

# **Federated CI Collaboration**

---

**Gordon K. Springer**  
**CS & MUII Depts, DoIT, UMBC**  
**University of Missouri**

**GPN 2010 Annual Meeting**

**Kansas City, Missouri**  
**June 3, 2010**

---

# Overview

---

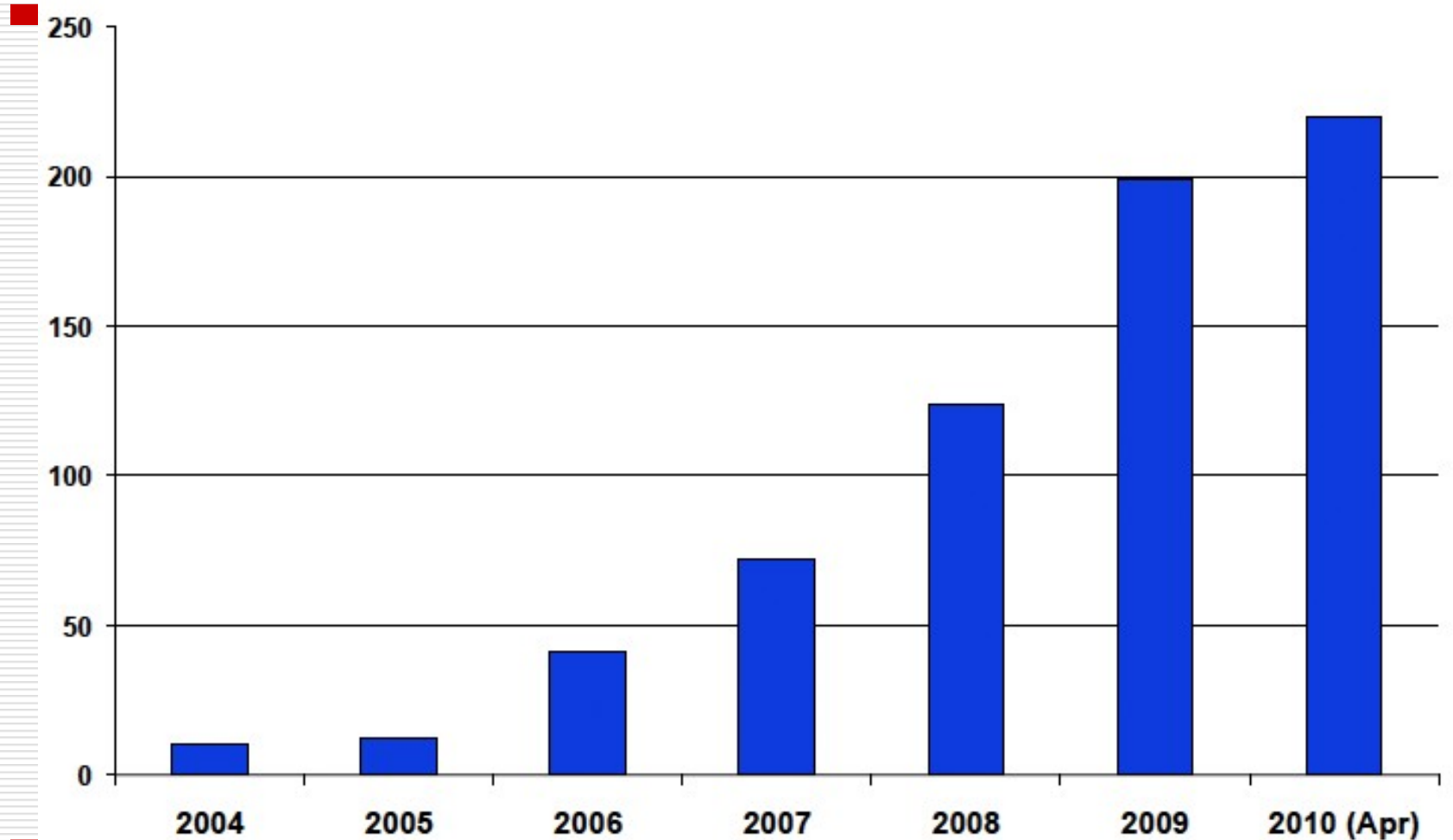
- Update on Federations
  - InCommon & NSF
  - JASIG/CAS, Kuali, aegisUSA and others
- Shibboleth in the GPN
  - Protocol Review
  - Advantages and shortcomings
  - Recent Entitlement Server Advances
- Conclusions

# InCommon Updates

---

- As of June 30<sup>th</sup> support for Shibboleth IdP 1.3 will expire and version 2.0 will be the standard. Just a FYI.
- The following slides are taken from updates provided at the I2 SMM in April.

# InCommon Participants Year-by-Year



# InCommon Growth

---

- 53 Organizations have joined since the Fall MM update: 32 percent growth.
- 4.5 million end users: faculty, staff, students
- ~120 Internet2 University Members are not InCommon Participants
- Adding new certificate service – (See Rob's talk)



# InCommon@NSF

Ardoth Hassler

Senior IT Advisor

National Science Foundation

Associate Vice President

University Information Services, Georgetown University

Spring 2010 Internet2 Member Meeting

April 27, 2010



# Overview

- **Update on InCommon at NSF**

InCommon is working to create and support a common framework for trustworthy shared management of access to on-line resources in support of education and research in the US.

- **Background on Research.gov and InCommon**

Led by NSF, Research.gov enables organizations and researchers to access streamlined research grants management services and other resources for multiple federal agencies in one location.



# What will NSF customers be able to do?

## ▪ **Research.gov**

- Login with credentials issued by their home institution (Bronze; LOA1)
- View proposal status
  - NSF
  - USDA/NIFA
  - DoD/Army Research Office
  - More in progress
- Create and submit Federal Financial Reports to NSF
- Maintain their user profiles
- And much more to come in time...



## ▪ **FastLane**

- Login with credentials issued by their home institution (Bronze)
- Access and use current PI/Co-PI suite of functions
- Perform research administration
- Use proposal and award functions





# Status of Pilot

- Demonstrated “proof of concept” with Ohio State University
  - Complete (fall 2008)
- Pilot Phase (in progress)
  - Pennsylvania State University
    - Technical staff testing: complete 11/2009
    - Sponsored Projects staff and faculty researchers complete: 1/2010
  - University of Washington
    - Technical staff testing complete 11/2009
    - Sponsored Projects staff and faculty researchers complete 3/2010
  - University of California-Davis
    - Testing started
- Pending
  - Colorado State University
  - Georgetown University

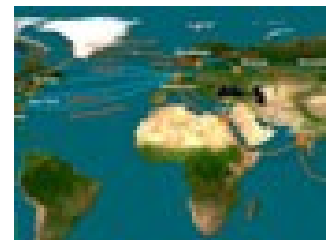




# What will NSF customers be able to do?

## ▪ External Wiki

- Collaborate with members both internal and external to the agency (task forces, etc.) similar to Internet2 Wiki
- Set this up for groups of specific members or use self registration
- Pilot coming soon...



# IAM Online

---

- Monthly presentations on identity and access management
- Presentations cover introductory identity and access management, hot topics, and advanced issues
- Next session – June 10<sup>th</sup> – Handling Affiliate Populations
- In cooperation with EDUCAUSE
- Support by InCommon Affiliates Unicon and AegisUSA

[www.incommon.org/iamonline](http://www.incommon.org/iamonline)

---

# CAMP and Advance CAMP

---

Conferences focused on federated identity and access management.

**CAMP: Exploring and Supporting Federated Access**, June 21-23, Raleigh, North Carolina

- Technical and management sessions
- Organizations new to InCommon or already in production

**Advance CAMP: The Second Identity Services Summit**, June 23-25, Raleigh, North Carolina

- Working together to align IAM approaches

[www.incommon.org/camp](http://www.incommon.org/camp)

# Other IdM Systems/Services

---

- ❑ **Central Authentication Service (CAS)** - CAS is an authentication system originally created by Yale University to provide a trusted way for an application to authenticate a user.

[www.jasig.org](http://www.jasig.org)

- ❑ **Kuali** – Developing a collaborative model for delivering open source enterprise-scale software for higher education -

[www.kuali.org](http://www.kuali.org)

- ❑ **aegisUSA** – Consulting on IAM -

[www.aegisusa.com](http://www.aegisusa.com)

---

# Shibbolith and the GPN

---

- ❑ Interconnected computing resources, data repositories, research tools and information sources may be widespread
- ❑ Research institutions develop research projects that access and share computing, information and research resources belonging to various other institutions, forming virtual organizations (VOs)

# Key Issues

---

## □ Authentication

- The process of establishing if an entity (e.g., user, service) is the entity that they claim to be
- Usernames and passwords, public and private keys, smart cards combined with some type of knowledge possession (e.g., answering a question presumably answerable only by the entity)

## □ Authorization

- The process of determining, *after* an entity is authenticated, if they are allowed to have access to a particular resource
- Authorization always implies the existence of a previous authentication

# Group Membership vs Individual Credentials

---

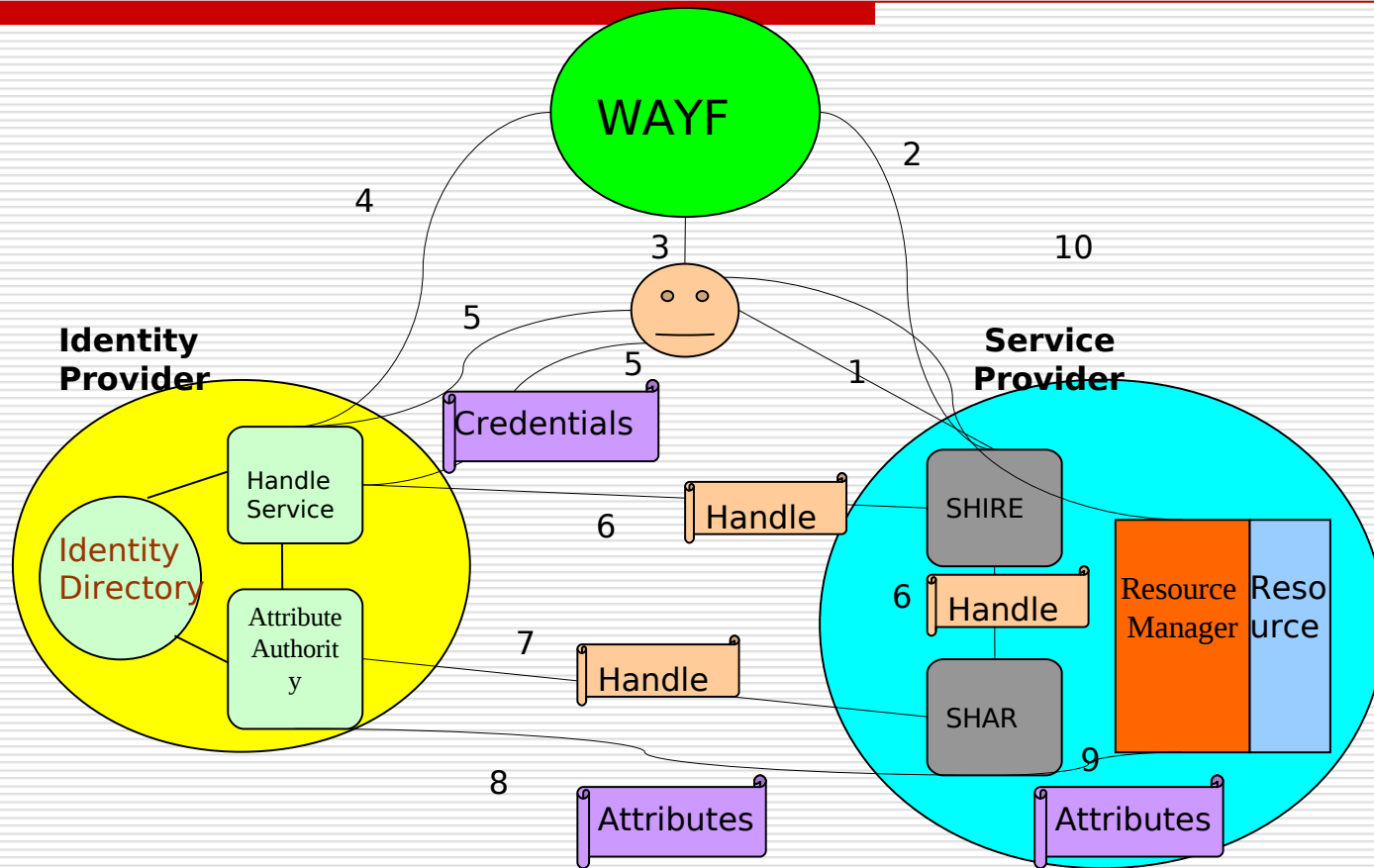
- ❑ Individual credentials: each entity needs to have a username and a password for every shared resource
- ❑ Group membership: is described by attributes, such as “student”, “manager”, “enrolled in CS 1001” or “member of the GPNVO group”

# Shibboleth Components

---

- An *identity provider* represents the Shibboleth entity that authenticates a user and answers attributes inquiries from the service provider
- A *service provider* represents the Shibboleth entity that communicates with the user, the user's identity provider at their home institution, and makes the access control decision based on the user's attributes
- A *Where Are You From (WAYF)* service is an independent service operated by a virtual organization. Its purpose is to identify a user's home institution and to redirect the user to the home institution's authentication system

# Shibboleth Protocol



# Attributes of Group Membership

---

- Attributes are a central part of the Shibboleth architecture as they provide the group membership information
- An attribute is a name - value pair
- Attributes are stored in the identity provider
- **We have two types of attributes: institution related attributes and virtual organization related attributes**
- An entitlement is an attribute value that allows a user access to a specific resource or group of resources

# Where to put the VO Attributes

---

- ❑ No IdP will allow VO attributes in their identity DB; nor should they allow them.
- ❑ Decisions on access should be left to the SP and not the IdP.
- ❑ A VO may cross many institutional boundaries and may not even be associated with an institution, so how do these VOs avoid separate silos with overhead to maintain separate identities?
- ❑ Solution: a separate Entitlement Server that is trusted, scalable, and with distributed management from VO authorities rather than institutional authorities. Examples include things like iTunes, Dreamspark, and similar academic and non-academic services.

# The Entitlements Repository

---

- Defines, manages and uses virtual organization (VO) entitlements that do not refer to any particular user or institution
  - They encompass the idea of a shared resource that needs to be made available to any entitled entity from any member organization
- Allows refined authorization for any virtual organization

# The Entitlements Repository

---

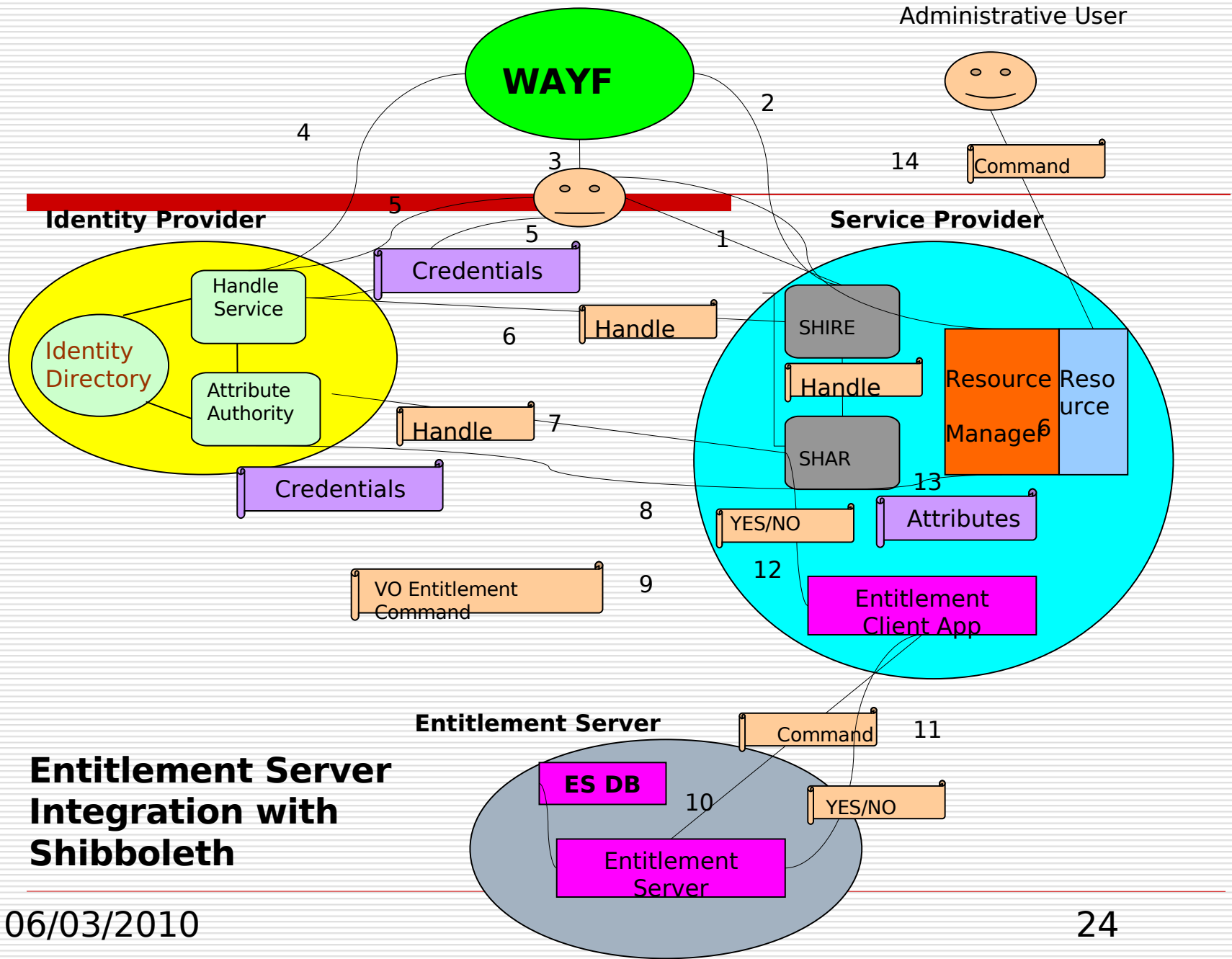
- Separates the VO entitlements (“member of the GPNVO group”) from institution related entitlements (“faculty”)
- The entitlements repository maintains the VO entitlements separately from the institution entitlements maintained in the identity provider
- The entitlements repository gives the virtual organization decision power over its own entitlements

# The Fine-Grained Authorization Design

---

- ❑ The identity provider is in charge of authenticating the users
- ❑ The service provider is in charge of the authorization decisions
- ❑ The entitlements repository is in charge of defining, managing and providing access for VO entitlements queries and updates

*The identity provider, the service provider and the entitlements repository jointly provide for creating a secure and robust collaboration environment for use by any VO.*



# Conclusions

---

- ❑ The entitlement repository and the prototype implementation facilitates secure and robust collaboration between groups of research institutions
- ❑ The entitlement repository provides for refined access control decisions at the service provider
- ❑ The entitlement repository allows the infrastructure of the virtual organization to control its VO entitlements
- ❑ The entitlement repository is a complement to the identity provider

# Recent Advances with ES

---

- A fault tolerant ES service has been created to permit reliability and scalability in a distributed environment.
- Users at institutions without a compatible IAM system or independent individuals with verifiable X.509 certificates (e.g., DoE/OSG certificates) can be authorized to participate in the VO collaborative environment.
- The next two talks by Singh & Shirole will discuss these advances.

