

# Liberty ID-WSF Overview

Conor P. Cahill  
Chief Architect  
America Online, Inc.

# Agenda

- Goals
- What is an Identity Based Web Service
- Liberty's ID-WSF Specifications
- AOL's Deployment

# Goals

- Generate Interest in ID-WSF
- Introduction to Liberty specifications

# Agenda

- Goals
- **What is an Identity Based Web Service**
- Liberty's ID-WSF Specifications
- AOL's Deployment

# Web Service Classes

- Identity Based
- Identity Consuming
- Non-Identity

# Identity Based Web Service

- Located through an identity
- Invoked in the context of that Identity
- Examples
  - Conor's Calendar Service
  - Eve's Profile Service

# Identity Consuming Interface

- Not located through Identity
- Server to Server Invocation Context
- Invoked with an Identity in the application layer
- Example
  - Promotion Service
    - AOL Radio Service invokes AOL Promotion Service
    - Identity used by PS to determine eligibility for promotions

# Non-Identity Services

- You're typical run-of the mill Web Service
- Not located or invoked with an Identity

# Service Interfaces mixed

- Alert service
  - Registration Interfaces are typically identity based
  - Invocation Interfaces (deliver an alert) are typically server to server
- Profile Service
  - Basic Interface is Identity based
  - Search Interface (for customer care) not identity based

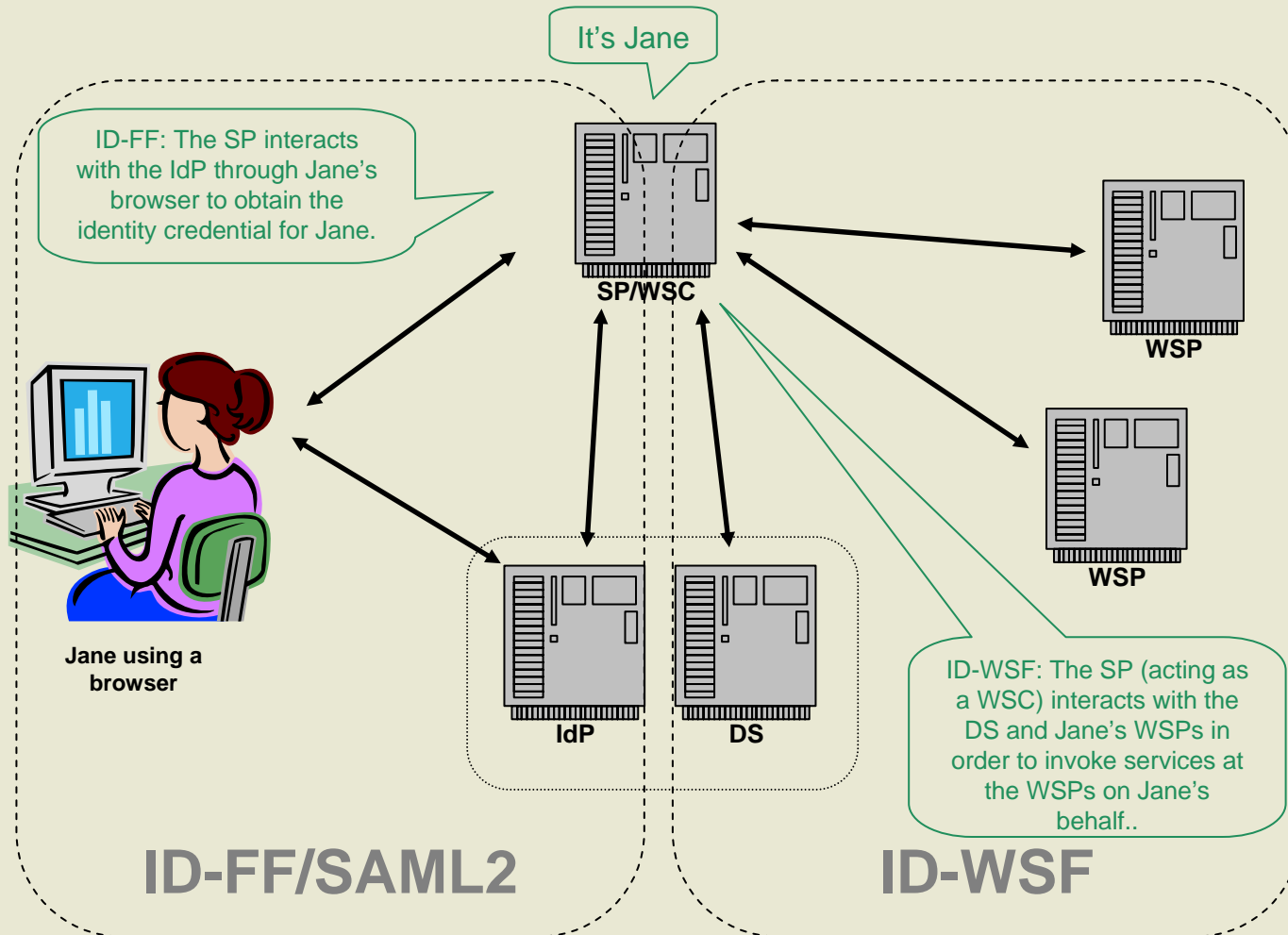
# Agenda

- Goals
- What is an Identity Based Web Service
- **Liberty's ID-WSF Specifications**
- AOL's Deployment

# What is ID-WSF?

- Framework for locating and invoking identity based web services
- Supports all types of Web Services
- Permissions-based Attribute Sharing
  - Invoking Services under control of user
    - At the DS **and** at the WSP

# Liberty ID-FF & ID-WSF



# ID-WSF 1.0 Core Components

- **Foundation Services**
  - Authentication Service
  - Discovery Service
  - Interaction Service
- **SOAP Binding Specification**
- **Data Services Template**

# ID-WSF 2.0 Major Enhancements

- Adoption of WS-Addressing
- Subscription/Notification Subsystem
- People Service
- Invocation Context extension

## ID-WSF 2.0: Adoption of WS-Addressing

- W3C Standard in progress (CR status)
- Adds Asynchronous Messaging support
- Multi-path messaging
  - Responses can be directed to an address
  - Useful in server-to-server messaging with clusters

# ID-WSF 2.0: Subscription/Notification

- Template for service based subscriptions
- Usable by all services
- Notification when data changed
- Supports Notifications with:
  - Data changed flag (recipient has to go get data)
  - Changed data
- Not built off of WS-Eventing nor WS-Notification (yet)

# ID-WSF 2.0: People Service

- Identity Federation between \*individuals\*
  - Conor establishes a connection with Paul
- Supports Invocation of another user's service
  - Conor can access Paul's Calendar (w/Permission, of course)
- Group (Collection) management
- Invitation model for cross-IDP federations

# ID-WSF 2.0: Invocation Context

- Extended Invocation Context to include:
  - Invocation Identity
    - Who is submitting the request
  - Target Identity
    - Who's resource is targeted in the request
  - Sender
    - Server sending the request
  - Destination
    - Server receiving the request

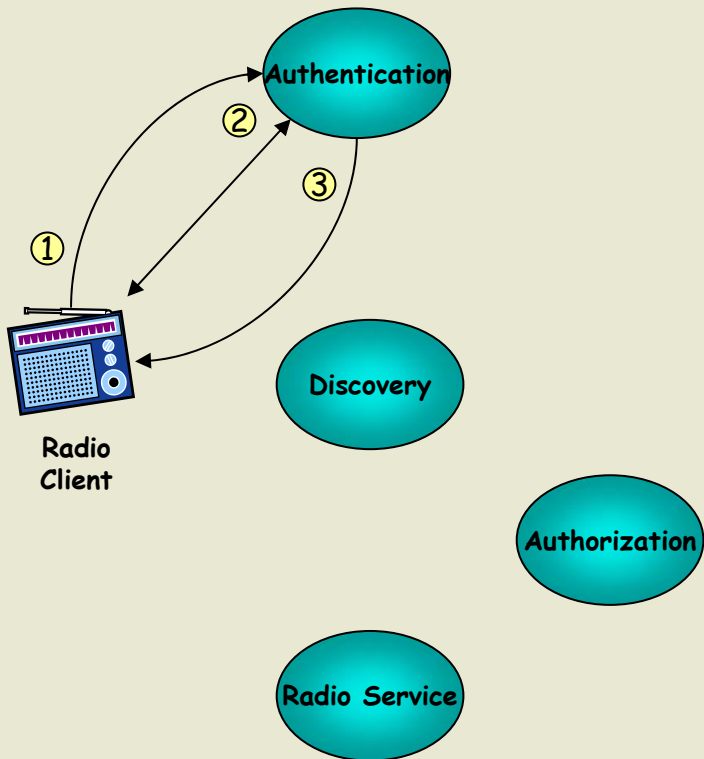
# Sample ID-WSF Invocation Session



Radio Client

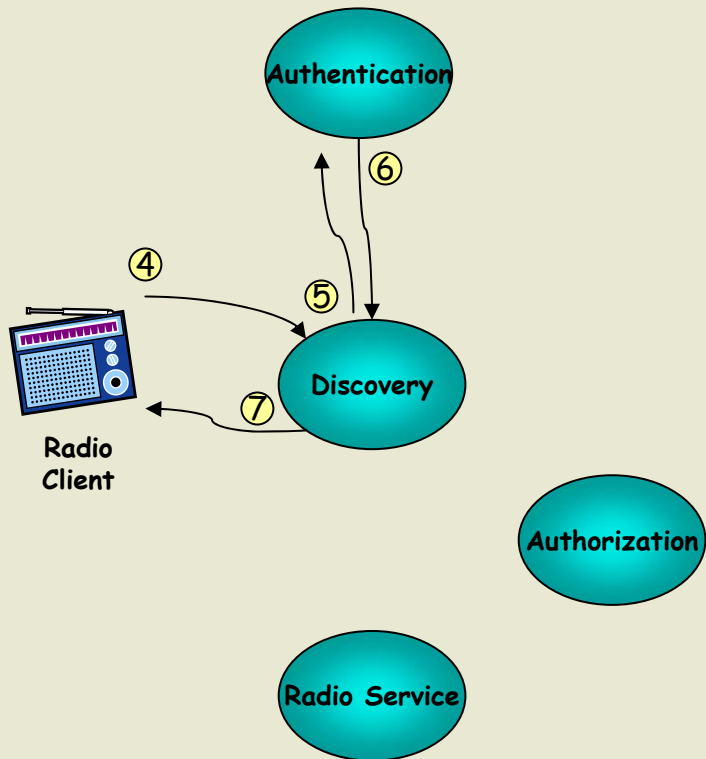


# Radio Application: Authentication



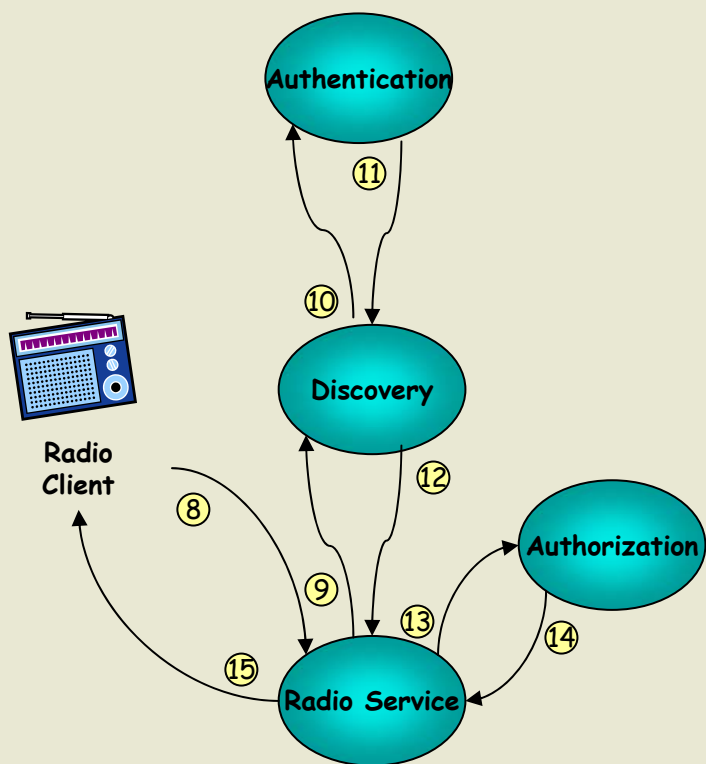
1. Radio Client (RC) contacts the Authentication service (AS) to authenticate the user Jim
2. The RC and AS exchange a series of messages to authenticate the user depending upon the authentication algorithm being used (e.g. PLAIN, CRAM-MD5)
3. The AS validates the credential, locates the user's identity at the AS (LUID 123) and generates a security token (T1) for the session and provides the client with both the token and information on how to get to the Discovery Service (DS). The security token includes:
  - User: Identity at AS (LUID 123)
  - Issuer: AS
  - Issued for: AS
  - Issued to: (null)

# Radio Application: Discovery



4. The RC submits a discovery request for the Radio Service (RS) to the DS, including the security token (T1) obtained from the AS.
5. The DS looks up the user's RS and submits a request to the AS for a security token that the client can use to invoke the RS, including the security token (T1) provided by RC.
6. The AS looks up the LUID for the user at the RS and generates a security token for the RS and returns it to the DS. The security token includes:
  - User: Identity of user at RS
  - Issuer: AS
  - Issued for: RS
  - Issued to: (null)
7. The DS returns the token (T2) plus the information needed for the RC to access the RS.

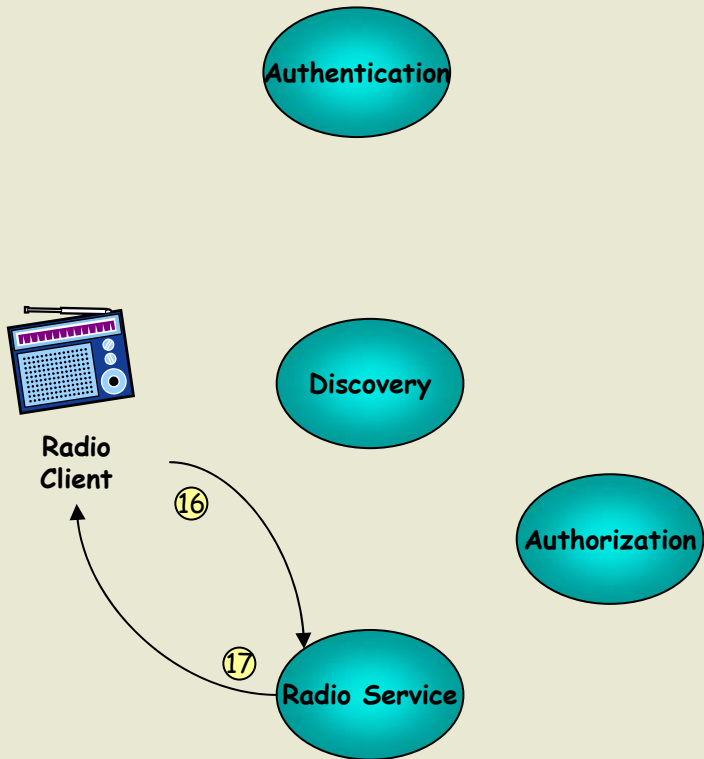
# Radio Application: Service Invocation



8. The RC submits a radio service call to the RS including the security token (T2) obtained from the DS.
9. The RS, sends a discovery request to the DS for the Authorization Service (AZS), including the security token (T2) it received from the RC.
10. The DS looks up the user's AZS and submits a request to the AS for a security token that the client can use to invoke the RS, including the security token (T2) provided by RS.
11. The AS looks up the user's LUID at the AZS and generates a security token (T3) for the AZS and returns it to the DS. The security token includes:
  - User: Identity at AZS (LUID: 789)
  - Issuer: AS
  - Issued for: AZS
  - Issued to: RS
12. The DS returns the token (T3) plus the information needed for the RS to access the AZS.
13. The RS invokes the AZS using the information and security token (T3) returned by the DS.
14. The AZS returns authorization book (AB) to the RS
15. The RS processes AB, figures out appropriate response for RC and returns appropriate results for query as well as a replacement security token (T4) to be used on subsequent calls



# Radio Application: Subsequent Invocation

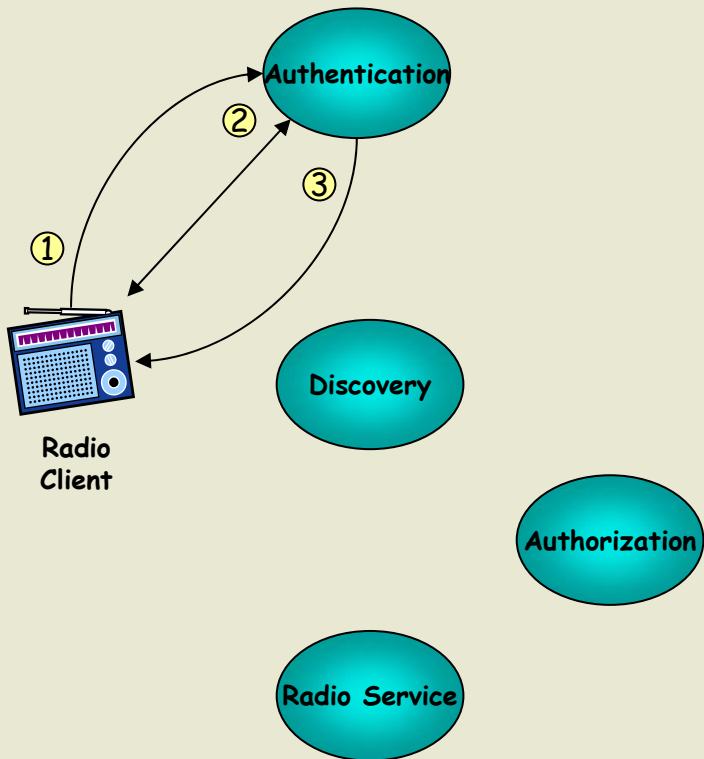


16. The RC submits another radio service call to the RS including the replacement security token (T4) obtained from the RS.
17. The RS sees that it already has current authorization information, processes the request and sends a response back to the RC.



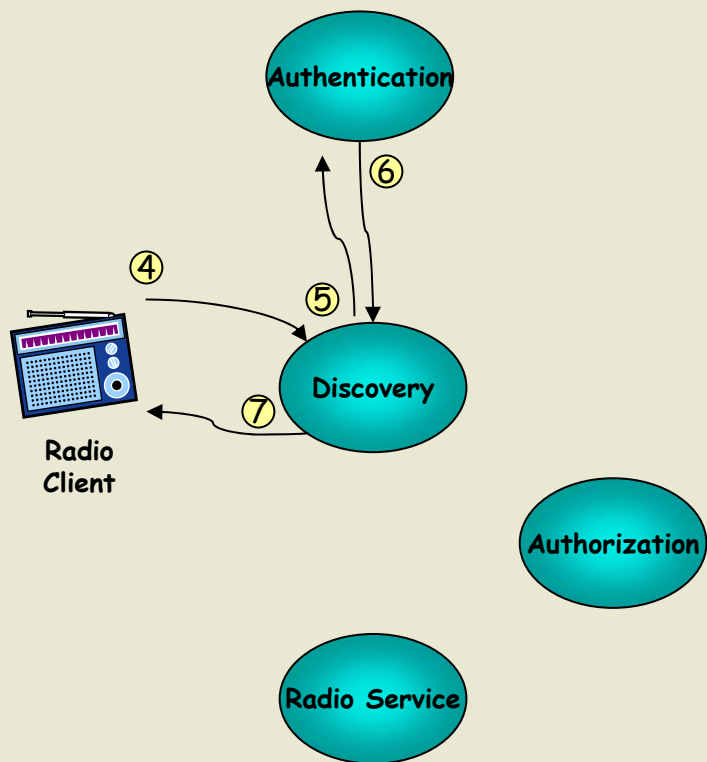
# Radio Application: The next day

# Radio Application: Authentication (same as before)



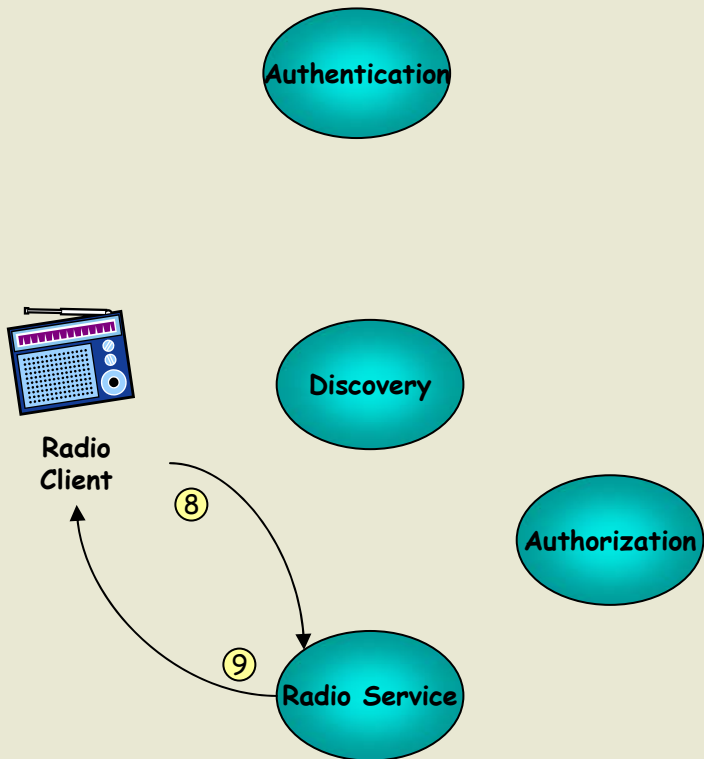
1. Radio Client (RC) contacts the Authentication service (AS) to authenticate the user Jim
2. The RC and AS exchange a series of messages to authenticate the user depending upon the authentication algorithm being used (e.g. PLAIN, CRAM-MD5)
3. The AS validates the credential, locates the user's identity at the AS (LUID 123) and generates a security token (T1) for the session and provides the client with both the token and information on how to get to the Discovery Service (DS). The security token includes:
  - User: Identity at AS (LUID 123)
  - Issuer: AS
  - Issued for: AS
  - Issued to: (null)

# Radio Application: Discovery (same as before)



4. The RC submits a discovery request for the Radio Service (RS) to the DS, including the security token (T1) obtained from the AS.
5. The DS looks up the user's RS and submits a request to the AS for a security token that the client can use to invoke the RS, including the security token (T1) provided by RC.
6. The AS looks up the LUID for the user at the RS and generates a security token for the RS and returns it to the DS. The security token includes:
  - User: Identity of user at RS
  - Issuer: AS
  - Issued for: RS
  - Issued to: (null)
7. The DS returns the token (T2) plus the information needed for the RC to access the RS.

# Radio Application: Service Invocation



8. The RC submits another radio service call to the RS including the replacement security token (T4) obtained from the RS.
9. The RS sees that it has current authorization information (still valid from yesterday), processes the request and sends a response back to the RC.

# Agenda

- Goals
- What is an Identity Based Web Service
- Liberty's ID-WSF Specifications
- **AOL's Deployment**

# AOL's ID-WSF Implementation (part 1)

- ID-WSF 1.0 based services
  - Authentication Service
  - Discovery Service
  - Radio & Photo Services
- Intelligent clients on connected devices
  - Direct WSCs
  - Client only configured with address of IdP (authentication svc)
- Demonstrations:
  - 3GSM World Congress, Feb 2004
  - Consumer Electronics Show, Jan 2004, Jan 2005
- In Production June 2004
  - D-Link DMS 320 and 320RD
  - Netgear MP101
  - Dell Media Experience
  - AOL Radio Client for MAC
  - Devices from several other manufacturers soon

# AOL's ID-WSF Implementation (part 2)

- AOL Platform Services
  - Approx 90 different services
    - Foundation
      - Authentication/Discovery
    - Infrastructure
      - Storage, Authorization, Subscription, Payment, etc.
    - Application
      - Presence, Contact Book, Calendar, Mail, etc.
  - Built on top of ID-WSF 2.0
    - First foundation components in progress at this time
    - Internal Pilot by end of 2005