# Working Groups Report: Making Federation Easier

## IAM Online
## February 11, 2015

Steve Carmody, Brown University

Janemarie Duh, Lafayette College

Eric Goodman, University of California, Office of the President

Keith Hazelton, University of Wisconsin – Madison

Jim Jokl, University of Virginia

David Walker, Internet2

*Brought to you by Internet2's InCommon in cooperation with*
*the Higher Education Information Security Council*

# What is the Technical Advisory Committee (TAC)?

- InCommon governed by Steering Committee (http://www.incommon.org/about.html)

- Two Advisory Committees
  - TAC - Technical
  - Assurance - oversight body of the InCommon Identity Assurance Program

# Doing the Work

- TAC develops a work program
    - Invites community review and comment

- TAC Charters Working Groups
    - specific deliverables and target dates
    - draws membership from the InCommon community (there are open calls for participation)
    - WGs deliver reports to the TAC
    - reviewed, approved, forwarded to appropriate place for action (TAC, Steering, InCommon operations, etc)

# You can help!

Participate in Working Groups!

Make sure your problems are addressed!

Establish relationships

Move the community forward

# 2014 Working Groups - Context

## Extend the Boundary

- Making Federation Easier to Implement
- New communities in the US -- QUILT
- Worldwide -- eduGAIN
  - http://www.geant.net/service/eduGAIN/Pages/home.aspx
- Other Authentication Domains - Social

# 2014 Working Groups - Context

## Making Management Easier

- Creating IDP/SP Policy based on various factors
  - Who Registered other party
  - Policies of other party

# Today’s Agenda

1. Alternative IdPs Working Group
2. External IdP Working Group
3. IdP of Last Resort Working Group
4. New Entities Working Group

# A Big Thank You!

## Working Group Chairs

Janemarie Duh, Lafayette College

Eric Goodman, Univ. of California Office of the President

Keith Hazelton, University of Wisconsin - Madison

Jim Jokl, University of Virginia

# A Big Thank You!

To all the the Working Group members!

Without you, there would be no reports today and we would not be moving the community forward!

# Identity Provider Strategies for Common Campus Environments

Alternative Identity Providers Working Group

Janemarie Duh (Lafayette College), Chair

# Alternative Identity Providers

## Goal

- Increase the number of campuses that operate an IdP so that they can federate

## Problem

- Some campuses perceive barriers to setting up an IdP

## Approach

- Provide solutions for institutions that do not have the expertise and resources to operate a Shibboleth IdP locally

# Alternative IdPs: Considerations

- A locally-run Shibboleth IdP provides a campus with the best capability and flexibility
- May be a more appropriate solution based on
  - Computing environment (Java, LAMP, Active Directory)
  - Available resources and expertise
  - Strategy to in-source or outsource infrastructure
- Careful consideration of current and future needs

# Alt IdPs: Assessment Criteria

Fact finders assessed strategies against a set of criteria and wrote detailed summaries

Technical support for

- InCommon’s Recommended Technical Basics for IdPs
- Attribute release
- Entity categories (R&S)
- Multiple authN contexts for MFA and assurance
- Enhanced Client or Proxy (ECP)
- User consent

# Alt IdPs: Assessment Criteria

Operational criteria

- Expertise required
- Resources required
- Upkeep and feeding
- Applicable environments
- Pros/Benefits
- Cons/Risks

# Alt IdPs: Applicability of Strategies

Technical offerings for in-house environments

- Java-capable with Linux affinity : Shibboleth
- Microsoft/AD-centric : ADFS
- LAMP-capable : SimpleSAMLphp

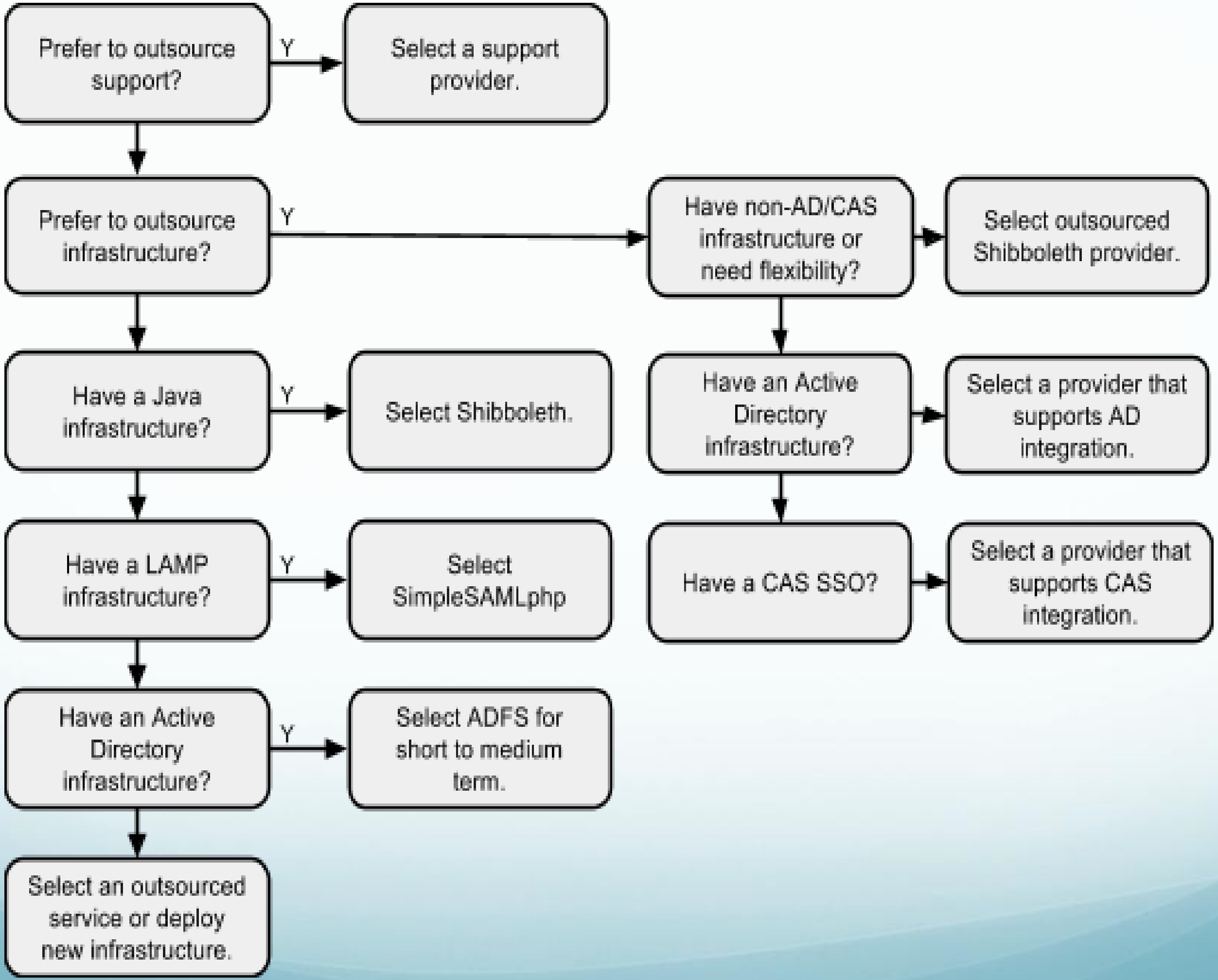
# Alt IdPs: Applicability of Strategies

Currently available outsourced services

- Shibboleth or vendor proprietary IdP
- “Gateway” IdP for Google Apps for Education or CAS environments
- In-sourced IdP with vendor support

State systems

- Hub and Spoke (i.e., centralized IdP with local authN)



Prefer to outsource support?

Select a support provider.

Prefer to outsource infrastructure?

Have non-AD/CAS infrastructure or need flexibility?

Select outsourced Shibboleth provider.

Have a Java infrastructure?

Select Shibboleth.

Have an Active Directory infrastructure?

Select a provider that supports AD integration.

Have a LAMP infrastructure?

Select SimpleSAMLphp

Have a CAS SSO?

Select a provider that supports CAS integration.

Have an Active Directory infrastructure?

Select ADFS for short to medium term.

Select an outsourced service or deploy new infrastructure.

# Alternative IdPs: Prerequisites

Required for any strategy

- Management of the service and the vendor even in outsourcing
- Operation of an IAMS
- IdM policy
- Governance

# Alternative IdPs

Alternative IdPs Working Group Wiki

- Final report
- Strategies and assessment criteria grid

https://spaces.internet2.edu/display/altidp/Home

# External Identities Working Group

Documentation:

https://spaces.internet2.edu/diplay/EXTID/Home

Mailing List: external-id@incommon.org

Meetings: Alternating Thursdays 12PT/3ET

# What is an External Identity?

- An identity asserted by an external authenticator

- Often implies Identities provided by an authenticator that is not a higher ed institution or not part of InCommon
  - Google, Facebook, Amazon, Comcast, etc.
  - External IDs of this type are the primary focus of the working group

# What is the External  IDs group?

- Follows on the work done by the Social IDs workgroup
- Goals focus on providing specific implementation recommendations:
  - Models for using external identities in a variety of risk profiles
  - Technical components to make external identities useful across a broad array of services
  - Account linking between campus-issued account and external accounts
  - Understanding differences between external identities and local identities

# Work done so far

- Use Cases (updating Social ID work)
- Use Case Categorization
- Account Linking Approaches
- Risks/Concerns of Using External Identities
- Criteria for Evaluating External Identity Provider

# Planned Output

White paper/report addressing:

- Types of External Identities
- Common Use Cases for External IDs
- Integration Approaches
- Recommendations
  - Selecting an Integration Approach for a given Use Case
  - Criteria for selecting External Identity providers
  - Addressing/mitigating identified risks/concerns
- Additional info
  - Evaluation of common External Identity providers (against common criteria)

Drafting process may uncover other areas to address.

# IdP of Last Resort Working Group

Documentation:
https://spaces.internet2.edu/display/IDPoLR/Home

Mailing List: idpolr@incommon.org

# Who needs an IdP of Last Resort?

- Research Service Providers (SPs) often find that the population they want to serve includes some individuals
  - Who are not represented by campus-based or other institutional Identity Providers (IdPs)
  - Or whose organizational IdP refuses to release attributes necessary for the operation of the SP
- Ideally in those cases such individuals could be directed to register with a participating IdP that
  - offered no-cost, easy registration processes
  - Released the standard required set of “Research and Scholarship”  (R&S) attributes
  - Met other requirements common to R&S SPs

# Why ‘Last Resort’?

- We continue to believe that in general, users are best served by an IdP
  - associated with their home institution
  - whose practices support users’ needs across the various missions of the institution
  - The Alternative IdP WG is helping here by defining additional paths by which an institutional IdP service can be offered

- So we don’t want an IdP of Last Resort to be seen as a way for an institution to justify not standing up its own IdP

# IdPoLR Working Group Progress Report

- Documented IdPoLR requirements that come from Service Providers in the Research and Scholarship category https://spaces.internet2.edu/display/IDPoLR/Requirements+for+an+IdP+of+Last+Resort

- Evaluated potential services against the requirements

- Now drafting short and long term recommendations aimed at making a production IdPoLR service available

# IdPoLR vis-a-vis External Identities

- IdPoLR requirements that classic social (‘external’) providers and social-to-SAML gateways typically fail to meet:
  - Stable, non-reassigned eduPersonPrincipalName values
  - Support for SAML ECP (Enhanced Client or Proxy)
  - No commercial interest in user data

- The IdPoLR WG will be an avid reader of the External Identities WG final report to see if the above statement is invalidated by future findings

# DRAFT Recommended near-term path

- Case for near-term service roll-out
  - Some research service providers have a critical unmet need to enable all of their potential users to access their research sites and tools
  - There may be existing IdPs that can meet the essential requirements with relatively minor technical and organizational changes

- The WG recommends that if InCommon adopts the near-term path, it take concrete steps to work with the most promising IdP to help find the resources needed to close any gaps and provide the federation home for the IdP

# DRAFT Recommended longer-term path

- Whether or not InCommon accepts the recommendations for the near-term path they should independently evaluate a recommended longer-term path
  - A single IdPoLR would mean there is a single point of failure
  - InCommon should create a level playing field on which multiple IdPoLRs could co-exist
  - The level playing field could be fostered by
    - Defining an entity category for IdPs meeting the Research SPs requirements for an IdPoLR
    - Inviting candidate IdPoLRs to seek InCommon certification that they meet the requirements

# New Entities Working Group

Documentation:
https://spaces.internet2.edu/display/NewEntities/Home

# New Entities WG: Purpose

- The federation world is changing
  - We need to carefully consider how to manage the changes
  - Focus for this working group: deliver a set of recommendations for how to deal with non-traditional entities in the InCommon metadata.
- InCommon is a homogeneous collection of entities
  - Entities are generally R&E or provide services to R&E sites
  - All entities sign the InCommon Participation Agreement
- InCommon will become something more
  - Support for international collaboration
  - Other types of non-R&E entities
  - Entities that have not signed the InCommon Participation Agreement
- Challenge – how do we manage the transition?

# New Entities WG: Process

- Use Cases
  - Quilt Partnership – a set of use cases revolving around K12 participation in InCommon
  - Proxy Entities – aggregation of multiple services behind a single InCommon entity-id
  - Interfederation – the ability of users from one federation to be able to access services hosted on a second federation
  - eduGAIN metadata – how do we deal with interfederation metadata
  - LIGO - support for international research collaborations

# New Entities WG: Process

- For each use case, start by answering the questions:
  - What would an existing InCommon IdP want/need to know about the new type of entity in the metadata?
  - What would an existing InCommon SP want/need to know about the new type of entity in the metadata?
- Many months of discussion has brought the committee close to consensus on most points

# New Entities WG: Some Issue Highlights

- K12 Entities
  - Would some SPs need to know age information before they provide services to elementary school students?
- Interfederation Metadata
  - There is no InCommon Participation Agreement in place for these entities, what are they obligated to do with the data that I provide?
- Proxy Entities
  - How can I configure a reasonable attribute release policy when I don’t know what is consuming my data
- Subordinate Registrars
  - Organizations under contract to InCommon using InCommon processes
  - Organizations not using a delegated InCommon process

# New Entities WG: Status

- Overarching Principle:
  - There must be an *easy* mechanism for current InCommon entities to retain the existing InCommon behavior
    - We also need to make it easy for InCommon entities to use enhanced capabilities
- We discussed many ideas
  - Separate metadata aggregates
  - Combined metadata aggregate
  - Additional metadata entity attributes that convey needed information
- Other Items
  - Baseline attribute release enhancement
  - eduPerson recommendation for some work on K12Person

# New Entities WG: Status

- Nearing completion of core work
- Web site reflects conversation but needs much work to pull out the set of concise recommendations
  - https://spaces.internet2.edu/display/NewEntities/Home
  - There is still time to join the effort if you spot something of particular interest

- Watch for a request for review of the completed recommendations sometime over the next several weeks

# IAM Online Evaluation

https://www.surveymonkey.com/s/IAM_Online_January_2015

# Coming Up

Internet2 Global Summit

April 26-30, 2015

Washington, DC

http://meetings.internet2.edu/2015-global-summit/

# Next Month

Shibboleth IdP Version 3.X

Scott Cantor

Wednesday, March 11, 2015

2:00 pm ET / 1:00 pm CT / Noon MT / 11 am PT

www.incommon.org/iamonline

*Brought to you by Internet2's InCommon in cooperation with the Higher Education Information Security Council*