

University of Guelph

Web Access Management with the Sun Identity Suite

Zdenek Nejedly, Matt Searle, Hugh Smith,
Saveena Patara, Bosco Tsang

Computing & Communications Services

Overview

- Challenges, Goals, and Solutions
- Implementation, Examples, Toolkits
- Lessons Learned

The screenshot shows the University of Guelph Central Login page. The header features the University of Guelph logo and navigation links: Academics, Campus, Libraries, Research, and Services. Below the header is a yellow banner with the text "CHANGING LIVES IMPROVING LIFE". The main content area is titled "Central Login" and includes a prompt to log in with a Central Login Account. It contains input fields for "User Name:" and "Password:", followed by a "Log In" button. A security notice at the bottom states: "For security reasons please logout and close your web browser before leaving your workstation." On the right side, there is a "Trouble Logging in?" section with links to "Make sure cookies are enabled in your browser", "Check your password", and "Contact CCS Help Centre". The footer displays the copyright notice "© 2008 University of Guelph".

UNIVERSITY OF GUELPH

Academics Campus Libraries Research Services

CHANGING LIVES IMPROVING LIFE

Central Login

Please log in with your Central Login Account

User Name:

Password:

For security reasons please logout and close your web browser before leaving your workstation.

Trouble Logging in?

[Make sure cookies are enabled in your browser](#)

[Check your password](#)

[Contact CCS Help Centre](#)

© 2008 University of Guelph

What we do



- Provide central IT infrastructure, systems and client support
- Web services on diverse platforms: Apache, IIS, Weblogic, Oracle AS, Tomcat, JRun,...
- Identity Services initiatives:
 - Identity Management
 - Federation
 - Web Access Management

Challenges & Goals

- Authentication and authorization done by individual applications, password caching
 ➡ central service with single sign-on
- Direct LDAP access
 ➡ seamless access to personal attributes
- Multiple datastores and user credentials
 ➡ consolidated identities

Solutions

- Sun Access Manager

 - Central authentication and authorization

 - Session management – SSO

 - Access to directory attributes via policy agents

- Integration toolkits and templates

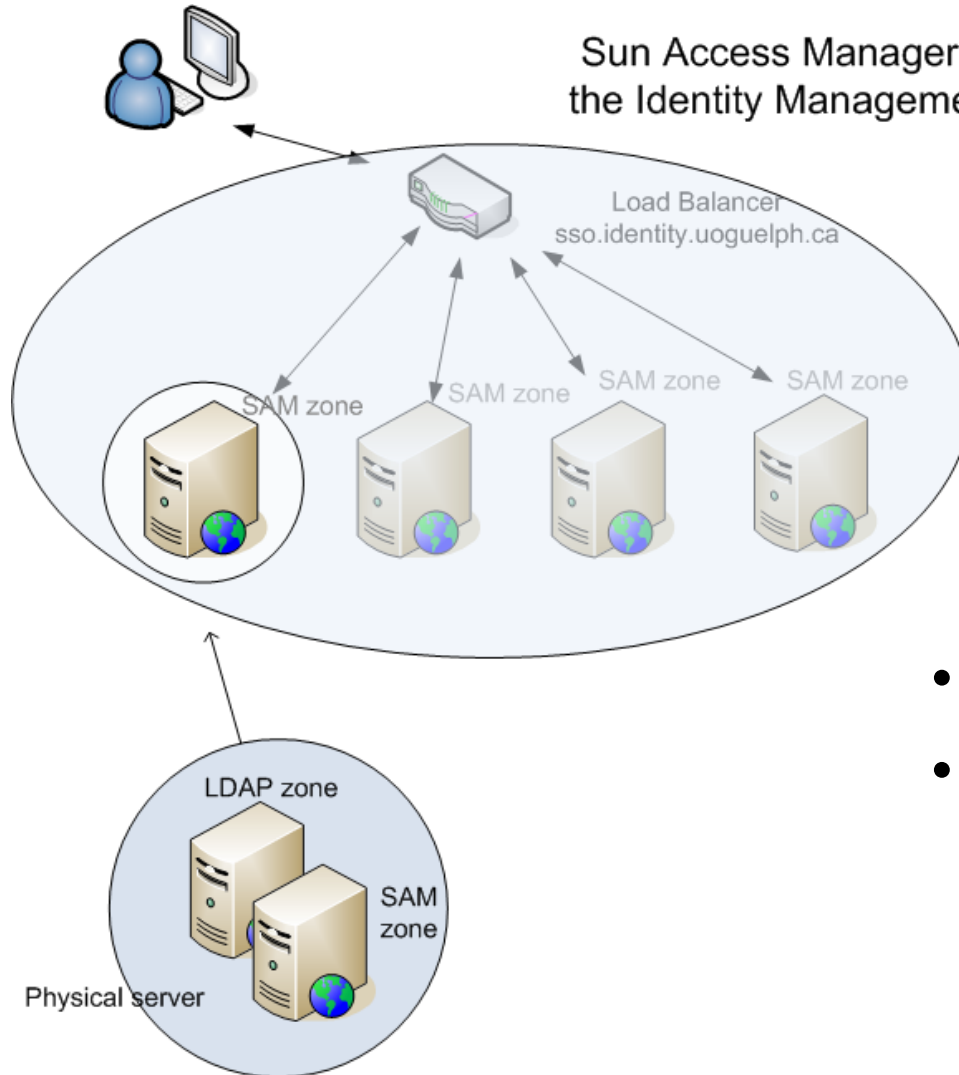
 - Simplified integration and management

- Consolidations and management of identities

 - Expanding the central directory, implementation of Identity Manager

[SAM...](#)

Implementation



- Solaris 10 with zones
- Resource sharing and effective allocation

Implementation Details

- IdM cluster: four SunFire 4150 with Solaris 10
- Two zones on each server:
 - Central directory (Sun Directory Server EE 6.x)
 - Access Manager 7.1
- Access Manager servers
 - deployed in Sun Webserver (JES5u1)
 - AM information tree: replicated across the cluster
 - Authentication: DSEE 6.3 in multimaster replication
- Cisco load balancer
 - SSL terminated on the LB
- Staging, monitoring (BigBrother)

Web@UofG : Diversity

- Web services on diverse platforms
 - Apache, IIS, Weblogic, Oracle AS, Tomcat, JRun,...
 - Linux, Windows, Solaris, HP
- 3rd-party versus custom-designed applications
- Various providers
 - CCS (central), departments and colleges, off-campus
- Major web services
 - Mail, Webhosting, BlackBoard, Registrar systems, D2L, Library

Integration with Webhosting

- Why organizational webhosting?

Full control 

complete solution 

higher service adoption rate

- Wide range of client needs: from static websites to web apps with custom authorization

Customization: Integration Toolkit

- Getting the attributes from AM not difficult:


```
<cfset req = GetHttpRequestData()>  
Hello #StructFind(  
    req.headers, "ca-uoguelph-display-name") #
```

- It needs to be even easier:

```
Hello #WAMGetDisplayName#
```

- Benefits:

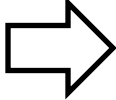
Seamless integration  faster adoption

Hidden implementation  easier maintenance

More Integration Toolkits....APEX

- Different technologies - common interface
- Oracle Application Express (APEX)

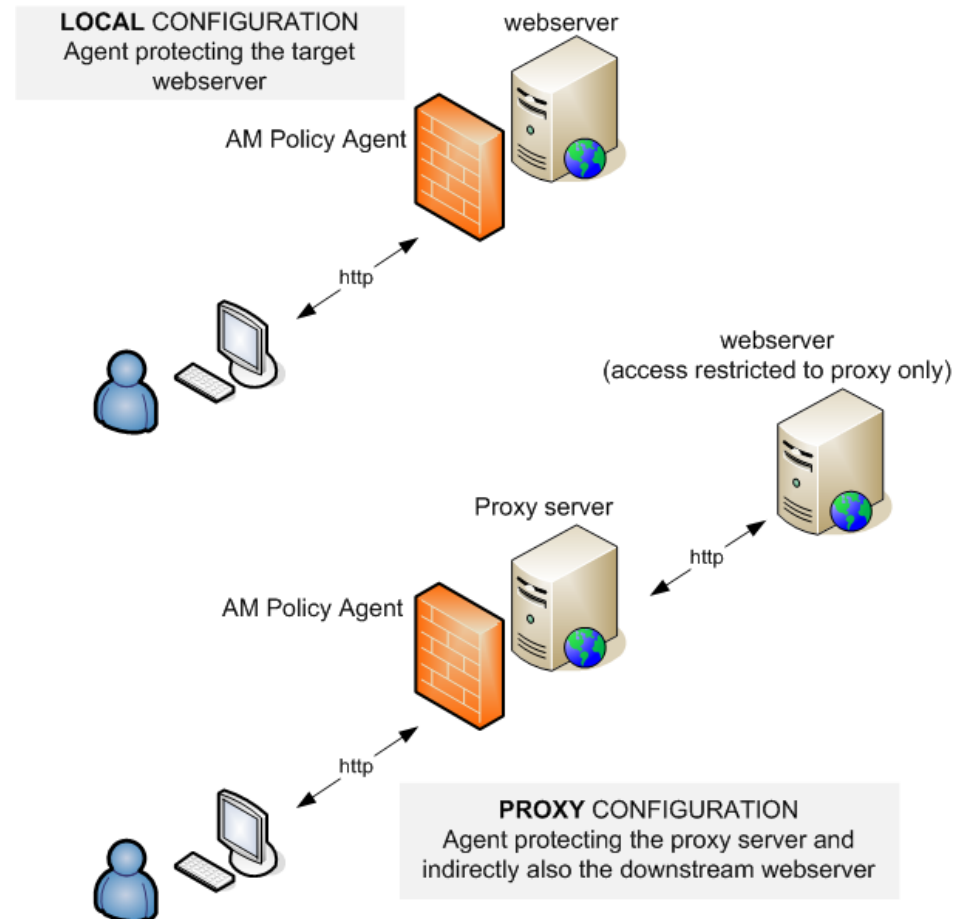
```
wam_uofg.get_display_name()
```

- Oracle HTTP server not supported by AM
  use AM-protected proxy
- Other options: integration with Oracle Access Manager

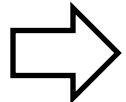
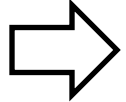
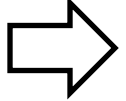
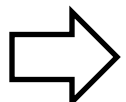
AM-protected proxy

Often applicable to 3rd-party applications
(black-box)

- No installation required on the target web/app-server
- Not suitable for applications relying on REMOTE_USER or J2EE apps with CMS



Lessons Learned

- Cost: integration of 3rd party apps – high cost
new solutions – low cost  start ASAP
- Easy? Make it even easier  toolkits
- URL-based rules  high cohesion of content
beneficial
- Roles for authorization  bridging tools for real-time management

Benefits

- To Community: Single Sign On, increased security
- To Developers: consistently accessible attributes, centrally provided and managed authentication UI, central authorization
- To Administrators: no-cost setup of protected resources, auditing

[Skip the optional discussion material and continue with FAM...](#)

Integration Toolkit details...

Available functions:

Basic authentication:

- `WAMGetUser()` ... returns the username
- `WAMIsUserInRole(roleName)` ... reflects group membership

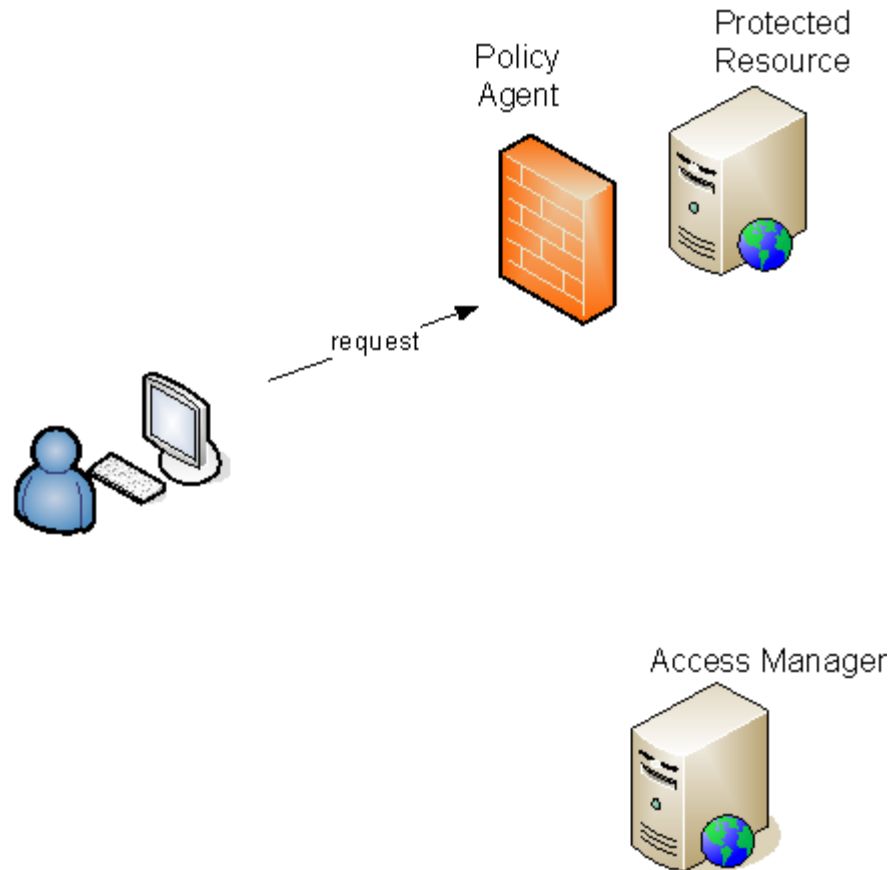
User attributes:

- `WAMGetFirstName()` `WAMGetLastName()`
- `WAMGetDisplayName()` `WAMGetCommonName()`
- `WAMGetEmail()` `WAMGetPhone()`
- `WAMGetOrganizationalUnit()` `WAMGetDepartmentNumber()`
- `WAMGetOrganizationalStatus()`

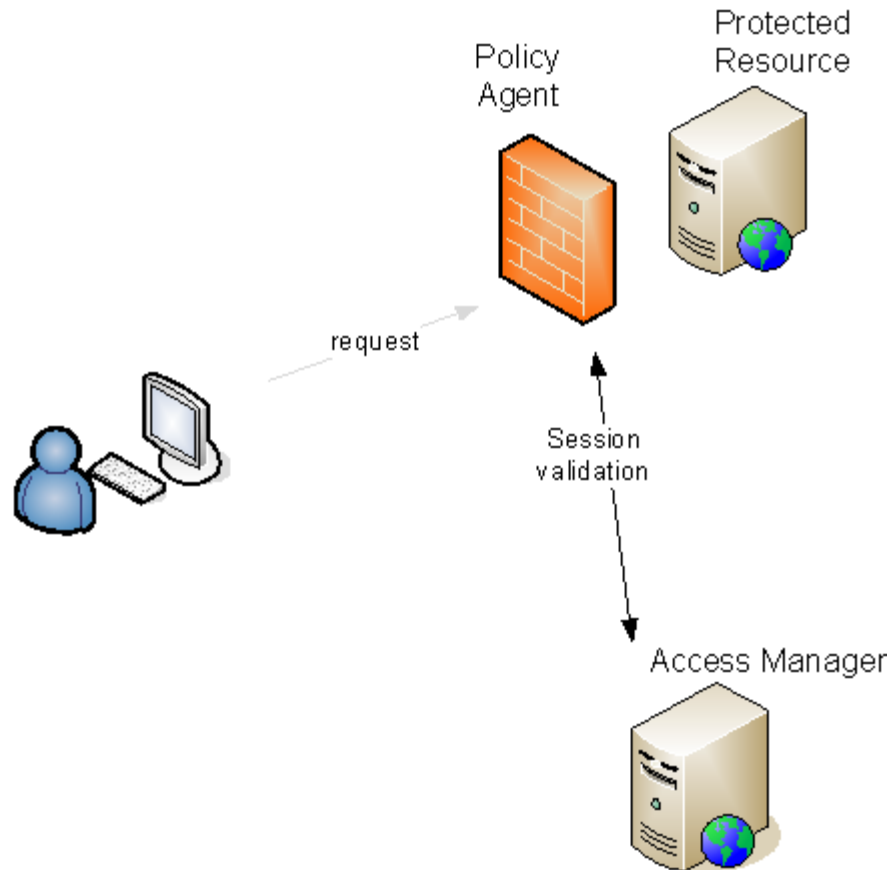
EduPerson attributes:

- `WAMIsEPFaculty()` `WAMIsEPStaff()`
- `WAMIsEPStudent()` `WAMIsEPEmployee()`
- `WAMIsEPAlum()` `etc, ...`

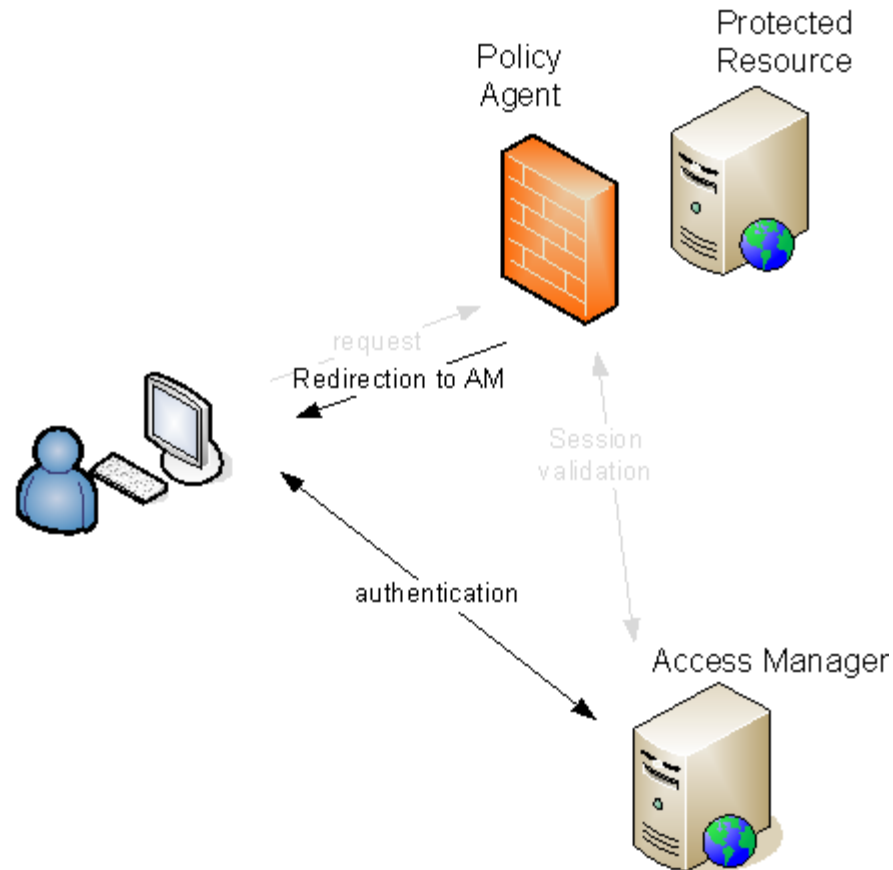
SSO and Policy Enforcement #1



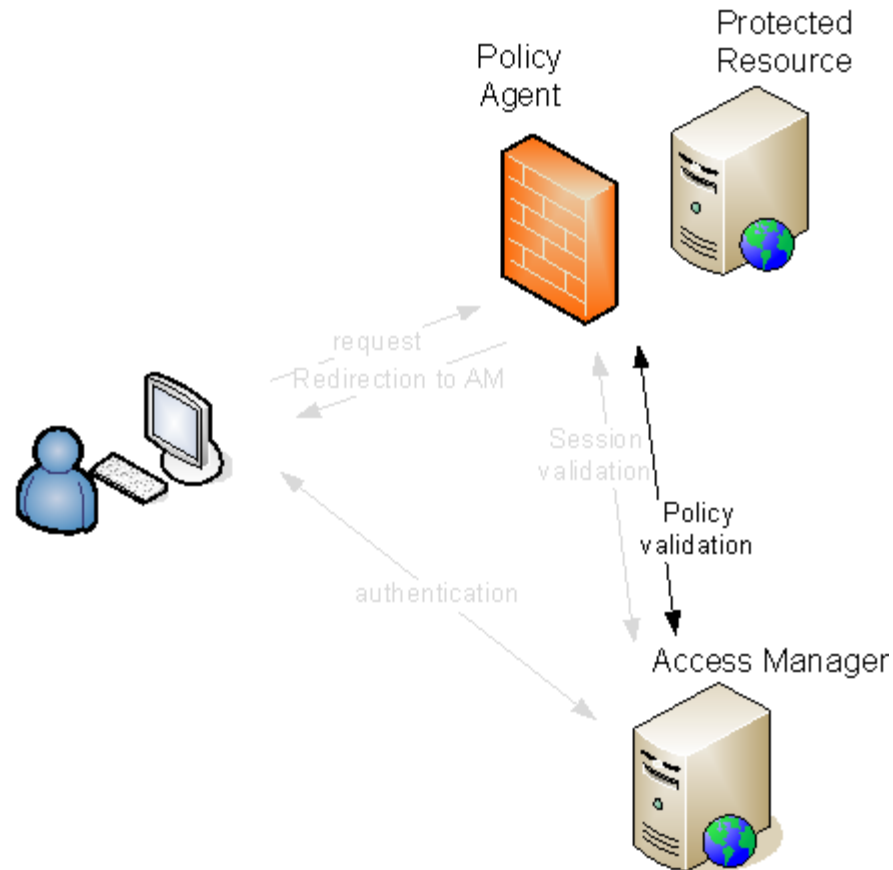
SSO and Policy Enforcement #2



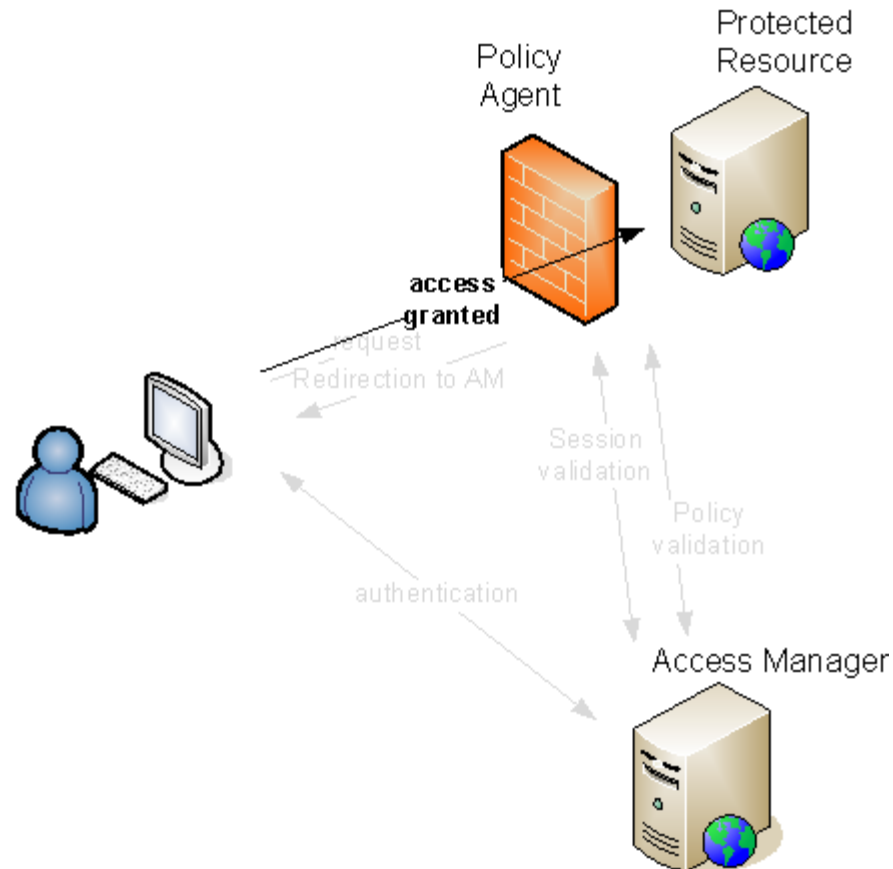
SSO and Policy Enforcement #3



SSO and Policy Enforcement #4



SSO and Policy Enforcement #5



[Solutions...](#)

Federated Access Management @ the University of Guelph

- Currently participating in edupass.ca (formerly CIMF)
- Components of federation so far:
 - Identity Provider - production date early June.
 - Service Provider – one test service provider, not part of edupass.ca yet.

Our Environment – Identity Provider

- Running RedHat AS v4 on a virtual machine.
 - JDK 1.6, Apache 2.0.x, Tomcat 5.5.x, Mod_jk 1.2
 - Shibboleth IdP 1.3.3
- VMware provides highly redundant environment, automatic failover, clone vm for cold standby, and ability to increase resources if needed.
- Authentication done by Sun Access Manager.
- Direct attribute querying via LDAP.

Challenges

- Getting buy-in to project – allocating time and resources.
- Technology issues – understanding how all the pieces fit together. Lack of service providers to test with.
- Integrating IDP with Access Manager and solving attribute handling issues.
- Determining policy around eduPerson attributes.
- Finding suitable services to become service providers.
 - Dedication of resources from service owners

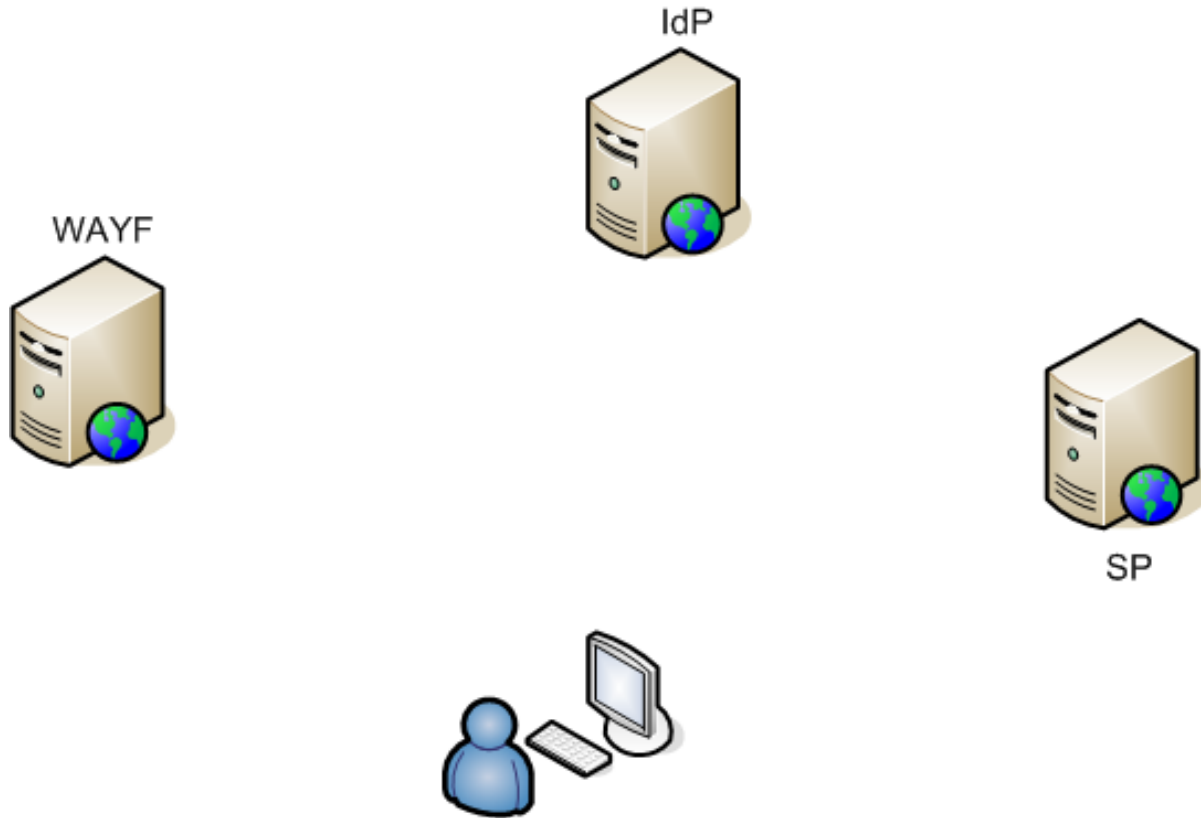
Future

- Investigating potential service providers:
 - ExLibris application for our library.
 - Office of Research interested in using federation to collaborate with other Universities for research projects.
- Full monitoring of Identity Provider in BigBrother
- Integration toolkits? – similar to WAM integration toolkits.

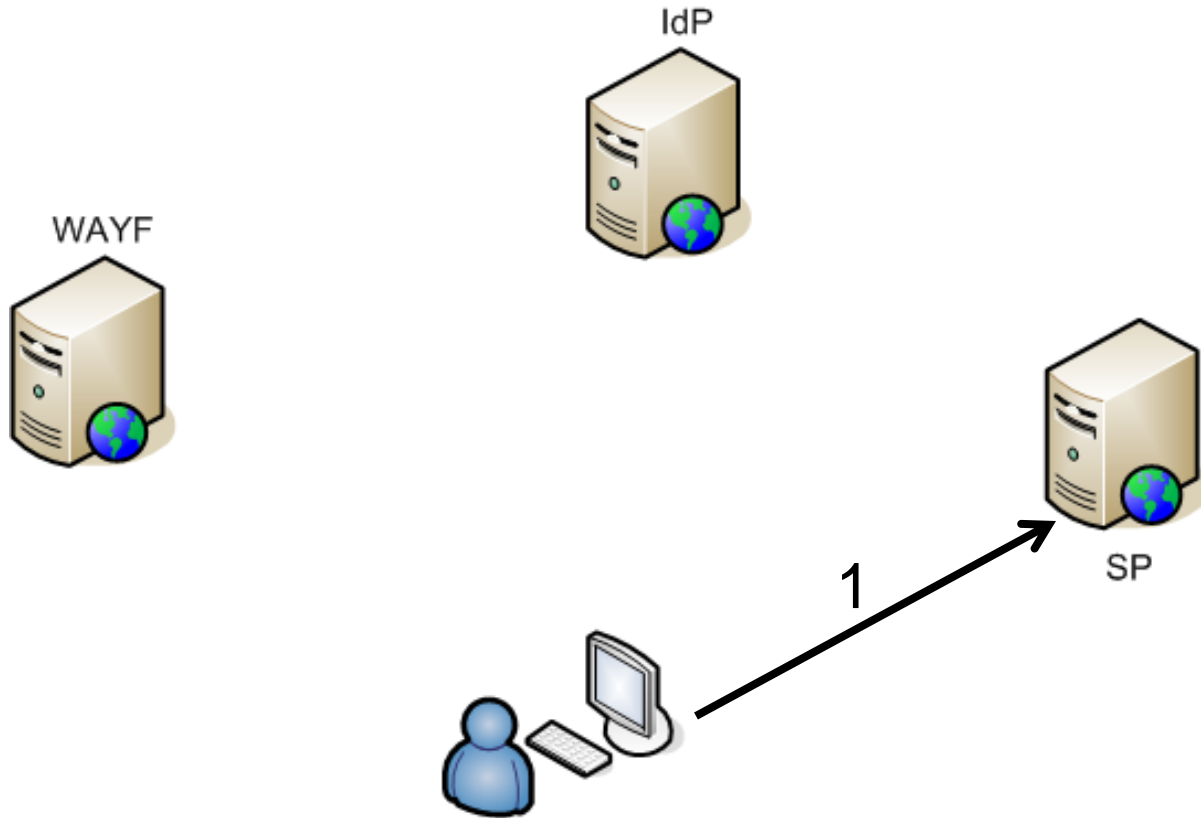
Future (Cont'd)

- Sun coming out with Federated Access Manager (FAM) in September. It's supposed to work with many of the other federation technologies.
 - Can it replace the direct LDAP queries for attributes?
 - Will it work with edupass.ca, which is a Shibboleth 1.3.x (SAML v1) federation?

Federation - How it works?

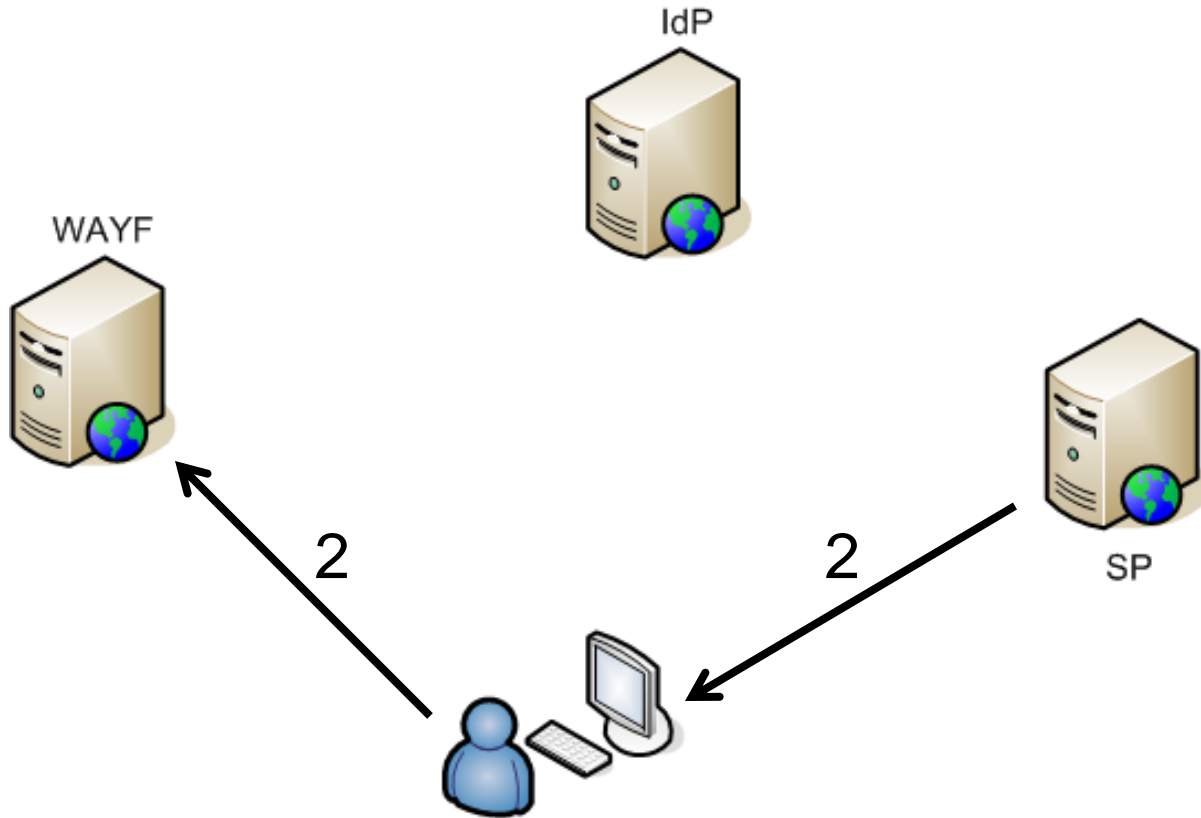


Federation - How it works?



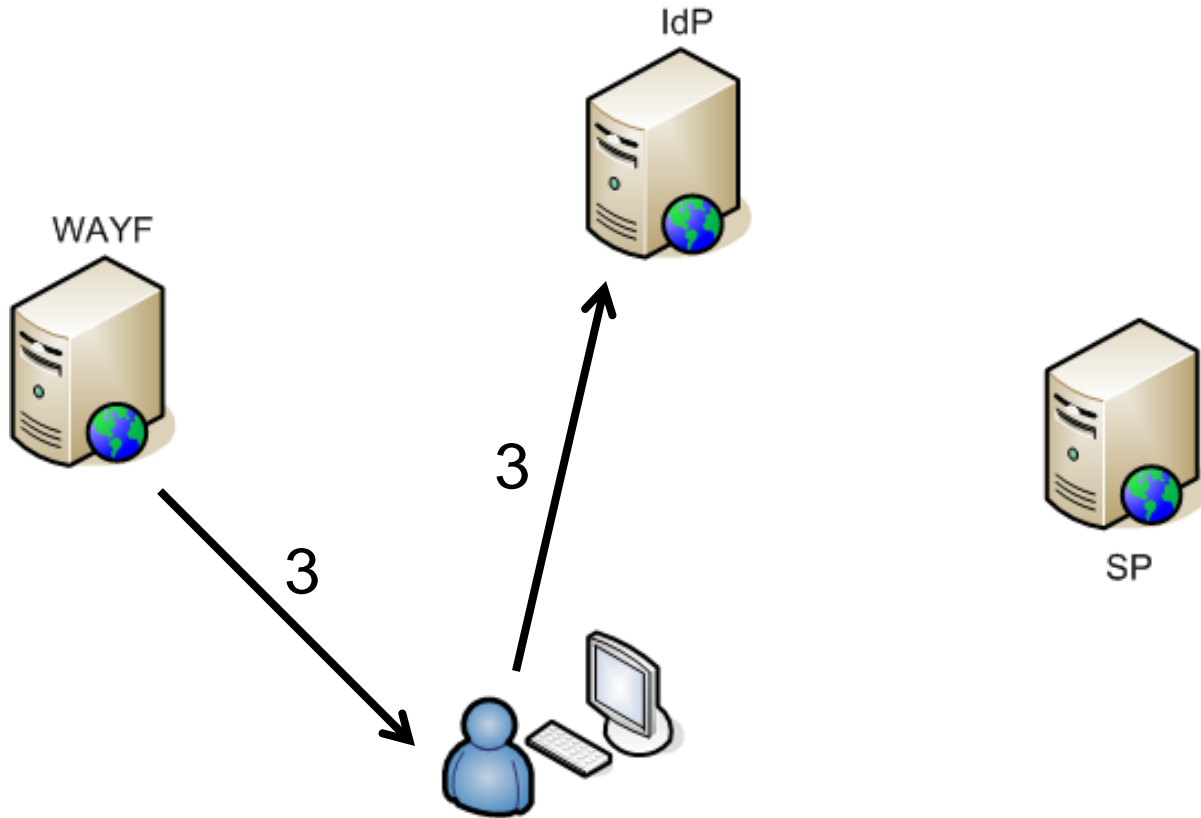
1. User navigates to service provider.

Federation - How it works?



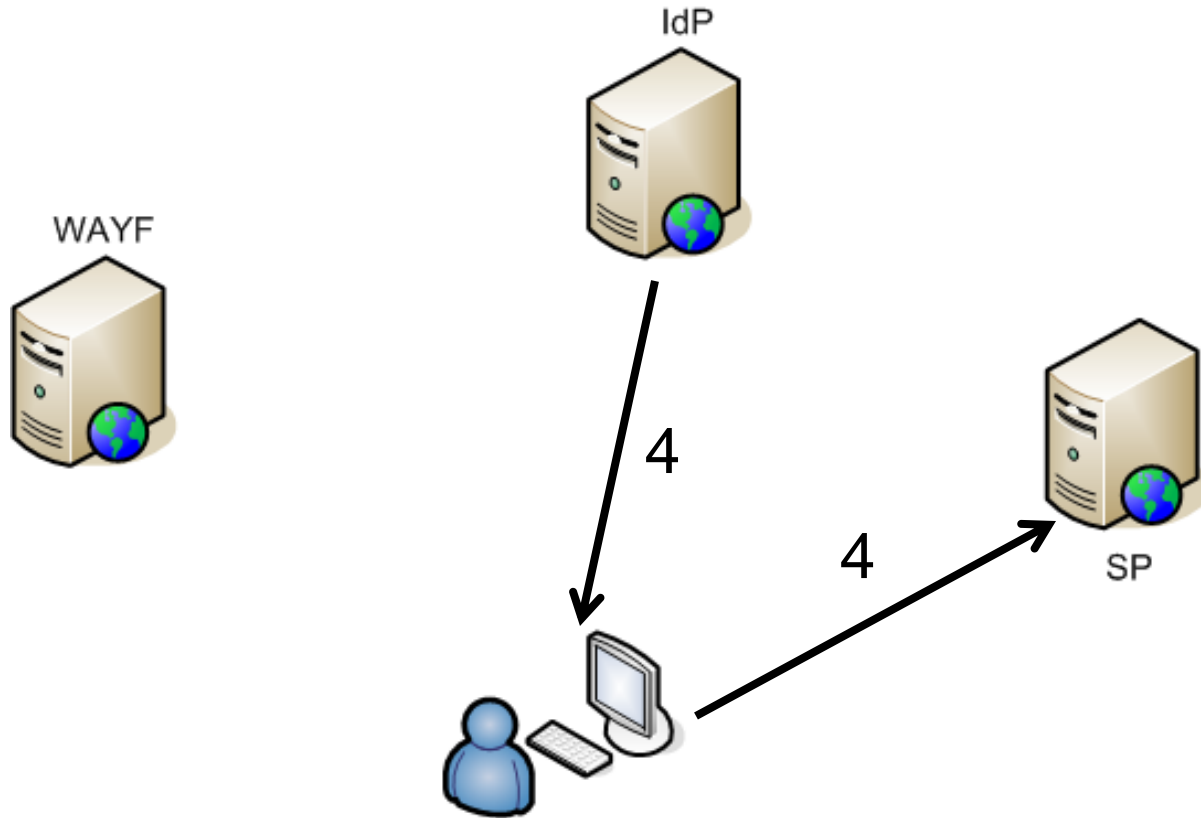
2. SP redirects user's browser to WAYF server.

Federation - How it works?



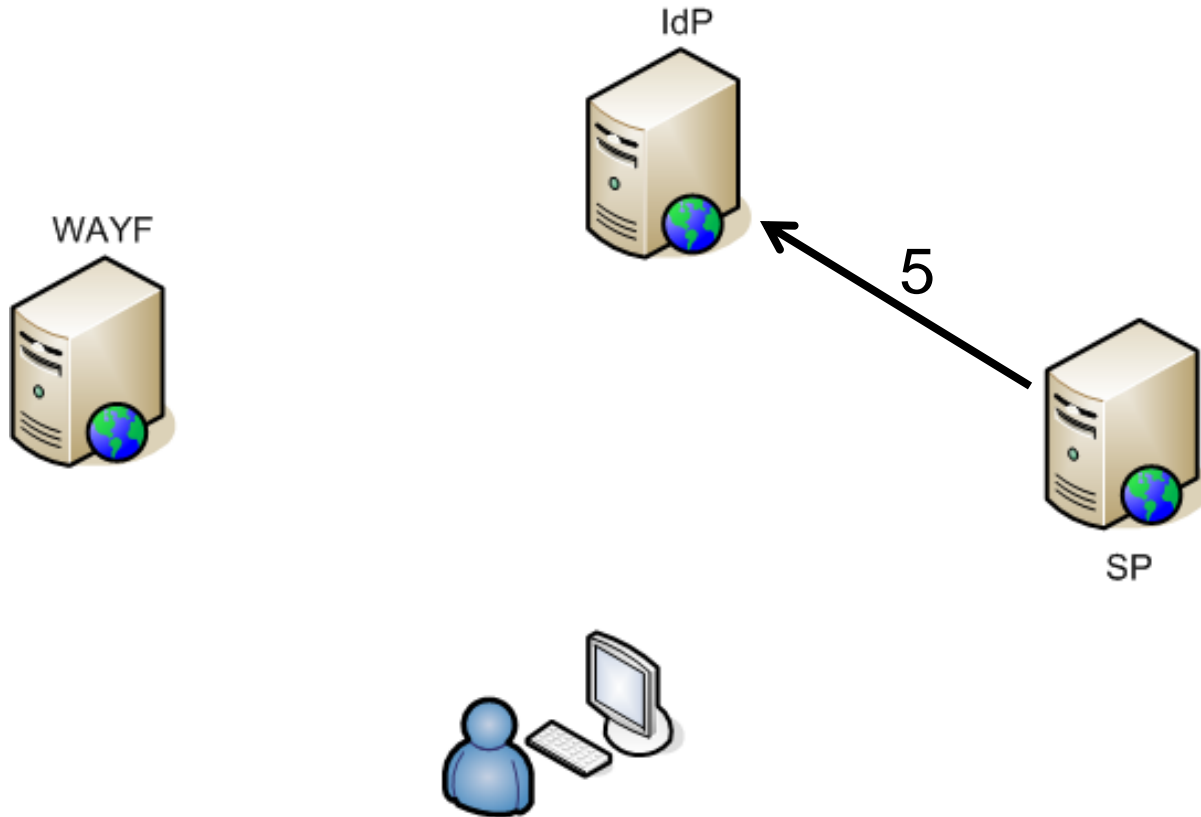
3. WAYF redirects user's browser to the idp of the institution the user selected.

Federation - How it works?



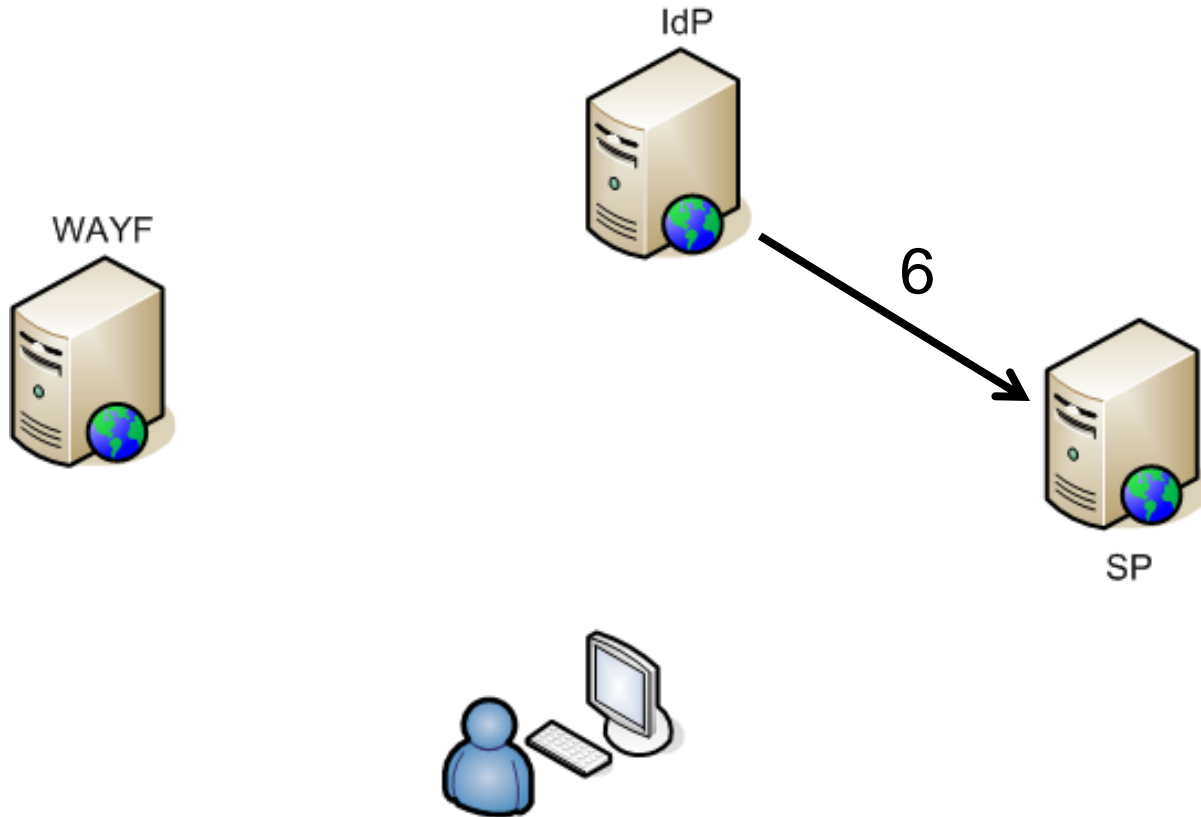
4. After successful authentication, IdP redirect's user's browser back to SP.

Federation - How it works?



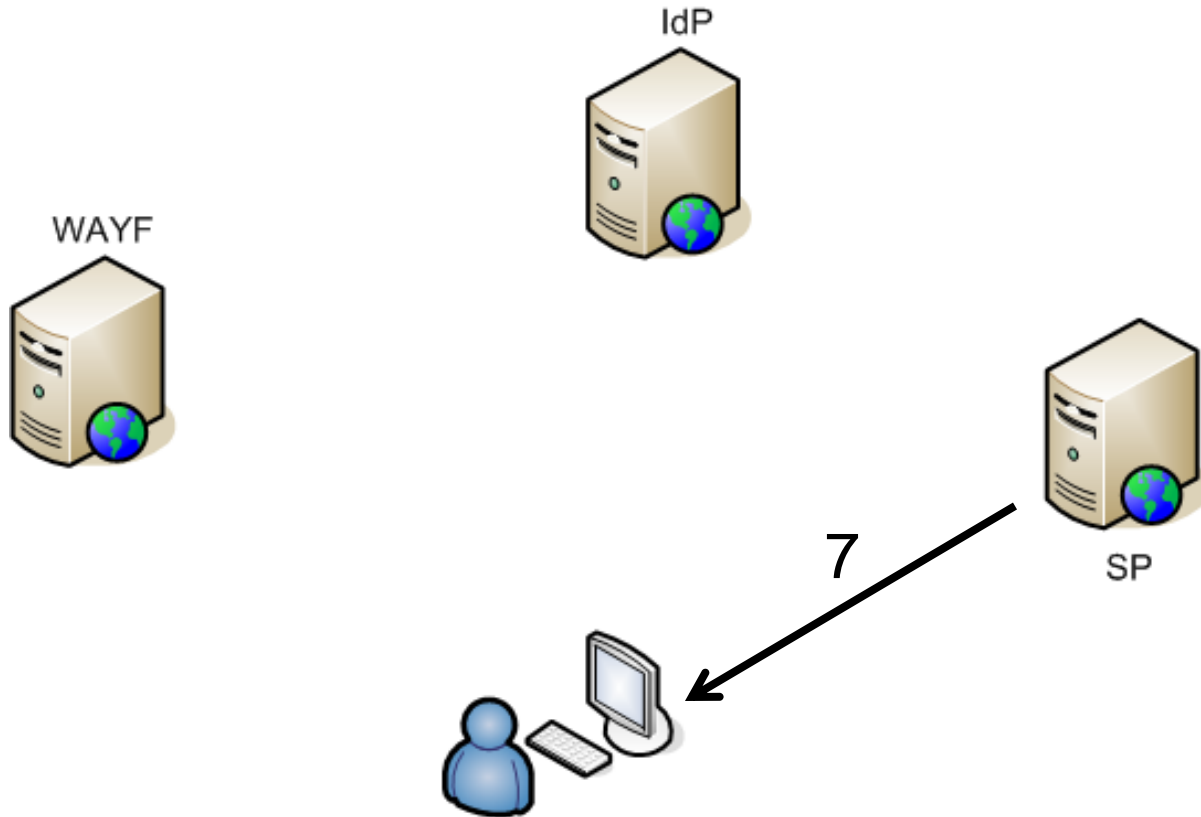
5. SP queries IdP and asks if there are any attributes for the authenticated user.

Federation - How it works?



6. IdP returns any of the attributes about this user that the SP is allowed to see.

Federation - How it works?



7. SP serves the original request to the user.

Summary & Questions?

- Challenges, Goals, and Solutions
- Implementation of AM and IdP
- Integration examples and toolkits provided
- Lessons learned

Contact info:

Zdenek (AM & WAM) – znejedly@uoguelph.ca

Matt (FAM) – msearle@uoguelph.ca