarySecurityToken>

Reliability

<wsrm:Identifier>http://fabrikam123.com/seq1234</wsrm:Identifier>
<wsrm:MessageNumber>10</wsrm:MessageNumber>

Traffic

<app:TrafficStatus
  xmlns:app="http://highwaymon.org/payloads">
  <road>520W</road><speed>3MPH</speed>
</app:TrafficStatus>
Federated Identity Administration
Problem

Access to Third-party Users
Access to Third-party Resources

Third-party Users?
Subsidiaries, partner-users, etc.

Third-party Resources?
External Web Sites, Internal Web Sites

CUSTOMERS, EMPLOYEES

APPLICATIONS

IDENTITY & ACCESS MANAGEMENT

PROVISIONING ENDPOINTS

ORGANIZATION

IBM DIRECTORY
Federated Identity

“Federated identity” is defined as collection of federated attributes that can be sourced across multiple federated and authoritative data sources.”

Technology for creating a globally interoperable Online Identity for driving Relationship or Affinity driven Business Models Between companies

To an individual user, it means the ability to associate his various application and system identities with one another.

It refers to the ability of one enterprise to associate with one or more others in a Federation, such that the identities from one enterprise domain (or identity provider) are granted access to the services of another enterprise (or service provider).

Federated Identity Management

Administrative concept that extends identity lifecycle management across identity domains –

Addresses lifecycle management of users across domains
Federation Roles: Identity and Service Provider

“Owns the user relationship”
“Asserting or Vouching” party in the transaction

Identity Provider (IdP)

Mutual TRUST

Service Provider (SP)

Provides Services to trusted users
“Validation or Relying” party in the transaction

1. Issues Network / Login credentials
2. Handles User Administration/ ID Mgmt
3. Authenticates User; “Vouches” for the user’s identity and entitlements in a transaction

1. Relying Party; “WHO is the USER?”
Access to Services are controlled by Service Provider
2. Third-party User is provided access to services for the duration of the federation
User Interaction

Who is the “Identity Provider”?
Who is the “User”?
How can get “identity information” from the User?
WS-Federation

Announced by BEA, IBM, Microsoft, RSA, and VeriSign

- **WS-Federation** (Web Services Federation Language)
  - Enables security realms to federate
  - Enhances policy to enable federation of related services
  - Describes federation messages
  - Describes federated Attribute and Pseudonym service relationships

- **WS-Federation: Passive Requestor Profile**
  - Uses the cross trust realm identity, authentication and authorization federation mechanisms in WS-Federation to support passive requestors, such as Web browsers

- **WS-Federation: Active (Smart) Requestor Profile**
  - Uses the cross trust realm identity, authentication and authorization federation mechanisms in WS-Federation to support active requestors, such as SOAP-enabled applications
Agenda

- Web Services Overview
  - Security Roadmap
  - Federation Overview
- Federation Drilldown
One Protocol, Multiple Bindings

- Common protocol (WS-Trust)
- Two “profiles” of the model are defined
  - Smart/Active clients (SOAP)
  - Passive clients (Browser – HTTP/S)
- Supporting services (attribute/pseudonym/...)

Diagram:
- HTTP messages
- SOAP messages
- HTTP Receiver
- SOAP Receiver
- Security Token Service
Trust Topologies

- Federation approach must address different trust topologies
  - Model existing business practices
  - Leverage existing infrastructure

- Sample topologies
  - Direct trust
    - Exchange
    - Validation
  - Indirect trust
  - Delegation
Direct Trust
Token Exchange

Get identity token

Get access token

Trust

Trust

1

2

3
Direct Trust
Token Validation

1. Get identity token
2. Trust
3. Get access verification
Indirect Trust

C trusts B which vouches for A who vouches for client
Delegation
Single Sign-Out

1. Connection to the server
2. Password verification
3. Logout signal to all servers

Diagram showing the process of Single Sign-Out.
Attribute Service

- Scenario: You ask a weather service for the current weather (or visit a weather site), it provides personalized response because it knows your zip code

- Why it worked:
  - Policy indicated an attribute service
  - Identity information was used to find zip code
  - Weather service was authorized to access zip code

- Specification defines the concept of an attribute service but not a specific interface
Attribute Scoping

Zip: 12309
FN: Fred
ID: 3442
Nick: Freddo
ID: FJ454
Nick: Fredster
ID: 3-55-34
...

Model allows for attributes to be scoped

(fabrikam123.com)
(business456.com)
(example.com)
Attribute Discovery

- Open design model
  - Any attribute store can be used
  - Integration with legacy systems

- Discovery *via* policy
  - Requestor’s policy $\rightarrow$ attribute service
  - Attribute service has its own policy
  - Communication governed this policy

- UDDI is an example store
Attribute Discovery

1. Policy
2. Policy
3. Policy
4. “Get FN”
Attribute Example

1. Trust
2. Trust
3. Zip: 12309
4. FN: Fred

...
Protecting Identity

- Single sign-on also needs to
  - Prevent collusion
  - Provide anonymity

- Other forms of collusion still exist:
  - Address
  - Phone number
  - Credit card
  - Social security number
Pseudonym Service

- This service provides a mechanism for associating alternate identities

- Pseudonyms represent alternate identities
  - Scoped by a domain expression
  - Subject to authorization control
  - Can be accessed by authorized services
  - Can be integrated with IP/STS
Pseudonym Discovery
Pseudonym Example 1

"Fred" → "A123"

Service sets pseudonym for its domain
Pseudonym Example 2

“Fred” → “B456”

Service fetches pseudonym for its domain

“B456” — “Freddo”

“B456” — “Fred”
Pseudonym/STS Integration

- Pseudonym & STS can work together
- Single physical service
- Separate but tightly coupled services
- Scope of request selects pseudonym
Pseudonym Example 3

Use pseudonyms to obtain initial token

“Fred” → “Freddo”
Federation Discovery Recap
Active (Smart Client) Profile

- Describes options with SOAP clients
- Allows rich caching
- Varied models based on policy
  - Business needs
  - Inter-organization
  - Regulations
- Strong authentication of all requests
Example Flow (SOAP)

Requesting Service | Requestor’s IP/STS | Target Service | Target’s IP/STS

Acquire policy

Request token

Return token

Request token

Return token

Send secured request

Return secured response
Passive Profile

- Describes options with browsers
  - Pure redirect with GET
  - URL-only
  - POST body
- Uses redirection to effect messages
- Tunnels WS-Trust messages
  - Implicitly
  - Explicitly
- Allows custom caching mechanisms
Example Flow (Browser)

Requesting Browser

Requestor’s IP/STS

Get resource

Redirect to resource’s IP/STS

Detect realm

Redirect to requestor’s IP/STS

Login

Return identity token

Return resource token

Return secured response

Target Resource

Target’s IP/STS
Federating Security

Summary

- Generic token acquisition
  - Enables different trust topologies
- Integrates with existing infrastructures
  - Business model
  - Token formats
  - Attribute stores
  - Directory services
Federating Security

Summary

- Identity Protection and Privacy
  - Varying levels supported
  - Allows true anonymity
  - Supports multiple privacy languages
  - Rich privacy options
- End-to-end, no HTTPS required
- Public review and participation
- Free to implement
Federating Security
Summary

- Together with the other WS-* specifications, provides a rich fabric for building secure, reliable, transacted systems across federation boundaries.
- SOAP composability model allows layering of vertical and value-add applications and protocols.
The Client’s Problem

- Multiple Logins, PW rules, etc
- Disjoint user experience, no crossover incentive
- Costly user administration at every Service Provider
Scenario
The Solution – Federated Identity Management

- Reduced ID Management costs
- User satisfaction creates ‘stickiness’
- Fast service provider adoption
- Passwords, passwords, passwords

- Single Sign On
- Authenticate
- SBC FreedomPass

- Service Provider
- Trust
- WS-Federation
- SAML
- Liberty

- MySBC

- Service Provider
- Trust
- Federal Do-No-Call Registry
Scenario 1: Sign On to Freedom Pass Portal

- Starting from welcome page on the Freedom Pass site
- Log into Identity Provider (IdP) as edward
- Arrive at Freedom Pass portal
Freedom Pass Intro page
Freedom Pass login
Portal Site

![Portal Site Image](image-url)

- **FreedomPass**: A portal site with options for personal information, address book, and notices.
- **Personal Information (Profile)**: View or change general information about yourself, such as your name, mailing address, email, contact preferences, etc.
- **Address Book**: For your personal contacts, manage your addresses, phone numbers, etc.
- **Notices (2 New)**: The SRC's portal will be down for maintenance from 1pm on Friday, Jan 2, 2004. Remember to have a conference call at 2pm CT on Wednesday, Jan 1, 2004. Update to SRC Totally Unified Index and save up to $5 per month.
Scenario 2: Federate Liberty
User and SSO

- Start from Edward’s Freedom Pass portal page
- Click on MySBC under the “Services Available to Link” menu to initiate account federation
- Confirm federation to partner by clicking Continue
- Log into SP as eddie
- Arrive at Federation Success page
- Click on MySBC button
- Arrive at MySBC page
- Click Local Logout
- Return to Freedom Pass
- Click on MySBC to SSO to SP
- Single-sign out using the Freedom Pass logout link.
Initiate Account Federation to Partner
Confirm Federation to Partner

You have chosen to link your MySBC account with your Freedom Pass account.

Continue

or

Return to MySBC

© 2004 SBC Knowledge Ventures, L.P. All rights reserved. Privacy Policy
User Logs into Service Provider

You are required to provide your MYSBC User ID and Password to initialize Federation.

User ID: eddy
Password: ********

[Log in button]
Federation Success Page

![Federation Success Screen](image_url)
Arrive at MySBC
Local Logout

User Eddie has logged out.

Return to MySBC

Return to Freddies Pass
Return to FreedomPass
SSO to MySBC

![SSO to MySBC](image-url)
FreedomPass Logout