



australian access  
federation

*eResearch Australasia Conference*  
*29<sup>th</sup> June 2007*

# Australian Access Federation

# Shibboleth Trust Federation

James Dalziel {james@melcoe.mq.edu.au}  
MAMS Chief Investigator

Neil Witheridge {nwitheridge@melcoe.mq.edu.au}  
MAMS Program Manager



# Workshop objectives

- Review importance of Identity and Access Management (IAM) middleware, Federated IAM (FIAM), Shibboleth and SAML;
- Review MAMS project outcomes, demo services in the Australian HE Testbed Federation, describe MAMS work on developing the AAF Shibboleth Trust Federation;
- Describe requirements for joining the Federation as an Identity Provider (IdP), and user privacy control;

# Workshop objectives (cont'd)

- Describe requirements for joining the AAF as a Service Provider in order to share your services with other AAF members;
- Describe Shib-enabled applications developed by MAMS (IAMSuite, a secure VO for collaborative eResearch);
- Describe mechanisms for accessing Grid services.

# AAF Workshop: Shibboleth Trust Federation

- Agenda
  - High level perspective
    - MAMS Background & Involvement in AAF (JD)
      - The importance of Identity & Access Management Middleware
    - Identity & Access Management (IAM) “101” (NW)
      - User Attributes: Directories and Schemas
    - Shibboleth Federated IAM Infrastructure
      - Identity Providers (IdP), Service Providers (SP), WAYF
      - Shibboleth and SAML
    - MAMS Testbed Federation
      - MAMS Federation Manager

# AAF Workshop: Shibboleth Trust Federation

- Agenda (cont'd)
  - Technical Details
    - Shibboleth Global Uptake: a path well trod
    - Shibboleth Federation entities
      - Identity Provider
      - Service Provider
    - Attribute Release Policy Management
      - ShARPE and Autograph
    - Federated Services
      - Shibboleth enabling a web application
      - Shibboleth enabling non-web applications (DAR-ASM)
    - OpenIdP (aka Virtual Home Organisation)
    - Shared/Hosted Services

# AAF Workshop: Shibboleth Trust Federation

- Agenda (cont'd)
  - Special Topics (time permitting)
    - auEduPerson Schema
    - IAMSuite
    - PeoplePicker
    - Grid Interoperability
    - Interfederation Peering
    - Entitlement Attributes Hosting
    - Authorisation and XACML
    - Shibboleth 2.0

# MAMS Background

- DEST funded projects
  - under Systemic Infrastructure Initiative (SII)
  - seeking to improve national research effectiveness

*For too long, information resources and computing services have been fragmented across the national ICT infrastructure sitting in small, inaccessible “silos” . <http://www.melcoe.mq.edu.au/projects/MAMS/>*

- Initial focus (FRODO projects) on information resources and computing services
  - Repository Projects (ARROW, APSR, ADT)
  - Identity & Access Management (IAM) project (MAMS)

*At the heart of the middleware required to unleash research potential is the cluster of services described as “access and identity management”.*

# MAMS deliverables

- MAMS Testbed Federation (Levels 1,2,3)
- Federation Manager
- Shibboleth IdP Easy Installation CD (knoppix)
- ShARPE: Shib Attribute Release Policy Editor
- Autograph: Configure your personal idCard
- Shibbolized Applications
  - DSpace, Fedora, Zope/Plone, Twiki, Moodle...
  - Authenticated Federated Search service
- Access control using XACML (Fedora repo.)

# MAMS deliverables (cont'd)

- Online Librarian: Shibboleth protected instant messaging (& generic helpdesk application)
- Shibbolized GridSphere portal → Virtual Organization Infrastructure (IAM Suite)
- Shibbolized MyProxy → Access to Grid Services
- Authentication State Manager (ASM) & Delegated Attribute Retriever (DAR)
- Roadshows, Workshops for Australian HE
- MiniGrant Scheme (Rounds 1 and 2)
- Debian Linux VMWare IdP/SP

# MAMS Testbed Federation

<http://federation.org.au/FedManager/listMembers.do>



**“Level-2” Federation** (at 26/6/07):

21 Service Providers

19 Identity Providers  
(~900,000 identities)

Organization Name
<a href="#">AARNet</a>
<a href="#">ac3 Research</a>
<a href="#">Australian National University</a>
<a href="#">Curtin University of Technology</a>
<a href="#">Edith Cowan University</a>
<a href="#">EMU</a>
<a href="#">eSecurity Framework Project Wiki</a>
<a href="#">Macquarie University</a>
<a href="#">Macquarie University Online Librarian</a>
<a href="#">MAMS Resources</a>
<a href="#">MELCOE IdP</a>
<a href="#">Monash University</a>
<a href="#">Monash University E-Research Grid Services</a>
<a href="#">Murdoch University</a>
<a href="#">Nanostructural Analysis Network Organisation</a>
<a href="#">QUT</a>
<a href="#">TestFed OpenIdP 2</a>
<a href="#">The Learning Federation</a>
<a href="#">The University of Melbourne IdP</a>
<a href="#">The University of Queensland</a>
<a href="#">UniSA</a>
<a href="#">University of Technology, Sydney</a>
<a href="#">University of Western Australia</a>
<a href="#">UQ Library</a>
<a href="#">VeRSI OpenIdP</a>
<a href="#">VeRSI VO</a>

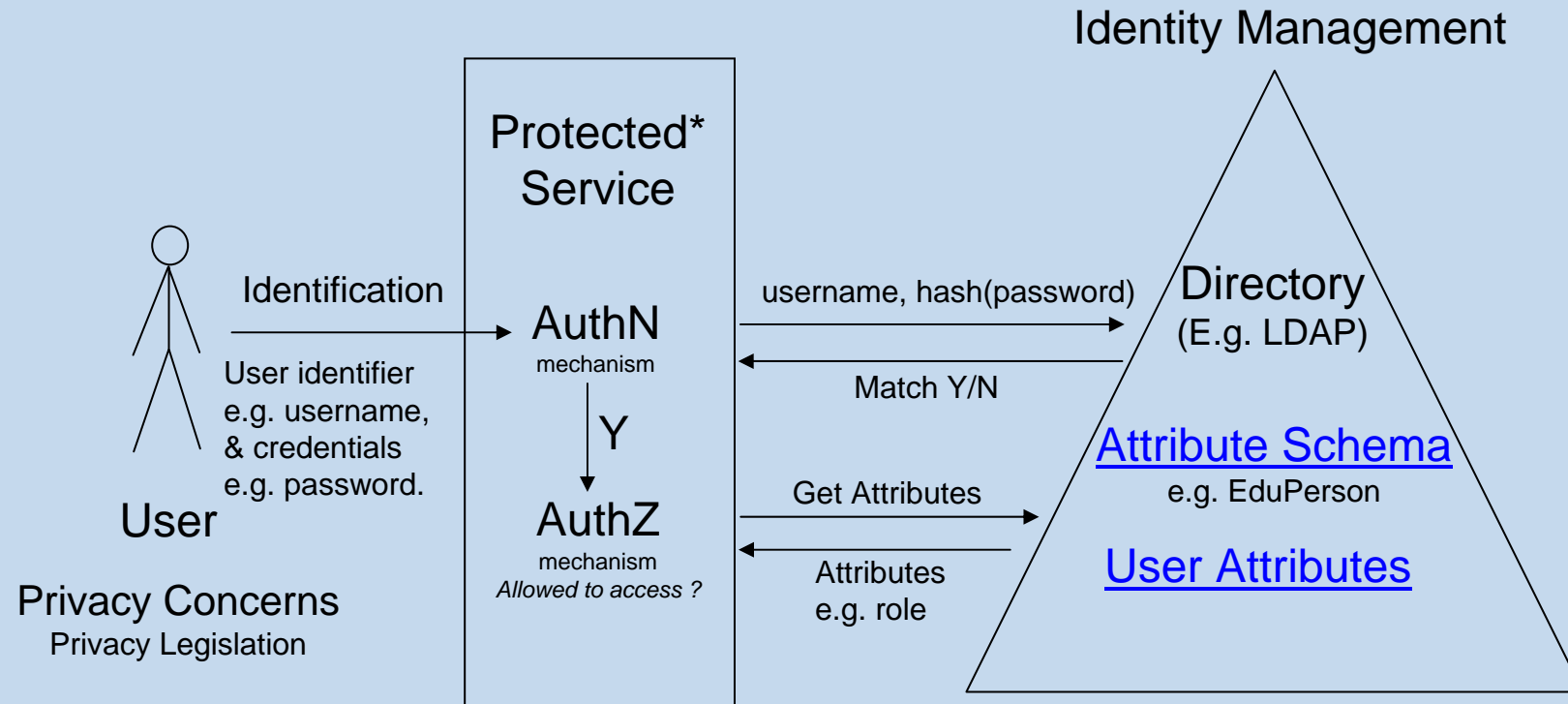


australian access  
federation

# Federated IAM, Shibboleth & SAML

# Access Control '101'

Authentication, Authorization & Accounting



\* Protected = implements access control  
(i.e. implements authentication, authorization, [accounting] )

# Internet & Security 'basics'

- HTTP
  - Request/Response, Commands (e.g Redirect)
  - Session Cookies
  - HTTP Server Filters
- Web Single-Sign-On (SSO)
  - intra- and inter-institutional requirements
- Public Key Crypto security applications
  - Digital signatures, digital certificates
  - SSL/TLS, HTTP over TLS (https://)
  - XML Signature / XML Encryption (in SOAP)
- Public Key Infrastructure (PKI)
  - Registration Authority, Certificate Authority, Certificate Revocation List, cross certification

# Federated IAM

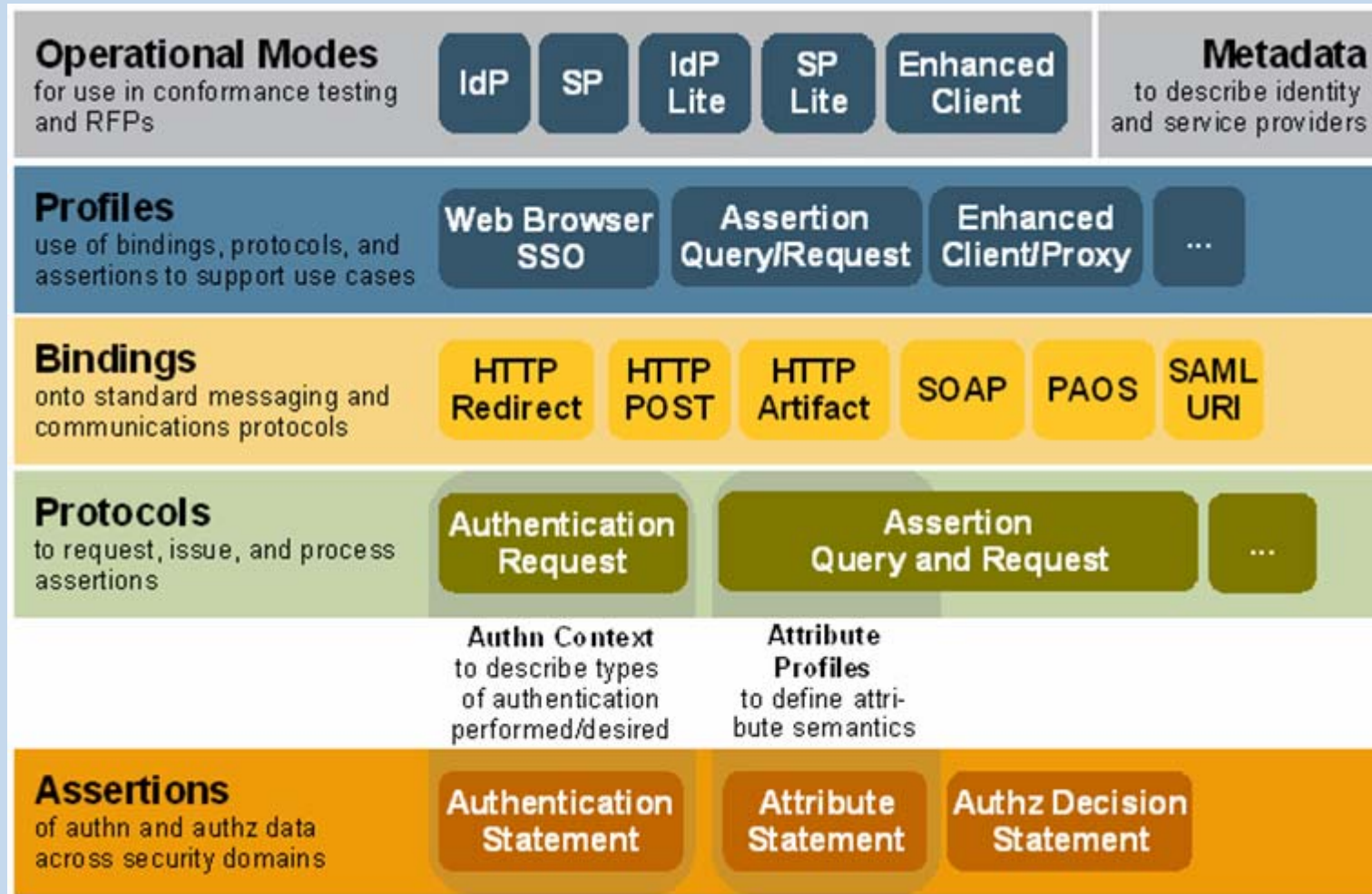
- A definition of 'Federation': *Set of organisational entities having mutual trust and interoperating collectively to share resources & achieve outcomes.*
  - a 'Trust Federation'
- Identity Providers (IdP)- role is to securely & accurately manage user identities, and provide a means of user authentication, and deliver authentication status and user attributes to SPs
- Service Providers (SP) - role is to provide a service to IdP members (users) based on user authentication and attributes obtained via an IdP
- Federation Infrastructure (metadata management, policy information, common services)

*Many organisations in the Trust Federation will be both IdP and SP*

# Secure Attribute Transfer

- OASIS' Open Standard: SAML
  - Security Assertion Markup Language
- Underlying standard for Federated IAM
- Secure transfer of *Security Assertions* from IdP to SP, containing *statements*
  - Authentication Statement
  - Attribute Statement
- SAML Request/Response protocol
  - Attributes pushed by IdP or pulled by SP
- Browser profiles

# SAML Anatomy (from wikipedia)



# Shibboleth in a nutshell

Shibboleth (developed by Internet2 in US) is

- a Federated IAM infrastructure
  - A “Federation” is comprised of trusted Identity Providers (IdP) and Service Providers (SP) (and WAYF)
- an open source implementation of SAML (OASIS’ Security Assertion Markup Language)
  - secure transfer of authentication status and user attributes via HTTP between IdP and SP
- a solution for inter-institutional (i.e. across-security domains) Single Sign-On (SSO) via a web browser
  - implements SAML browser profiles

# Shibboleth in a nutshell (cont'd)

Shibboleth provides for:

- Infrastructure for Trust between organisations
  - Federation level 'SAML' metadata
  - IdP, SP, WAYF software and configuration data
- Attribute resolution
  - Obtaining (resolving) attributes from IdP directory
  - Dynamically created attributes
- Privacy protection of users
  - Attribute release policies at IdPs
  - Ability to retain user anonymity

# Shibboleth in a nutshell (cont'd)

Shibboleth does not provide:

- a “shibboleth authentication mechanism”
- Shibboleth relies on the IdP’s local web-based authentication mechanism
  - e.g. Apache LDAP authentication, or WebSSO system such as PubCookie (with LDAP or Kerberos)
  - See <http://www.federation.org.au/twiki/bin/view/WorkShop2005/ShibPubCookie> for instructions on configuring Shibboleth with PubCookie

# Shibboleth Federation Overview

- Federation Entities



Identity Provider

Secure identity management is a core business requirement



Federation Manager

Agreements  
Policies  
Auditing ?  
WAYF Agent



Service Provider

Provide Services accessible via the web

Want to focus on core business & avoid risks of managing users' confidential info.

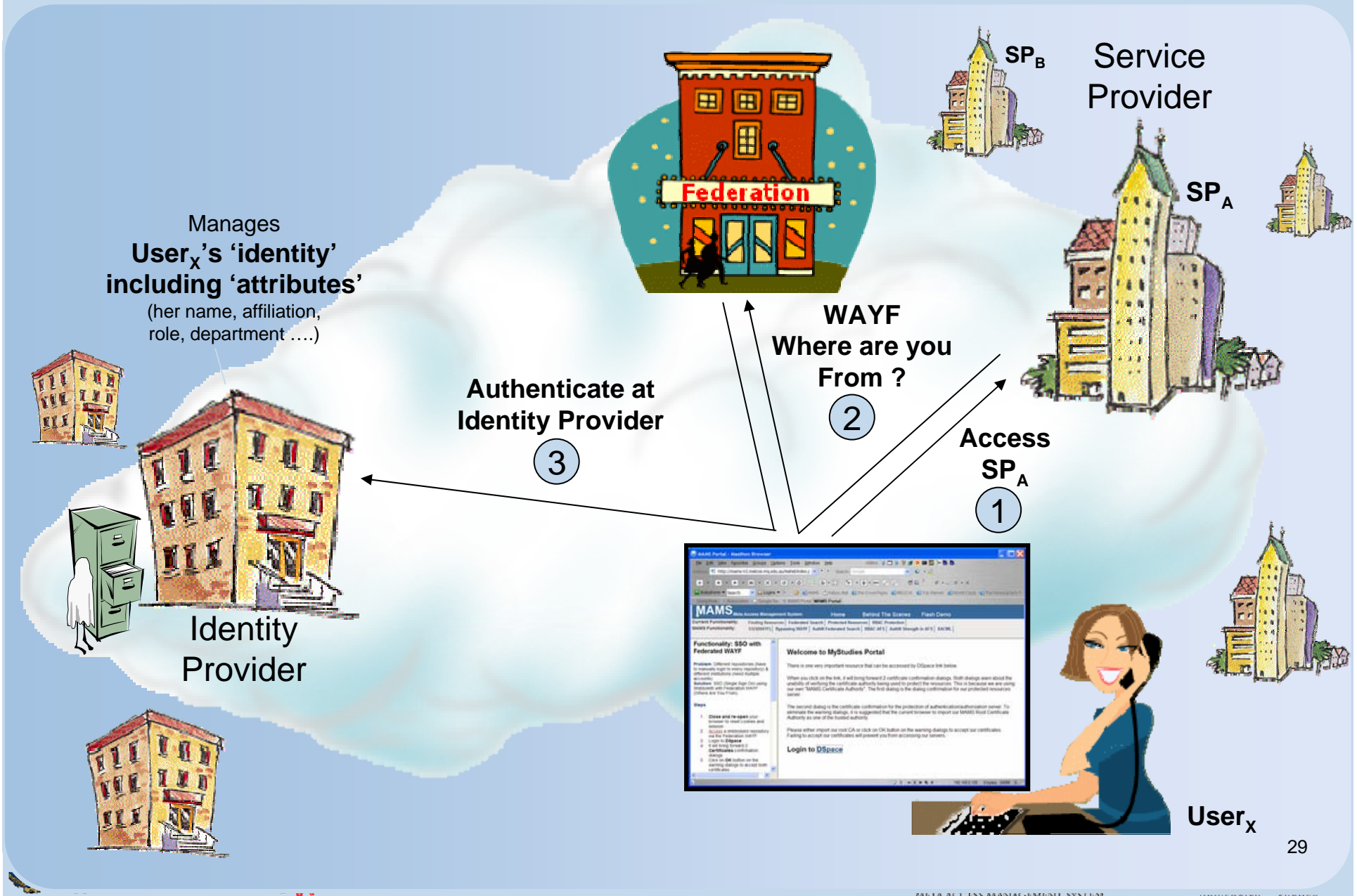
User

Belongs to an organisation which manages their identity

Privacy concerns

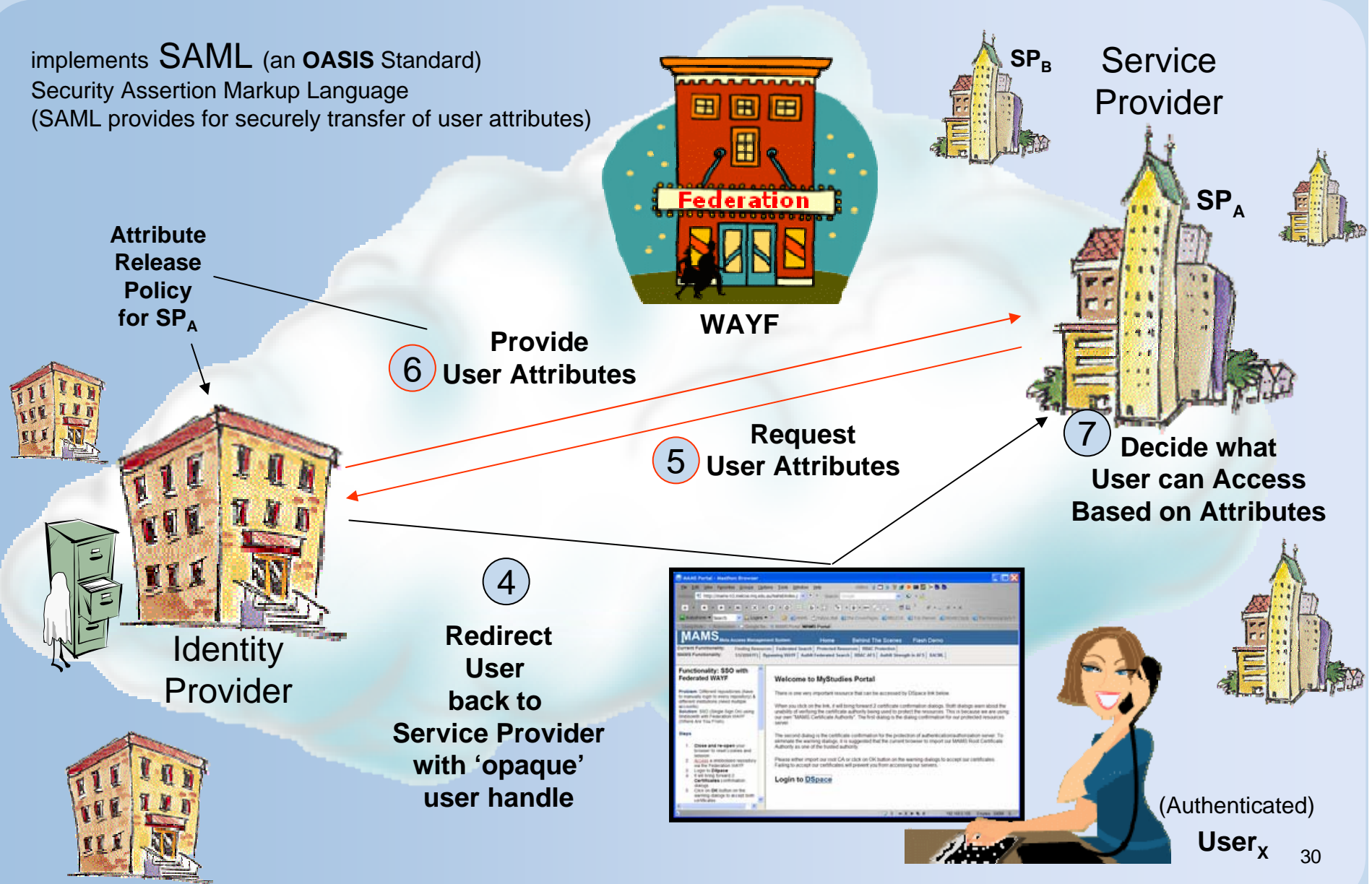


# Shibboleth Protocol - User Authentication



# Shibboleth Protocol - User Attribute Transfer

implements **SAML** (an **OASIS** Standard)  
Security Assertion Markup Language  
(SAML provides for securely transfer of user attributes)



(Authenticated)  
User<sub>x</sub> 30

# Shibboleth Protocol - Single Sign On

Within authenticated session, SSO to other service providers in Federation (uses session cookies)

Attribute Release Policy for SP<sub>B</sub> for U<sub>x</sub>



WAYF

Another Service Provider

Decide what User can Access based on Attributes

Service Provider



SP<sub>B</sub>



SP<sub>A</sub>



Identity Provider

⑥ You can have these

⑤ Gimme attributes

I know you!

I know you!

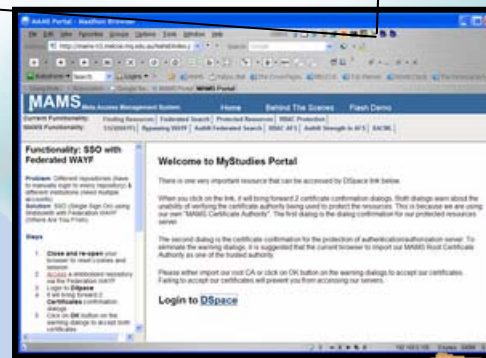
④ Redirect Authenticated User back to Service Provider with 'opaque' user handle

②

③

①

SSO !



(Authenticated)

User<sub>x</sub>

# Shibboleth Protocol - without need for WAYF

Log into your Institution's portal ...  
Logs you into your IdP via your Institutions WebSSO mechanism...

Hence no need for the WAYF to get involved ...



WAYF

Service Provider

Decide what User can Access based on Attributes

Service Provider



SP<sub>B</sub>



SP<sub>A</sub>

④ You can have these

Gimme attributes

③

② Redirect User to Service Provider with 'opaque' user handle

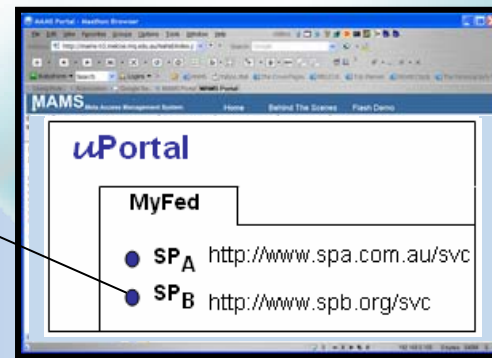


Identity Provider

I know you!

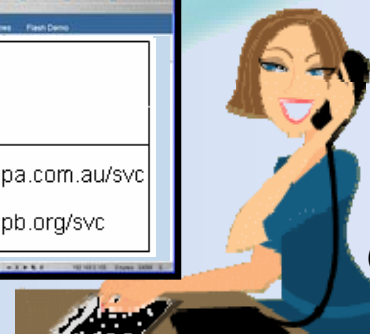
①

Access a Federation Service via the portal



Portal

SSO !



(Authenticated)

User<sub>x</sub>

32

# Federation Trust Relationships

- Trust relationship between IdPs and SPs
- Trust requires a policy framework and accountability
  - Adoption of an agreed attribute set & adherence to a common vocabulary
  - Membership rules (roles & responsibilities)
  - IdP-specific policies
    - User registration process (e.g. 'point' system)
  - SP-specific policies
    - How user attributes are stored and used

# MAMS Mini-Grant Program

(2 rounds of 5 projects, AUS\$40k per project)

## Round 1 (Feb 2006):

- AARNet:
  - IdP, ENUM SP
- Griffith Uni:
  - IdP,  
IT Department Wiki SP
- Uni of Qld
  - IdP,  
eSpace Fedora+Fez SP
- Qld Uni of Technology :
  - ATN IdPs,  
eGrad School SP
- Uni of Sydney
  - IdP,  
NANO image database SP

## Round 2 (Jul 2006):

- Deakin Uni:\*
  - IdP, eLectures SP
- James Cook Uni:
  - IdP,  
JCU/AIMS data access SP
- Melbourne Uni:
  - IdP, LIGO data access SP
- Monash Uni:\*
  - IdP, Shibbolised SRB SP
- Murdoch Uni:
  - IdP, Online Librarian SP
- Curtin Uni:
  - 5 IdPs (WAGUL),  
Reciprocal Borrowing SPs

\* Shared project funding

# Demo: Shibboleth SP examples

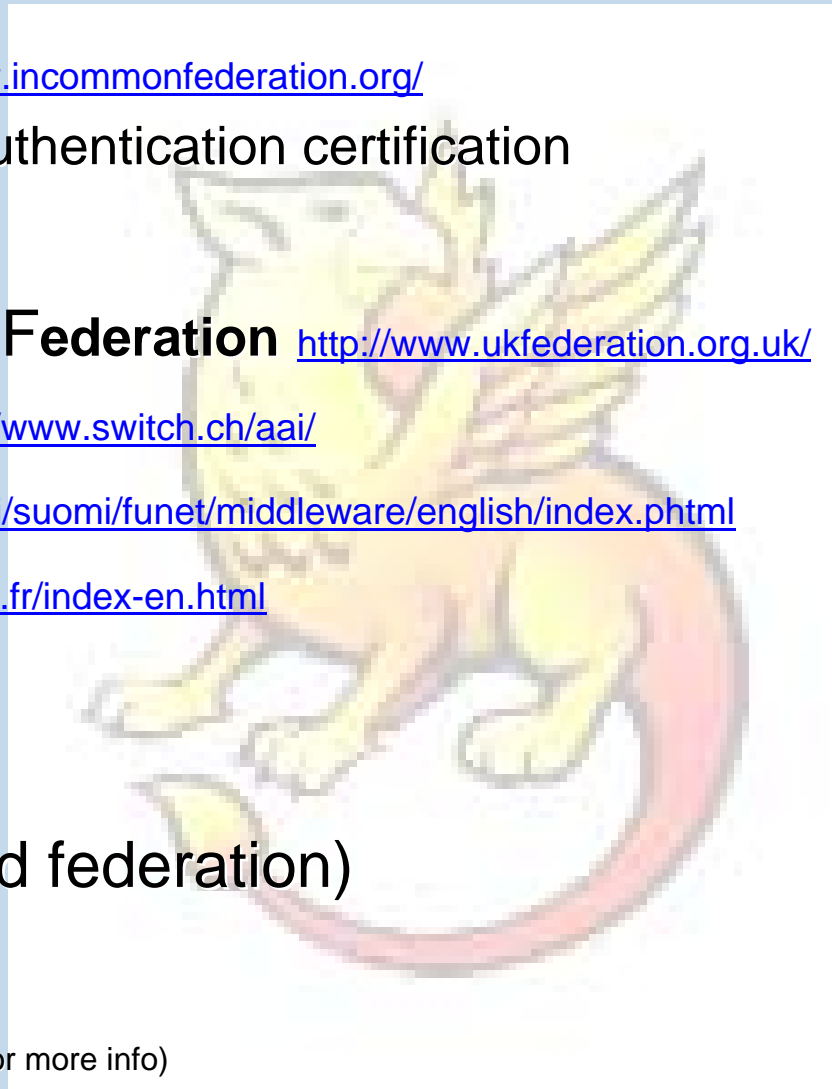
- Information Repository Service
  - accessing using Macquarie University identity
  - [UQ ePrints Service](https://espace.library.uq.edu.au/) ( <https://espace.library.uq.edu.au/> )
- Collaborative Tools
  - [Shibboleth Wiki](#)
- Sharing Library Service
  - WAGUL Reciprocal Borrowing
  - [Borrower Registration](#), [Workstation Authentication](#)
- Database Access Service
  - UQ/USyd NANO Project
  - [Image database](#)

*One name and password = access to many services.*

# Global Shibboleth Up-Take in HE

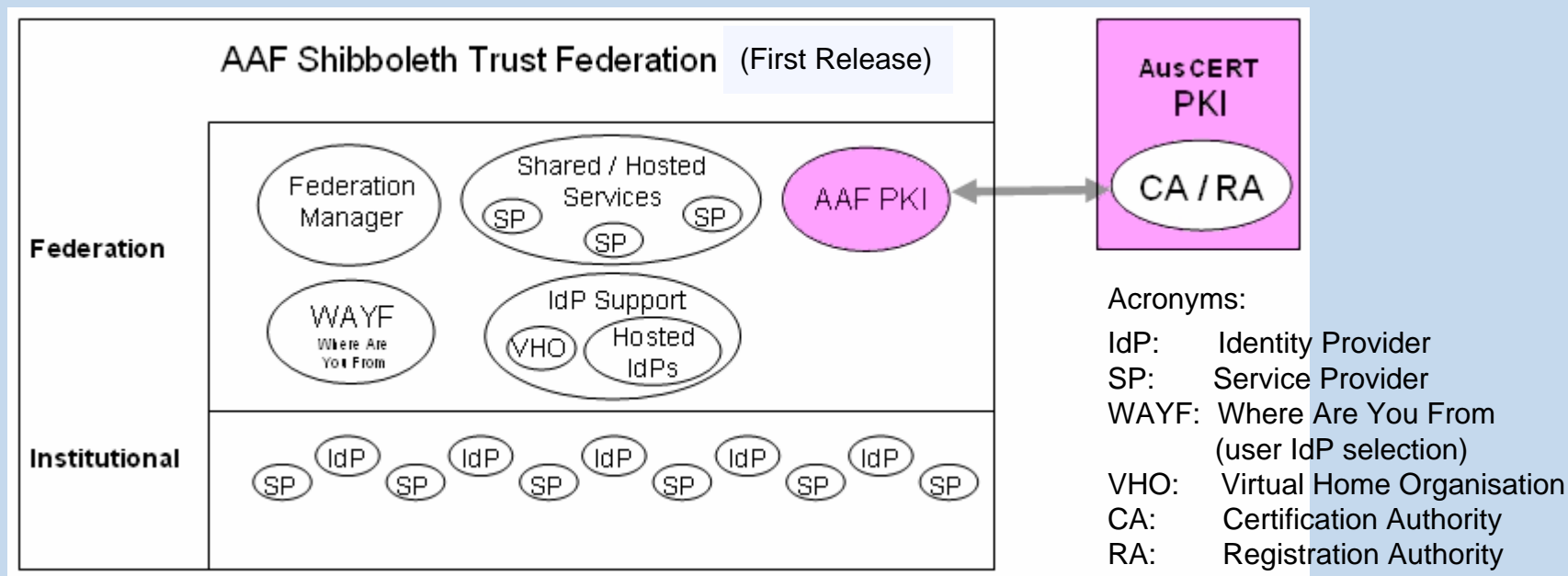
- \* US (InCommon) <http://www.incommonfederation.org/>
  - Shibboleth has US Gov't E-Authentication certification
- Europe
  - \* UK Access Management Federation <http://www.ukfederation.org.uk/>
  - Switzerland (SWITCH) <http://www.switch.ch/aai/>
  - Finland (HAKA) <http://www.csc.fi/suomi/funet/middleware/english/index.phtml>
  - France (CRU) <http://federation.cru.fr/index-en.html>
  - Germany, Italy, Greece
- Asia/Pacific
  - Australia (MAMS Testbed federation)
    - <http://federation.org.au>

(See <http://shibboleth.internet2.edu/community.html> for more info)



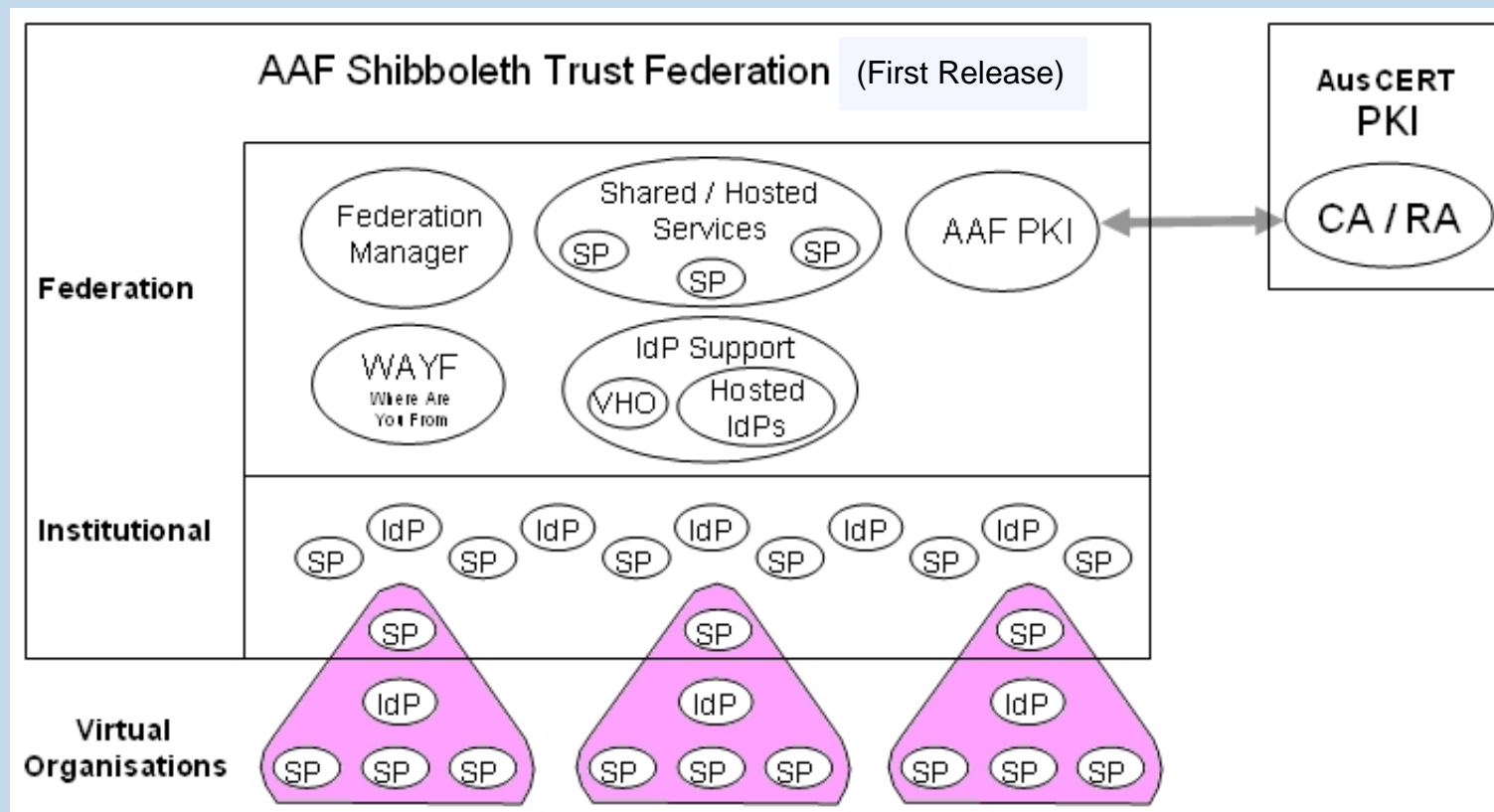
# Shibboleth Trust Federation

- Federation Manager & Federation Website
- WAYF (Where Are You From) agent
- Shared Services (Fed White Pages)
- Integration with AusCERT PKI (server, end-user certs)
- Hosted Services (potential yet to be determined)



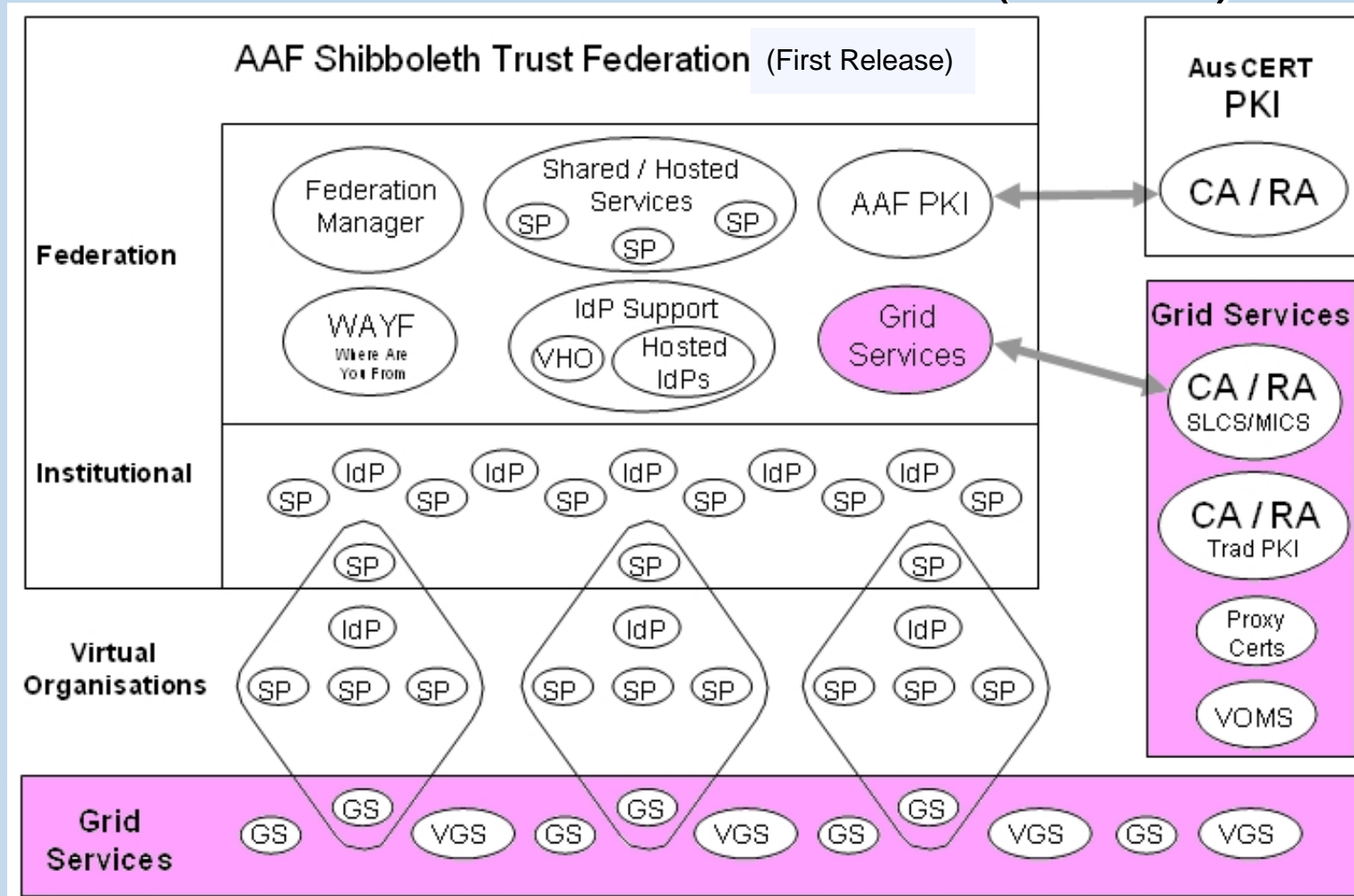
# Australian Access Federation

- Shibboleth Trust Federation (cont'd)



# Australian Access Federation

- Shibboleth Trust Federation (cont'd)



# Joining the Federation as an Identity Provider

- Pre-requisites:
  - Secure Identity Management
  - Directory with user attributes
    - Directory Schemas
  - Authentication Mechanism
  - IdP Server
    - Public IP Address
    - Web Server and other required software
    - Certificate(s)
    - Shibboleth IdP software installed

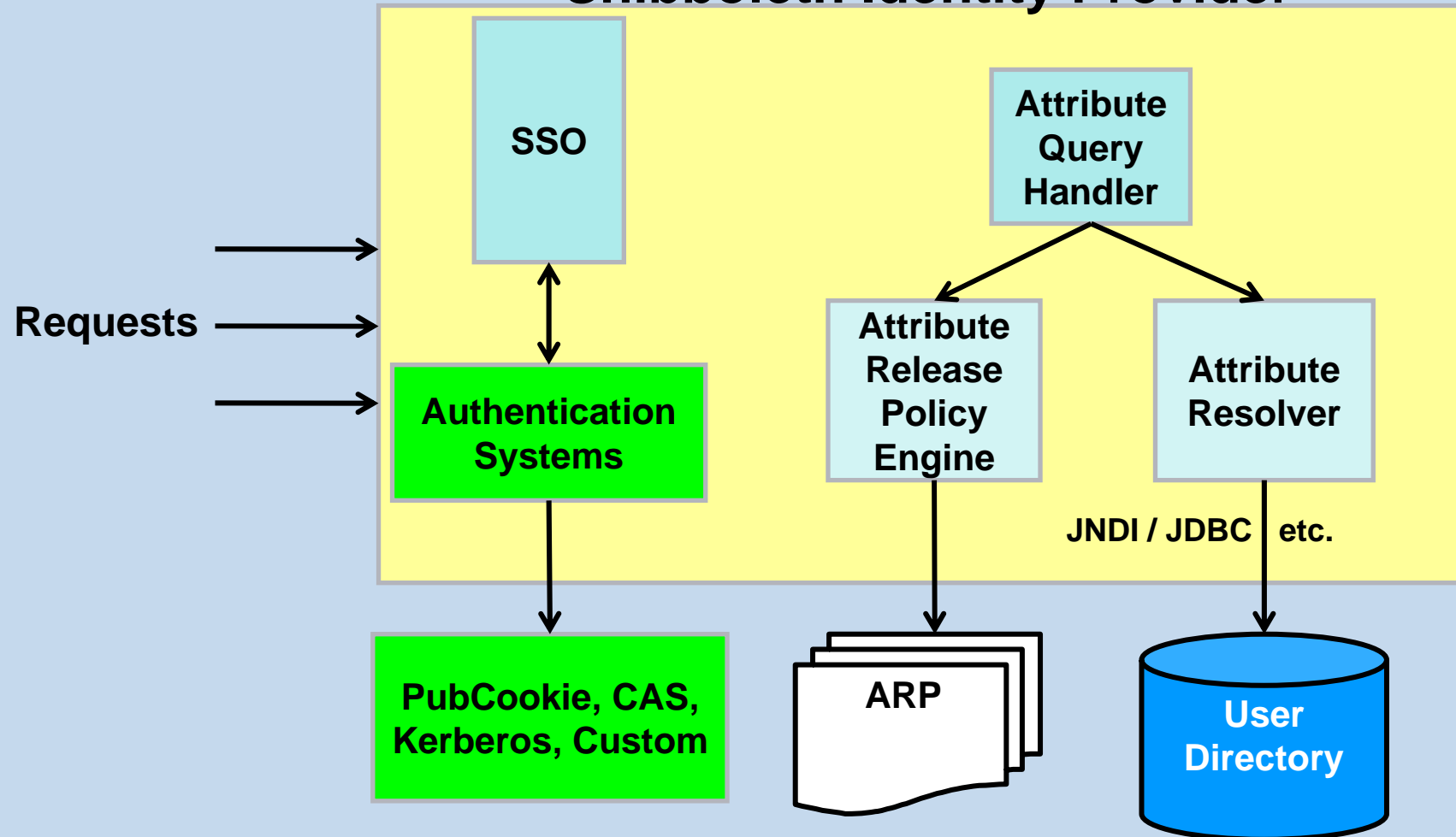
# Identity Provider (IdP)

- Authenticates the user
- Returns user identifier (user handle), authentication state & method to SP
- Receives request from SP for attributes for user associated with handle
- Obtains attributes from IdP directories
- Releases set of attributes specified by Attribute Release Policy (ARP)
  - protects and manages user's privacy

17 - 18 April 2007

# Shibboleth IdP Architecture

## Shibboleth Identity Provider



17 - 18 April 2007

# Shibboleth IdP Flow

1. User login is handled by SSO Handler which interfaces user with the IdP's authentication mechanism
2. Upon successful authentication, user "handle" is sent to Service Provider
3. Service Provider requests user attributes via the IdP Attribute Query Handler
4. Attribute Query Handler interfaces with IdP's Directory Service to obtain user's attributes
5. A SAML Assertion containing permitted attributes is sent back to Service Provider

17 - 18 April 2007

# IdP Configuration & Maintenance

- IdP Set-up & Configuration
  - Download Federation (SAML) metadata
  - Configure connection to user directory
  - Defines ARPs for “site” and “groups”
    - Defines Attribute Release Policy per Service Provider (or for all Service Providers)
- IdP Maintenance
  - Download Federation (SAML) metadata
  - Update Attribute Release Policies
  - View log files for incident tracking
  - Upgrade to latest software (patches)



17 - 18 April 2007

# Attribute Release Management

- IdP Attribute Release Policies (ARPs) contain rules determining which attributes are released from the IdP to individual SPs
  - Different SPs obtain different attribute sets for the same user.
- ARPs at IdP
  - Site, Group & User ARPs
  - User ARP over-rides Group, Site
- ARP Management tools - ShARPE and Autograph - enable Privacy Control at IdP

# Admin tool: ShARPE

IdP Administrators import “service descriptions” and create site & group ARPs

Manage Service Provider Contracts

**GETTING STARTED** Contract for service provider  
**University of Art**

**SERVICE PROVIDERS ...** Test site for federation applications  
Picture Gallery Service

**CONTRACTS**

Service Provider:  
University of Art

Community:  
\*all communities\*

Service Level	Description	Required Attributes
download	This Service Feature offers the functionality to download pictures in high resolution.	-FullName ( any value) -community ( any value) -surname ( any value)
search	This Service Feature offers search functionality.	-community ( any value)

**MAPPINGS**

**AUTOGRAPH ...**

**LOGOUT**

Contract for communities	Released Attributes	Enabled service levels
*all communities*	<input checked="" type="checkbox"/> community remove add SPAttributes:	<input type="checkbox"/> download <input checked="" type="checkbox"/> search

# User tool: Autograph

Users can view attributes released to a SP and create User ARPs.

The screenshot displays the Autograph web application interface. At the top left is the 'Autograph' logo, and at the top right is the Macquarie University Sydney logo. Below the header, a blue bar contains the text 'A privacy management tool.' The main content area is divided into a left sidebar and a main panel. The sidebar has two sections: 'INSPECT ATTRIBUTES' with a dropdown menu for 'Select a Service Provider:' set to 'MAMS Public', and 'OTHER OPTIONS' with links for 'Home', 'Preserve my privacy', and 'More information'. The main panel shows a 'Welcome admin as Moritz' message and a 'MY IDCARD' box with the following attributes: 'eduPersonAffiliation: Staff', 'givenName: Moritz', and 'sn: Theile'. Below this, a message explains that the service is provided by MAMS Public and that the idCard gives access to service features, indicated by a green light. A 'PICTURE GALLERY SERVICE' section follows, showing two service features: 'search' and 'download', both with 'access available' status and green indicator lights.

**INSPECT ATTRIBUTES**

Select a Service Provider:  
MAMS Public

**OTHER OPTIONS**

- Home
- Preserve my privacy
- More information

Welcome admin as Moritz  
This is the idCard you are offering to MAMS Public when you visit it. You can edit the card if you are concerned about your privacy.

**MY IDCARD**

- eduPersonAffiliation: Staff
- givenName: Moritz
- sn: Theile

This is the Service provided by the MAMS Public. The idCard gives you access to the Service Features with a green light. Click the link next to the red light to make the Service Feature accessible.

**PICTURE GALLERY SERVICE:**

A large repository of pictures.

<b>The access to Service Feature 'search' is available.</b> This Service Feature offers search functionality.	access available
<b>The access to Service Feature 'download' is available.</b> This Service Feature offers the functionality to download pictures in high resolution.	access available

# ShARPE & Autograph Demonstration

1. [Uploading Service Description and using ShARPE to create Attribute Release Policy](#)
2. [User Attribute Release Policy Management using Autograph](#)
3. [Autograph in the Shibboleth cycle](#)

# Authentication, How Trustworthy ?

- Level of Assurance
  - IdM Processes
    - Identity Proofing & Registration
  - Standard Definitions used by Government
- Authentication Strength
  - PKI vs Username/Password
  - Multi-factor authentication
- LoA information requirement for AAF

# Joining the Federation as a Service Provider

- Pre-requisites:
  - Web Resources (i.e. accessible via URL) requiring protection
    - Shibboleth-enabled applications
      - Authorisation based on user attributes
  - SP Server
    - Public IP Address
    - Web Server and other required software
    - Certificate(s)
    - Shibboleth SP software installed

# Index of Shibboleth-Enabled Applications and Services

- ArtSTOR
- Blackboard
- Bodington.org
- CSA
- Darwin Streaming Server
- Digitalbrain PLC
- eAcademy
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris - SFX
- Fedora
- Higher Markets
- Horde
- Hupnet
- ILIAS
- JSTOR
- Moodle
- Napster
- NSDL
- OCLC
- OLAT
- Ovid Technologies Inc.
- Proquest Info. and Learning
- Serials Solutions
- SYMPA
- Thomson Gale
- TWiki
- Useful Utilities - EZproxy
- WebAssign
- WebCT

Source: <http://shibboleth.internet2.edu/seas.html>

# Service Provider (SP)

- Provides and protects web-based services
- Links to an IdP discovery service (WAYF)
- Defines attributes required for service authorisation
  - Federation - realm - bilateral agreements
  - SP Description
- Trusts IdP to perform user authentication and to provide user attributes
- Protect user's attributes – conformance to federation policies

17 - 18 April 2007

# Shib-enabling a web application

- Attributes received via shibboleth are inserted in HTTP header and sent to application
- Application reads attributes from HTTP header
- Authentication mechanisms must be modified to use the attributes received
- Persistent identifier available to allow customisation

# SP Pattern: Simple case

- Shibboleth SP deployed as a HTTP Filter
- Filter redirects unauthenticated user to WAYF, IdP, for authentication
- Following authentication, Shibboleth SP receives user handle, then requests user attributes
- Attribute name-value pairs inserted into HTTP request header and passed through to application
- Application may create user account dynamically, and use attributes for authorisation.

# Shibboleth SP Flow

1. User accesses SP protected web resource, SP filter intercepts, identifies user as unauthenticated
2. Redirect user to WAYF to select Identity Provider
3. Receive User handle following successful authentication
4. Request user's attributes from IdP
5. Receive and process the attributes (use Attribute Acceptance Policy to map attributes to HTTP header values to be delivered to application)
6. Deliver attributes to protected web resource
7. Attributes used by web resource for authorisation

# SP Configuration & Maintenance

- Set-up & Configuration
  - Configure Attribute Acceptance Policy
  - Protect web resources/applications
    - Configure applications to use attributes for authorisation
- Maintenance
  - Upgrade software (patches)
  - Track incidents as reported by applications
  - Update AAP according to attribute requirements

# IdP Selection Service (WAYF)

- If SP service is available to multiple IdPs, user must select their IdP
- Where Are You From (WAYF)
  - Provided with Shibboleth IdP Installation
- Federation may support multiple WAYFs
  - WAYF URL is specified in SP metadata
- Service Provider may provide custom WAYF Service
  - Only lists IdPs which have service agreement
  - Provide customised look and feel



# Example of Online Librarian WAYF

DeploymentBackground - Shibbole... Online Librarian - Home Institutio...

https://www.federation.org.au/mqmurdoc

## Online Librarian - Where are you from?

Please choose your home university:



or if you are from another university, please select it from the list below:

Macquarie University Select Remember for session

# Service Provider Descriptions

- How does an IdP know what attributes a SP requires ?
- MAMS introduced “Service Descriptions” (SDs) as part of ShARPE development
- SDs define “Service Levels” and their attribute requirements
- ShARPE GUI enables upload of SD’s and SD is used to inform admin & user of SP’s service levels and attribute requirements.



aus  
fed access



# Demonstration of Online Librarian Service

## and OpenIdP

# Demonstration Script

1. View current Federation
2. Role of IdP, SP, WAYF (using dummy service)
3. Installing an IdP, certificates, LDAP
4. Installing an SP
5. Installing a Service
6. Creating a Service Description
7. Registering a new admin, organisation, IdP and SP in Level-1
8. Setting up the Resolver, ARP, AAP.
9. Metadata update on IdP and SP.
10. Demonstrating using dummy app. (Role-based and Attribute based access control)
11. View configuration files: IdP idp.xml, resolver.xml, arps; SP shibboleth.xml, aap.xml
12. ShARPE and Autograph to manage IdPs and attribute release.
13. Changes to Site, Group and User ARPS.
14. Demonstrating with dummy app.
15. Deployment models for SP's
16. Separate ProviderIds
17. Under one ProviderId (not rec.)
18. Service Description update
19. Metadata update
20. Demonstration using dummy app.

# Demonstration Script

21. Service Providers: DSpace, Fedora, Confluence, JIRA
22. Shibboleth-enabling web applications
23. Common Services: PeoplePicker
24. DAR/ASM
25. Authenticated Federated Search
26. Fedora Repository
27. XACML Access Control
28. Web Services
29. n-Tiered Web Services & Delegation Profile
30. OpenIdP
31. Grid Interoperability
32. DAR/ASM and MyProxy as CA
33. SLCS and MICS
34. Generating short-lived X.509 certs
35. Proxy certs in Grid world for SSO and Delegation
36. IAMSuite as the 'Killer App': secure eResearch VO
37. Configuring IAMSuite (VeRSI Flash demonstration)
38. Vision for the AAF
39. AusCERT PKI
40. Benefits for Australian HE institutions as IdPs or SPs.