Identity Management and Attributes in GENI

Tom Mitchell

GEC 11

July 26, 2011

Sponsored by the National Science Foundation

Agenda

- Identity Management 101
- Review GEC 10 Community Agreement
- Review GEC 10 Next Steps
- Identity Portal Status
- Identity Portal Demonstration
- Next Steps

Identity Management For GENI

- Why add external identity providers to GENI?
  - Using external identity providers can make it easy for experimenters to access GENI. They use existing accounts for authentication.
- Why join the InCommon Federation?
  - There are over 200 Higher Education Participants in the InCommon Federation
  - Many potential GENI experimenters already have InCommon accounts
- How does GENI benefit?
  - More experimenters can gain access to GENI

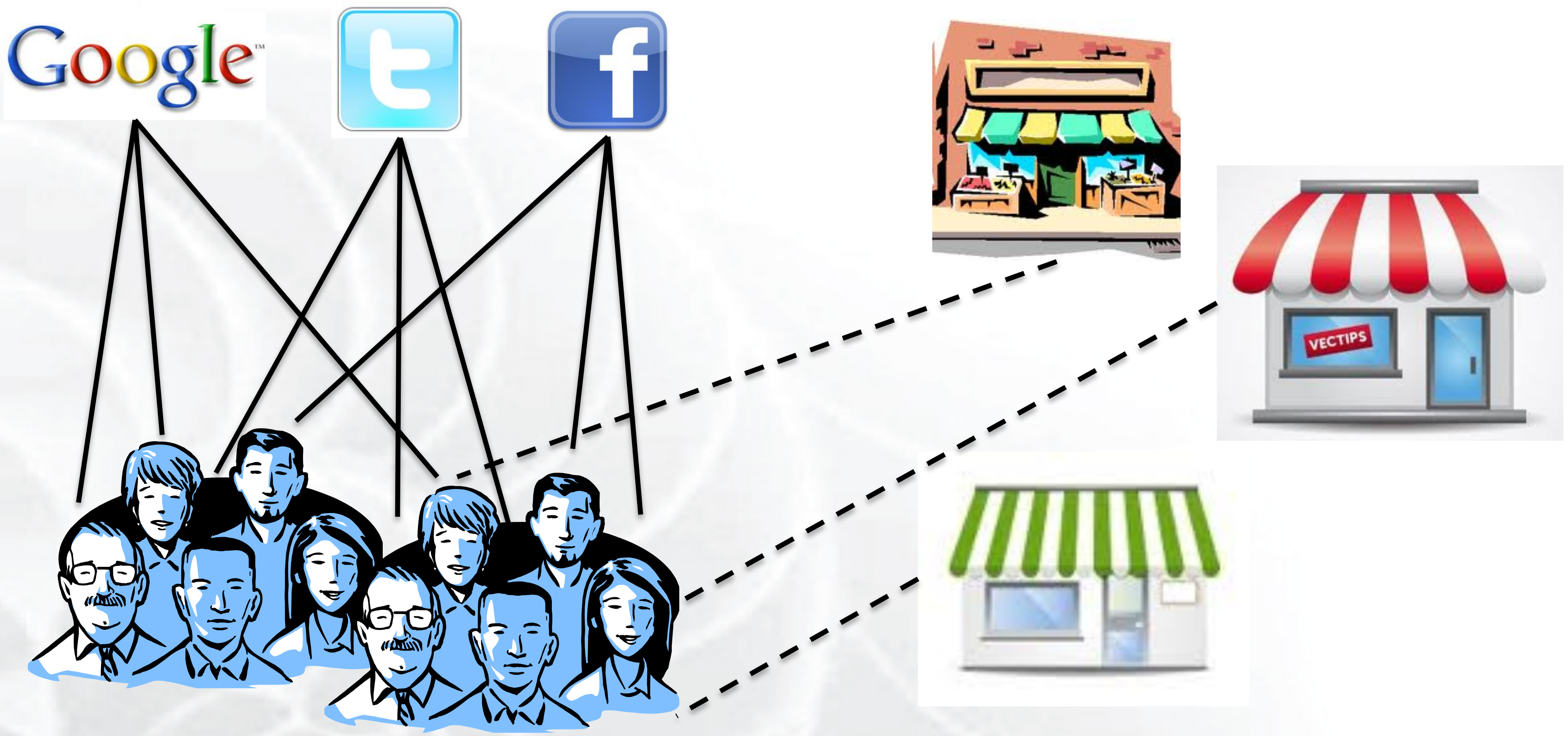
Identity Management 101

- Web-based Single Sign On (SSO)
- Lots of examples you may already be familiar with:
  - Google (OpenID)
  - Yahoo! (OpenID)
  - Facebook (OAuth)
  - Twitter (OAuth)
- These are all examples of Federated Identity

Identity Management 101

Connecting People With Services

Identity Providers **Service Providers**



Identity Management 101

Identity Providers

- Manage
  - Accounts
  - Passwords
  - Attributes
- Assert
  - Authentication
  - Attributes
- Trust Service Providers
- Examples:
  - Google, Yahoo, Facebook Twitter
  - Your College/University

Service Providers

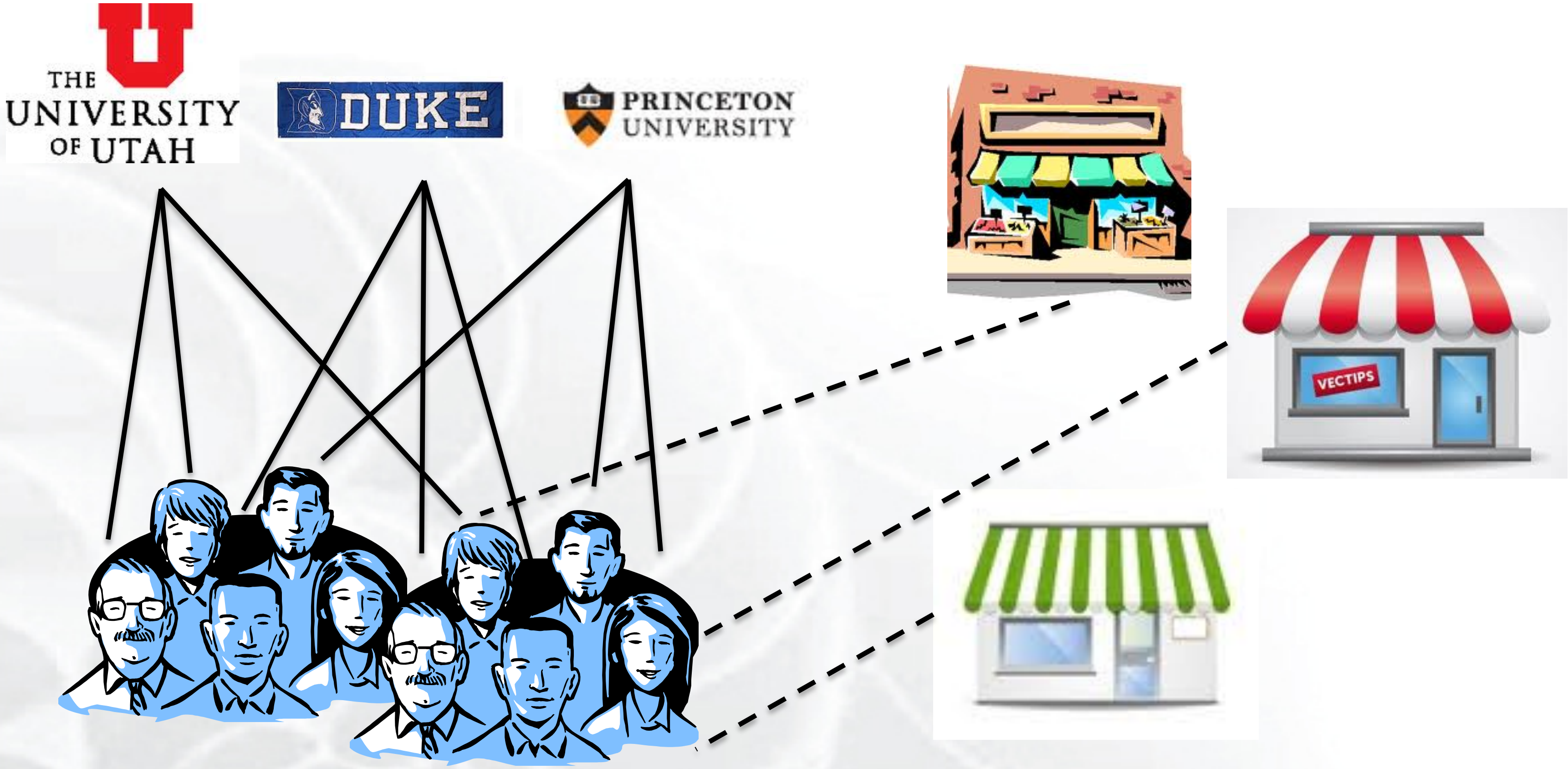
- Provide services
- Outsource password management
- Trust Identity Providers
- Examples:
  - CNN.com (Facebook)
  - ESPN.com (Facebook)
  - TypePad (Google, Yahoo, Facebook, Twitter, etc.)
  - Washington Post (Facebook)
  - twitpic.com (Twitter)

Identity Management 101

InCommon®

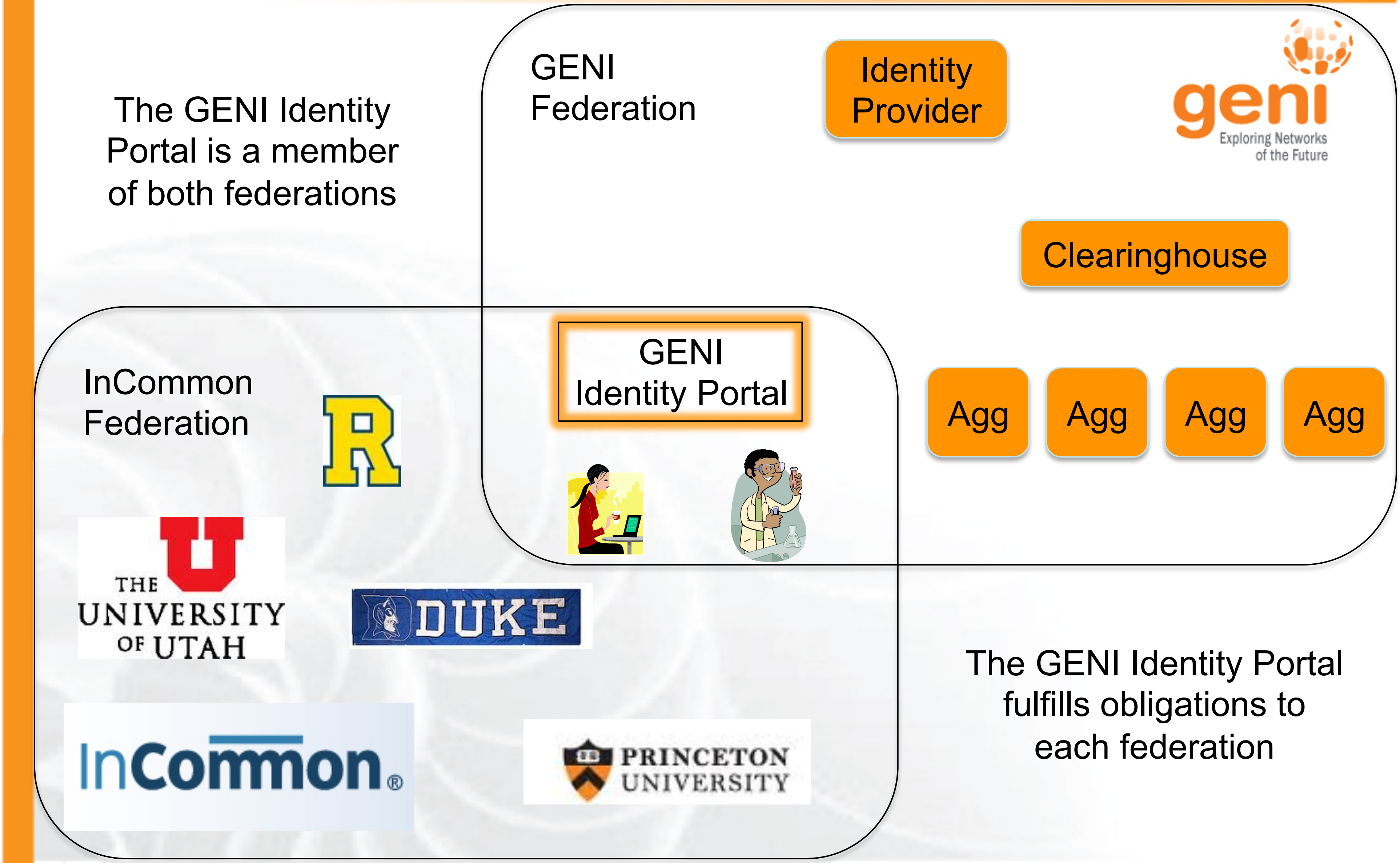
Identity Providers

Service Providers



Bridging Federations

The GENI Identity Portal is a member of both federations



GENI Federation

Identity Provider

Clearinghouse

Agg

Agg

Agg

Agg

GENI Identity Portal

InCommon Federation

The GENI Identity Portal fulfills obligations to each federation

Bridging Federations

- The GENI Identity Portal:

InCommon

  - Acts as an InCommon Service Provider
  - Gets experimenter attributes from InCommon identity providers through SAML assertions

GENI

  - Acts as a GENI slice authority
  - Generates GENI-compatible user certificates
  - Generates GENI-compatible slice credentials

GEC 10 Community Agreement

- Add external identity providers to GENI
- GPO should build a prototype, InCommon compatible, GENI identity portal / slice authority
- Agreed on an initial set of required identity attributes
  - Name
  - Institution
  - Affiliation
  - Email address
  - Phone number

GEC 10 Next Steps

- GPO will build a prototype portal / slice authority that accepts InCommon logons and produces slice credentials
  - ✓ – Build a portal
  - ✓– – Become an InCommon service provider
  - – Work with a few test institutions to get desired attributes from their identity providers
  - ✓ – Federate with a few GENI Aggregates
- Demonstrate this portal at GEC11
  - – Pending group evaluation, expand this portal to other institutions and aggregates

Status: Build A Portal

- Prototype GENI Identity Portal implemented
- Integrated with Shibboleth for InCommon compatibility
- Produces GENI-compatible certificates and credentials
- Home-grown PHP web site
  - Still investigating toolkits like CoManage, Drupal, etc.
- Demo in a few minutes

Status: InCommon Membership

- GENI Project Office became a member of the InCommon Federation on July 13, 2011

- GENI is part of a new category of InCommon Membership: Research Organizations
  - One of 12 “Government and Nonprofit Laboratories, Research Centers, and Agencies”

Status: Federate With Institutions

- We are just starting this process
  - Now that we are members of InCommon we can begin
- Negotiate With Institutions For Attributes
  - Anonymous attributes are readily available but…
  - GENI needs a few identifying attributes
    - Name, email, phone
- Planning to work with a few institutions at first, then add more

Status: Federate With GENI Aggregates

- Temporarily federated with a few ProtoGENI aggregates

- Federating with more aggregates should be easy, it is a simple matter of trust

- The portal looks like a slice authority to GENI aggregates
  - Issues user certificates and slice credentials

DEMO

Agenda

- Identity Management 101
- Review GEC 10 Community Agreement
- Review GEC 10 Next Steps
- Identity Portal Status
- Identity Portal Demonstration
- Next Steps

Next Steps: InCommon

- Publish Participant Operational Practices (POP)
- Publish Service Provider Metadata
- Negotiate For Attributes From A Few Institutions
  - Anonymous attributes are readily available
  - GENI needs a few identifying attributes

Next Steps: Identity Portal

- What's missing:
  - Proper certificate management – outsource or build?
    - Protected signing key
    - Certificate Revocation List (CRL)
  - Programmatic access to Slice Authority functions
  - Programmatic access to Registry functions
  - Management/Operations integration
    - Publish monitoring data
    - Tie into GENI operational infrastructure
  - Slice expiration
  - Projects, Groups, Sharing Slices
  - Etc.

THE END.