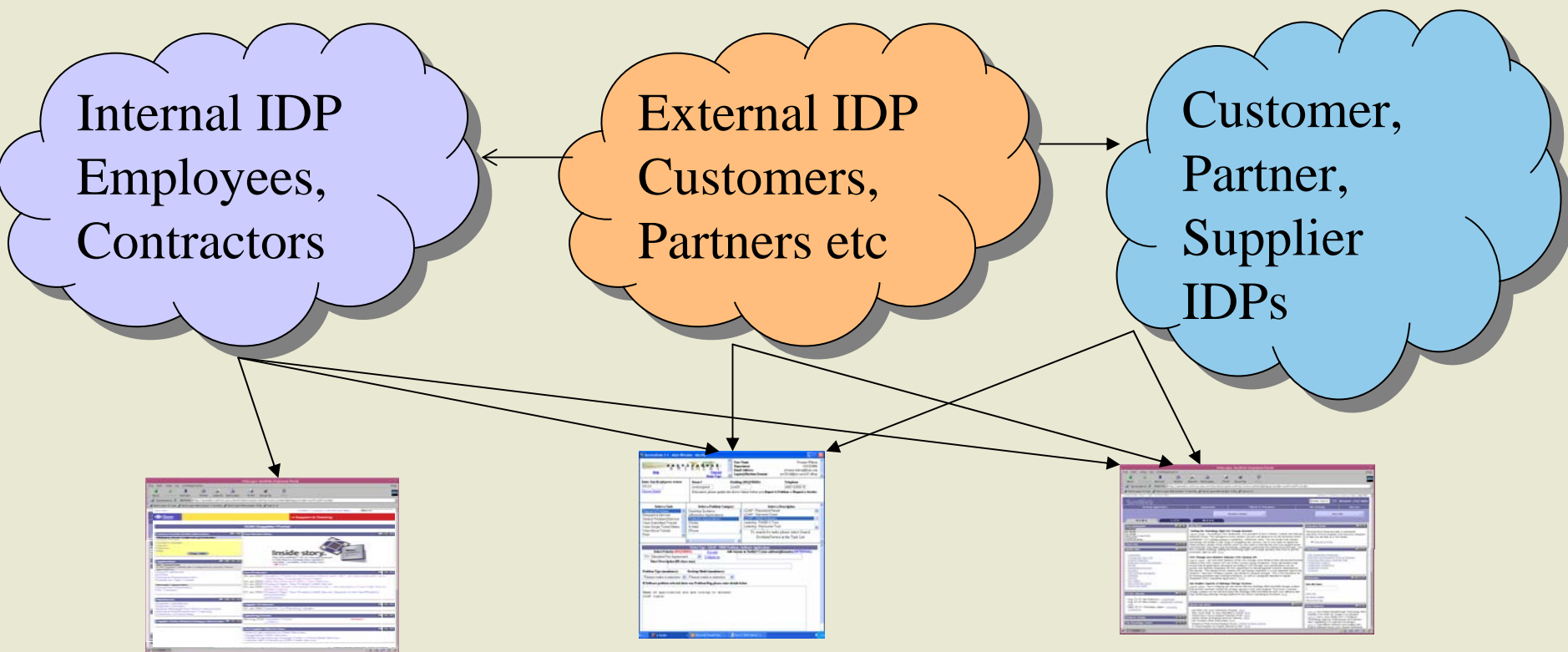


# Liberty in the Enterprise

Use of Liberty at Sun Microsystems, Inc. to  
Support Outsourcing

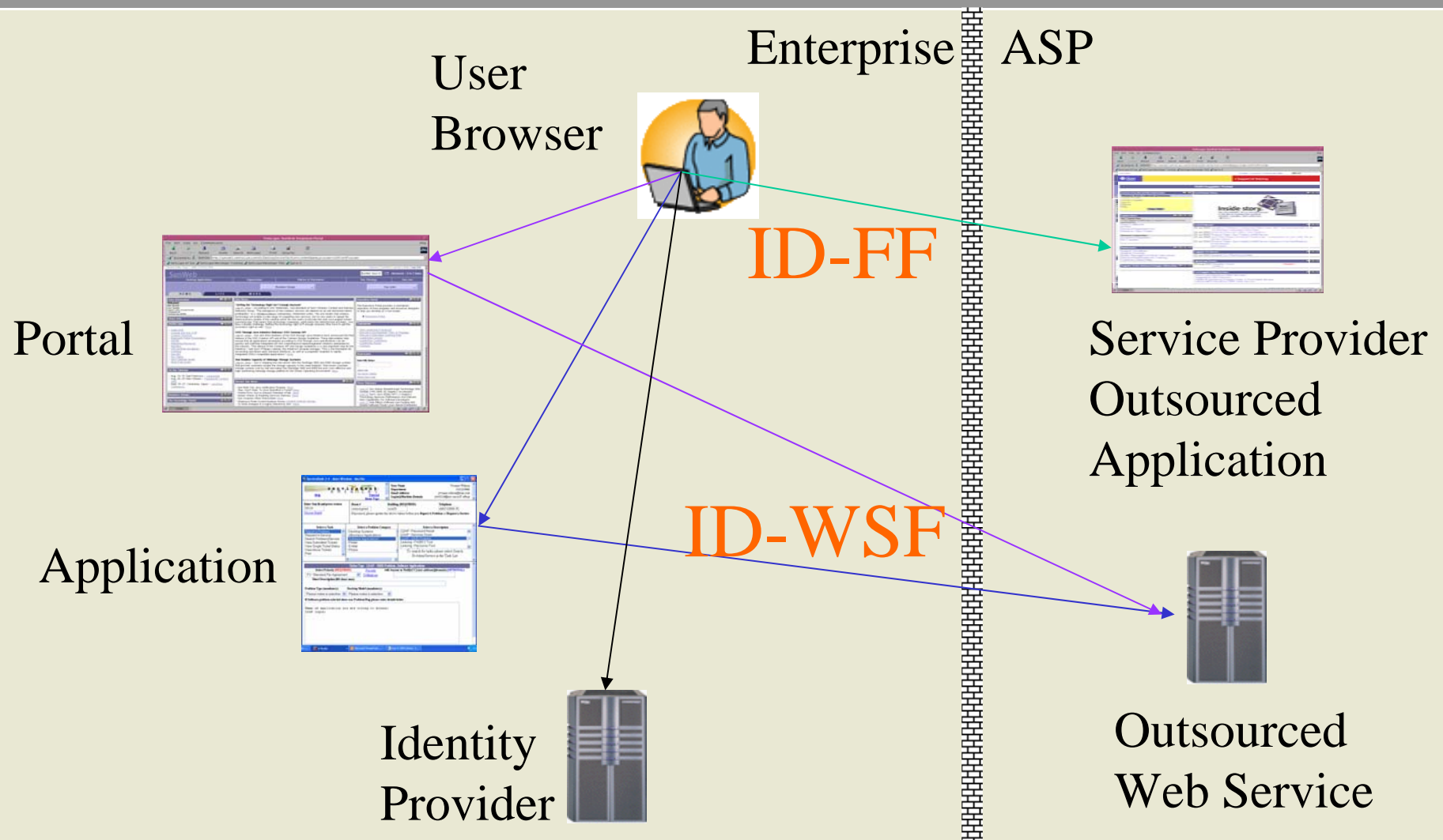
Yvonne Wilson, Sun IT Architect

# Liberty Bridging Communities

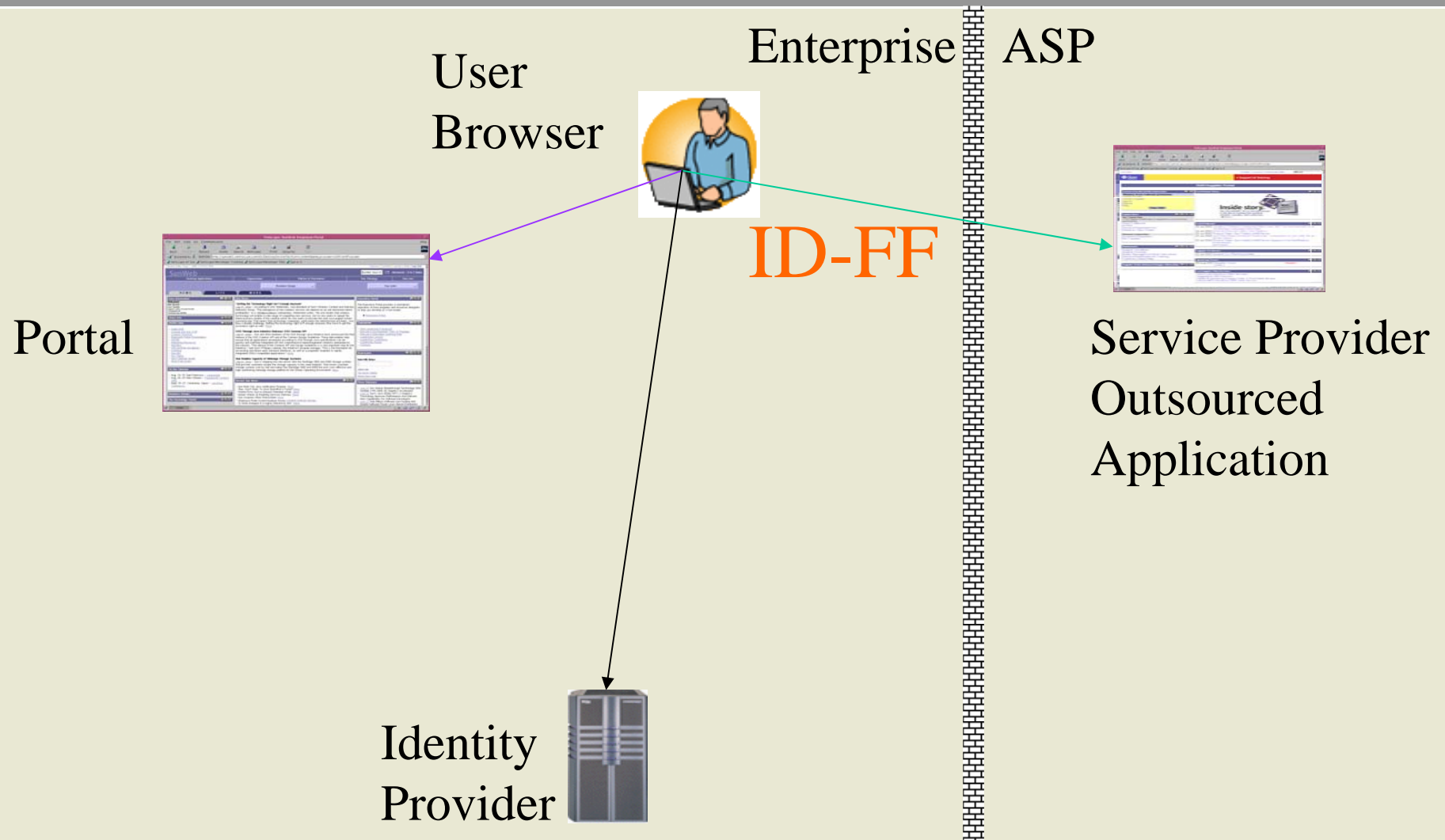


Strategy: Consolidate, Synchronize and Federate Identities as needed

# Liberty in Outsourcing Scenarios



# Deployment – Phase 1



# Lessons Learned

- Account Creation
  - Manual vs Bulk registration & federation
  - Bulk registration, permanent federation
  - Generated SP ID and Password
  - Bootstrap with periodic data transfer for phase 1
  - Replace with ID-WSF in phase 2
- Account Termination
  - Remove vs Defederate
- Provisioning MRD should help
  - 4.0 effort to add interface/model for bulk federate/de-federate use cases
  - MRD under development now

# Lessons Learned

- Data needed by ASP
  - Authentication
    - Example - SP ID, SP Password
  - Authorization
    - Example – job level, department, citizenship status...
  - The actual ASP service
    - Example – zip code for customization

# Lessons Learned

- Authorization at outsourced ASP
  - Data from many sources, some outsourced
  - For privacy, we need to combine and obfuscate data needed by ASP
  - Need an 'interim' store for raw data & obfuscated 'flags' to facilitate support
  - Replace with ID-WSF and role scheme in phase 2

# Lessons Learned

- Support
  - SP account federated to IDP account
  - User always uses IDP account to login
  - User forgets (or never knew) SP account ID
  - SP doesn't know user's IDP account
  - User calls SP for support, how do they identify their account?
  - How to do this without violating privacy established with Liberty?
  - Options: Lookup, translation etc

# Business Benefits – Phase 1

- **Facilitate security of outsourcing**
  - Authentication handled by Sun
  - One ASP asked me “Why encrypt passwords?”!!!
- **Help reduce some work for application teams**
  - App teams don’t have to invent new authentication scheme for every application
  - One industry standard approach used
- **Help reduce some support costs**
  - May result in fewer password resets
  - Fewer application-specific authentication schemes to learn, monitor, support

# Q&A