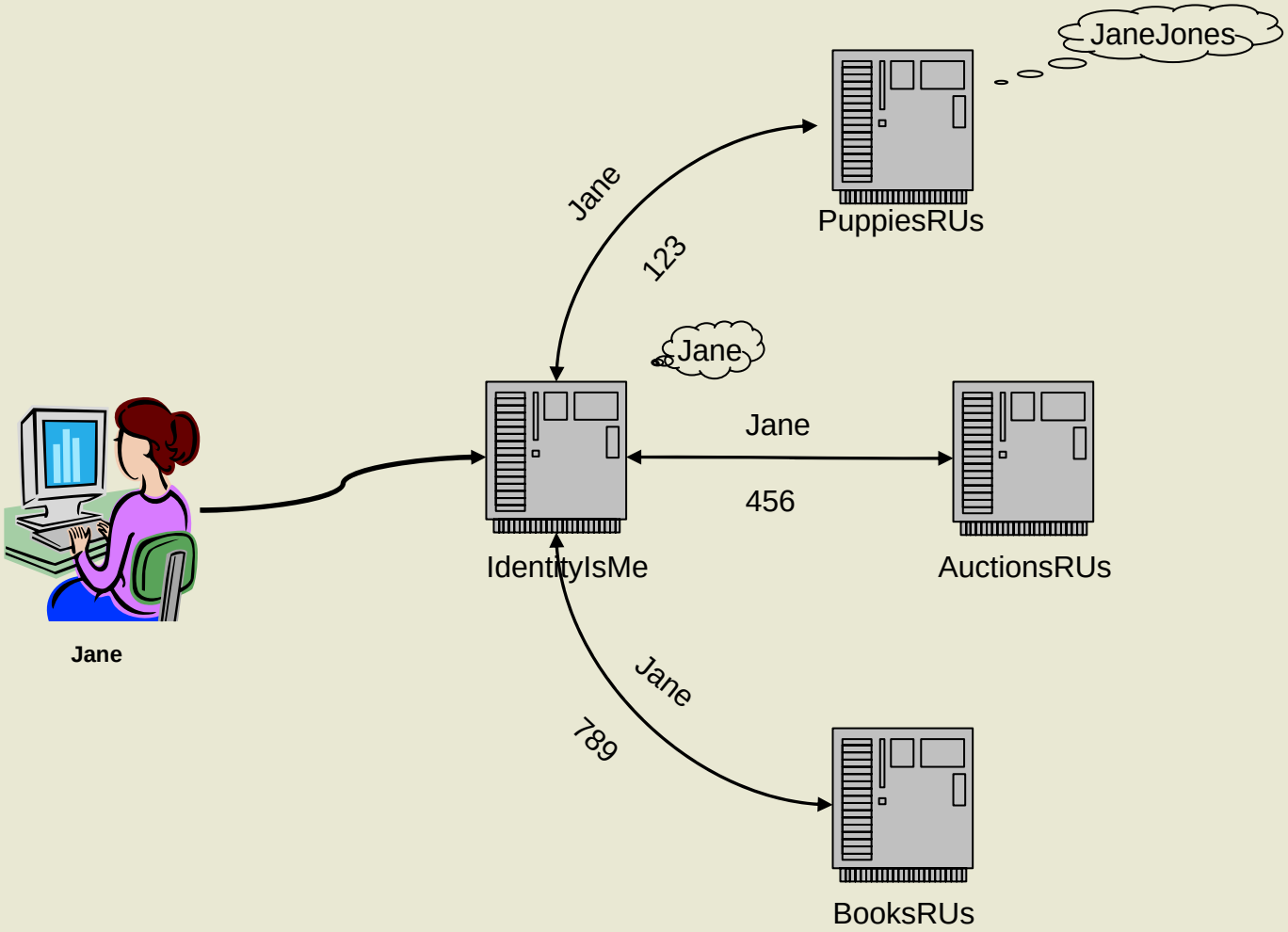
Liberty Technology Overview

Conor P. Cahill
Chief Architect
America Online, Inc.

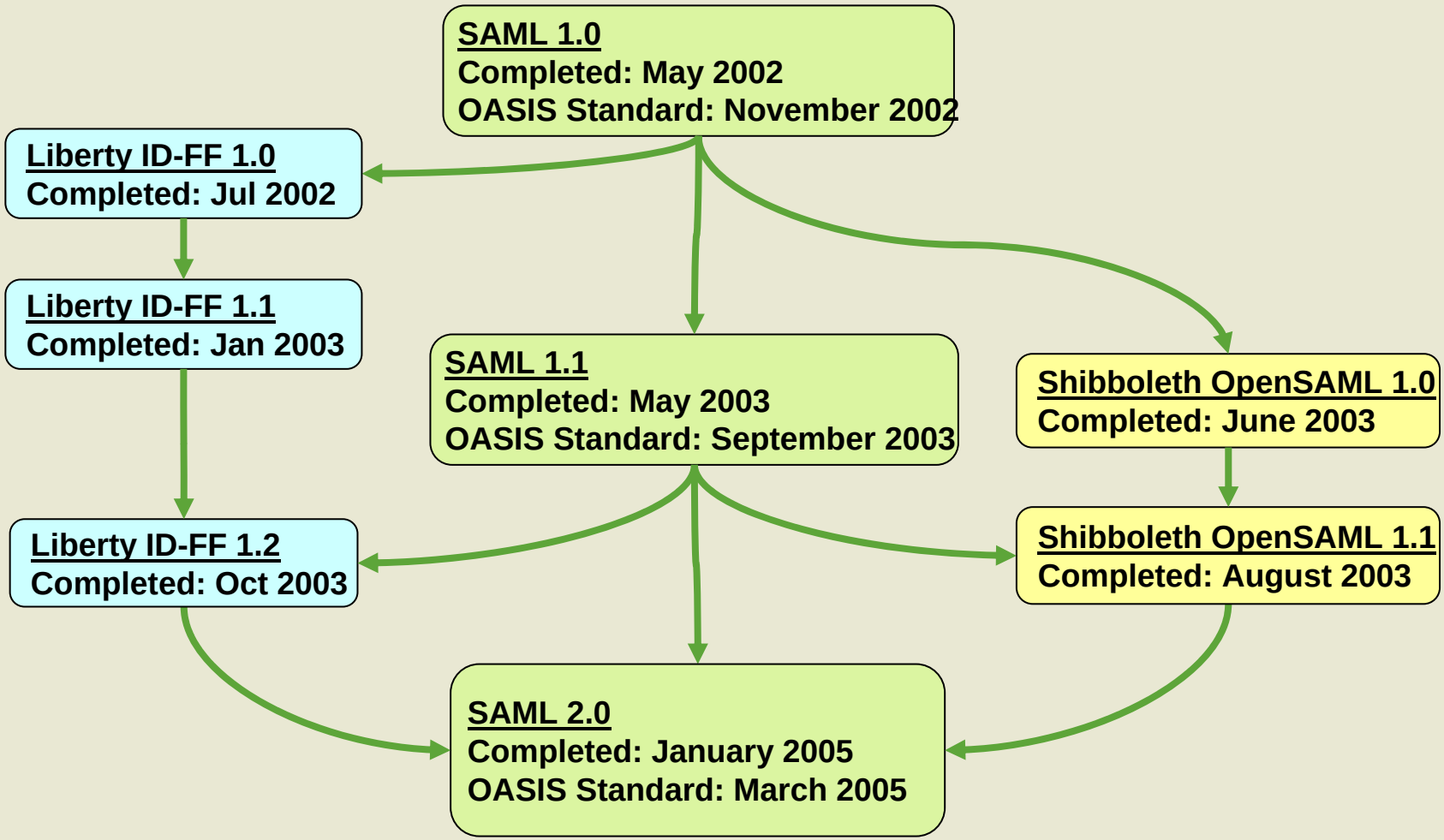
Agenda

- Identity Federation (ID-FF)
- Identity based Web Services (ID-WSF)
- AOL’s Deployment

What is Identity Federation?



Identity Federation Timeline



ID-FF & SAML 2.0

- Single Sign On
  - Browser & ECP Profile
  - Authentication Context
  - IDP Discovery
  - Active & Passive
  - Pseudonymity
- Single Log Out
- Federation
  - Establishment
  - Management
- Metadata

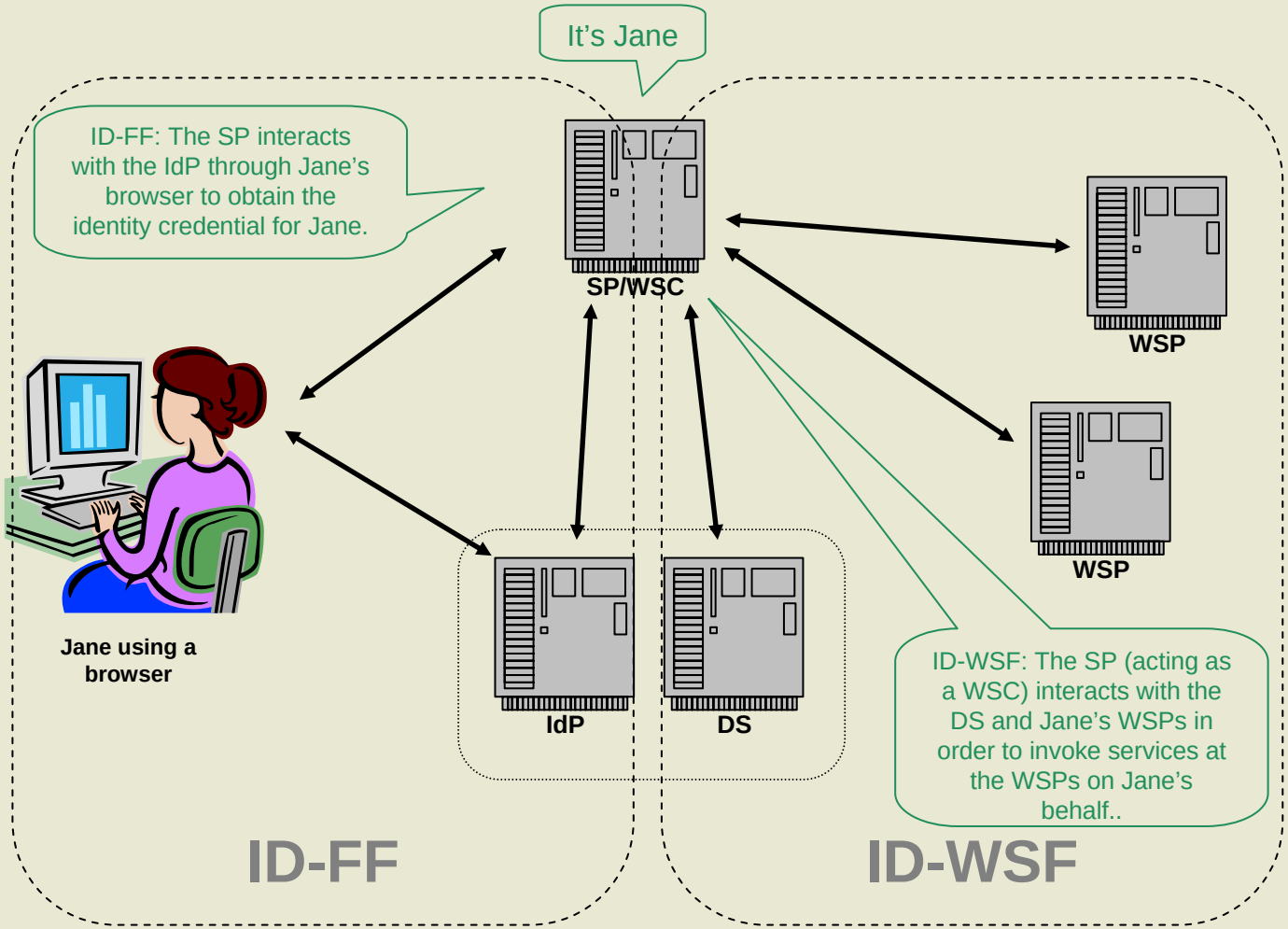
Agenda

- Identity Federation (ID-FF)
- **Identity based Web Services (ID-WSF)**
- AOL's Deployment

What is ID-WSF?

- Framework for locating and invoking identity based web services
- Identity web services:
  - Associated with a Principal's Identity
    - E.g. Conor's calendar
  - Can be Invoked using a Principal's Identity
- Permissions-based Attribute Sharing
  - Invoking Services under control of user
    - At the DS **and** at the WSP

Liberty ID-FF & ID-WSF



LIBERTY ALLIANCE PROJECT

ID-WSF Core Components

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

ID-WSF Futures

- Key technologies
  - Asynchronous messaging
  - Multi-path messaging
  - Principal Relationships and Groups
  - Intelligent Client/Trusted Module

Sample ID-WSF Invocation Session

Radio Client

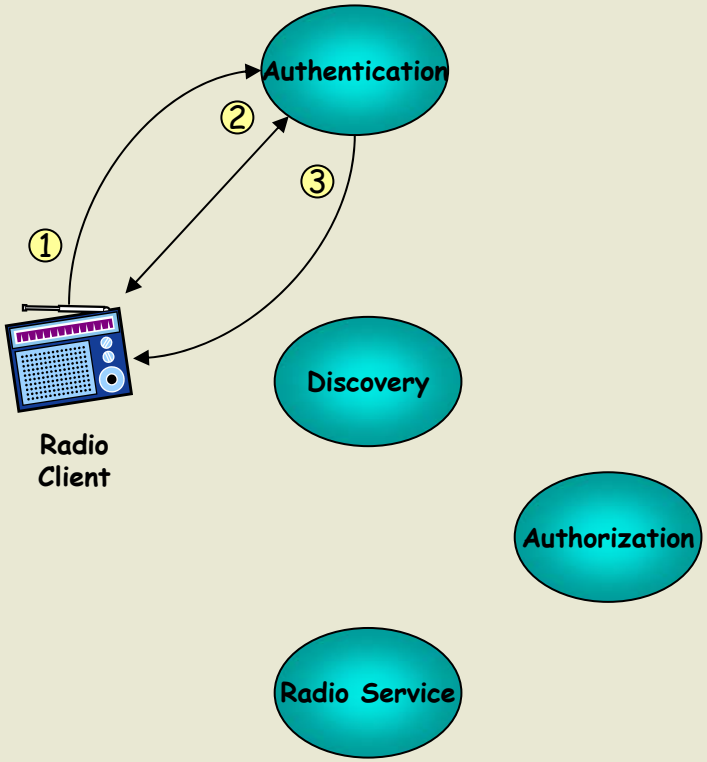
Authentication

Discovery

Authorization

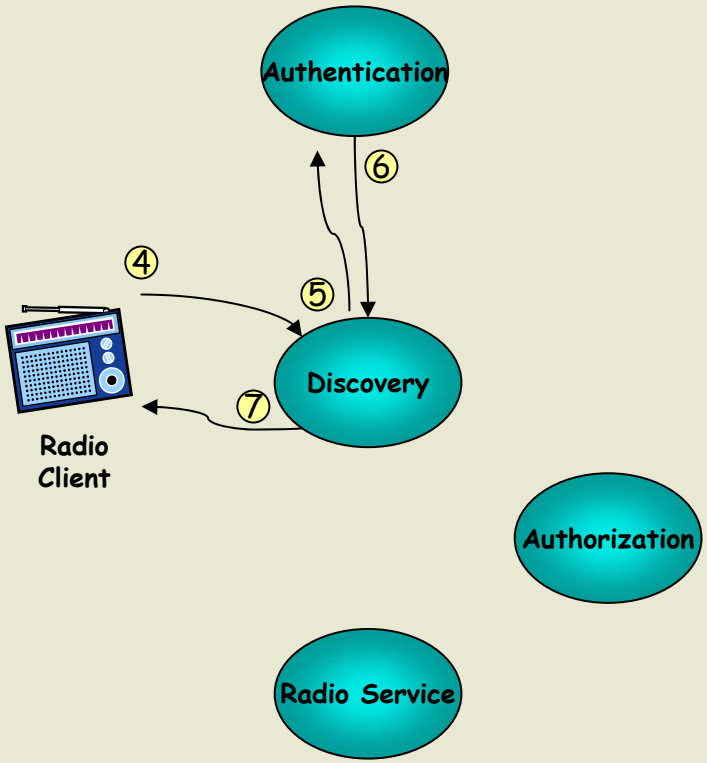
Radio Service

Radio Application: Authentication



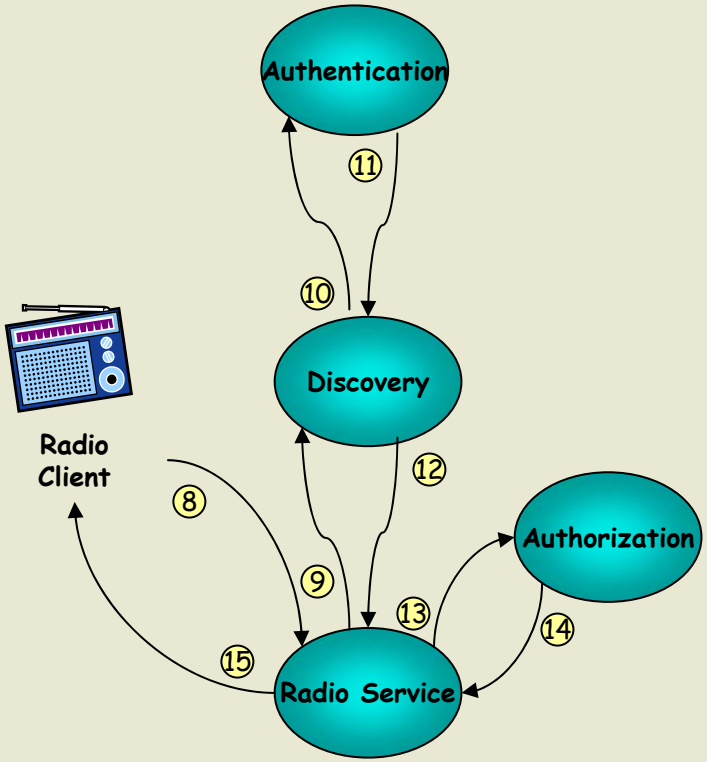
1. Radio Client (RC) contacts the Authentication service (AS) to authenticate the user Jim
2. The RC and AS exchange a series of messages to authenticate the user depending upon the authentication algorithm being used (e.g. PLAIN, CRAM-MD5)
3. The AS validates the credential, locates the user's identity 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



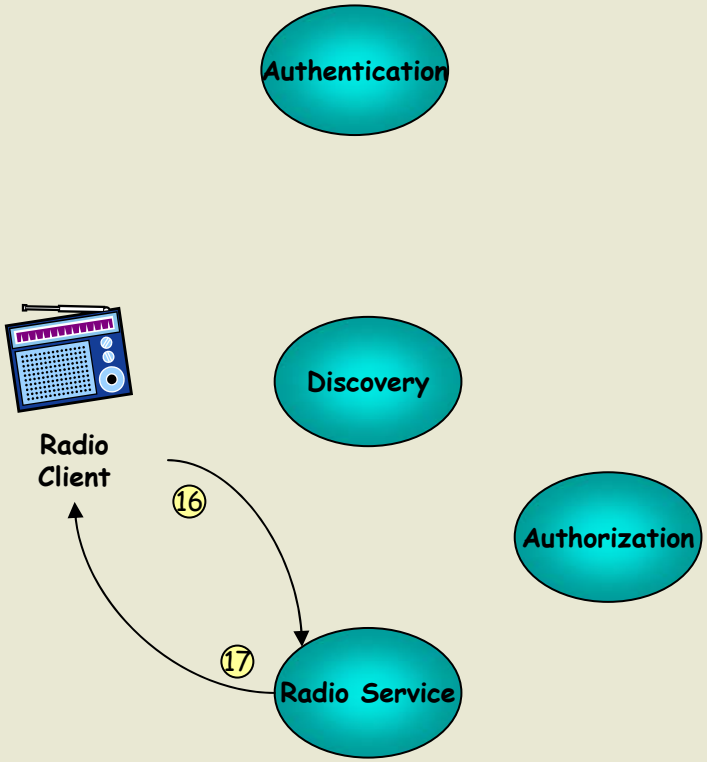
4. The RC submits a discovery request for the Radio Service (RS) to the DS, including the security token (T1) obtained from the AS.
5. The DS looks up the user's RS and submits a request to the AS for a security token that the client can use to invoke the RS, including the security token (T1) provided 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

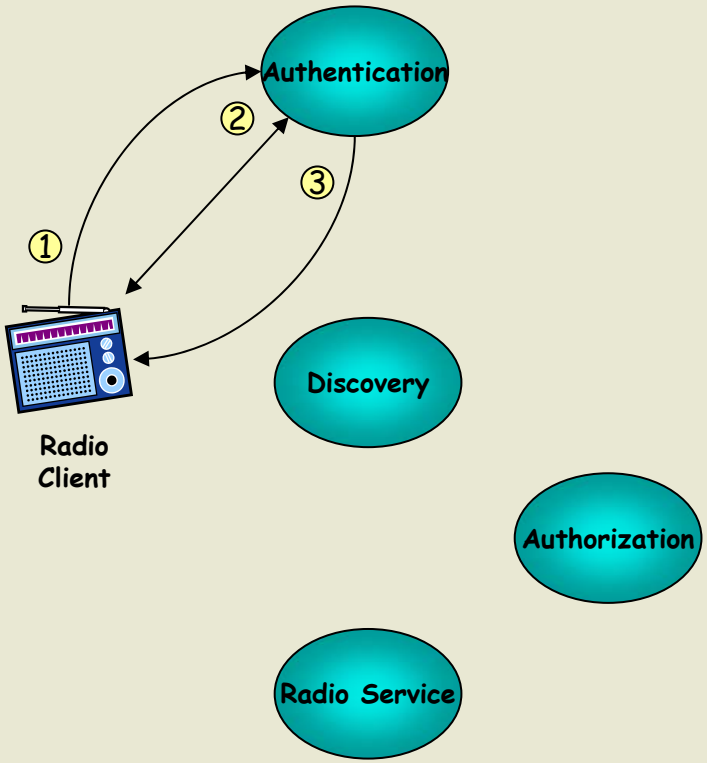


16. The RC submits another radio service call to the RS including the replacement security token (T4) obtained from the RS.
17. The RS sees that it already has current authorization information, processes the request and sends a response back to the RC.

LIBERTY ALLIANCE PROJECT

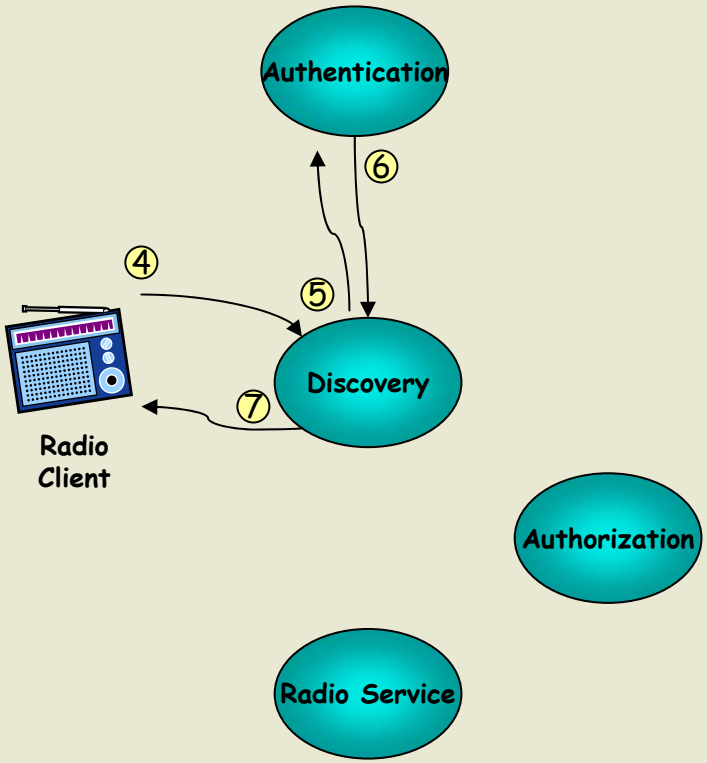
Radio Application: The next day

Radio Application: Authentication (same as before)



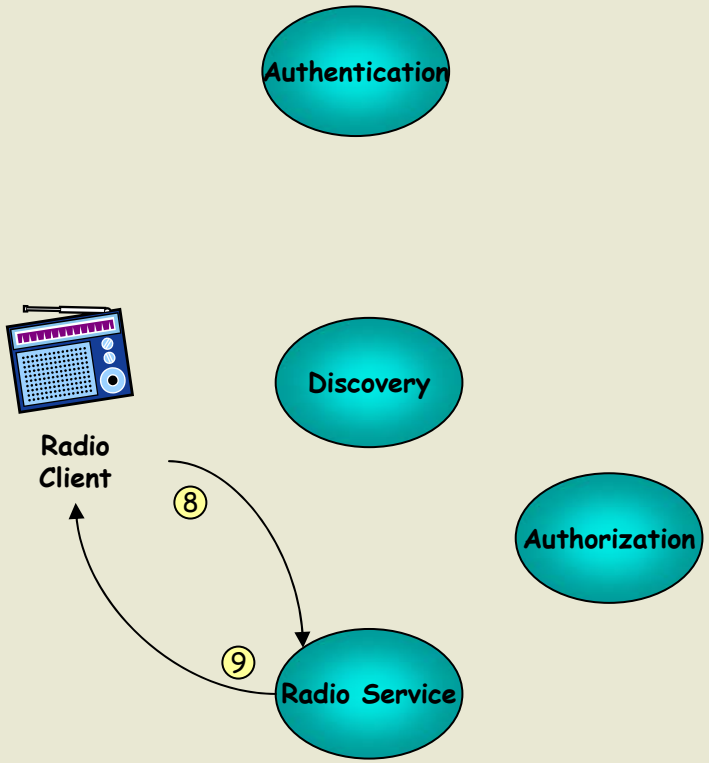
1. Radio Client (RC) contacts the Authentication service (AS) to authenticate the user Jim
2. The RC and AS exchange a series of messages to authenticate the user depending upon the authentication algorithm being used (e.g. PLAIN, CRAM-MD5)
3. The AS validates the credential, locates the user's identity 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.

AOL's ID-WSF Implementation (part 1)

- ID-WSF 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 (soon)
  - 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
    - First foundation components in progress at this time