Alternative IdP Working Group Final Report

Identity Provider Strategies for Common Campus Environments

Janemarie Duh, Chair

David Walker

This report came out of the Alternative Identity Providers Working Group

Report Finalized: December, 2014

Table of Contents

- Identity Provider Strategies for Common Campus Environments
  - Executive Summary
  - The Group's Approach
  - Applicability of the Strategies to Campus IT Environments
    - In-House Strategies
      - Java Capable Campuses (with a Linux affinity)
      - Active Directory Centric Campuses
      - LAMP-capable Campuses
    - Outsourced Strategies
      - Outsourced Shibboleth
      - Campus Environments Based on Google Apps for Education or CAS
      - Insourced IdP with Vendor Support
    - State Systems
    - Selecting a Strategy
  - Prerequisites for the IdP Strategy
    - Manage the IdP Service Offering
    - Operate an IAMS
    - Identity Management Policy
    - Governance
  - Recommendations for Future Work
  - Appendix A: Alternate IdP Strategy Assessments
  - Appendix B: Alternative Identity Providers Working Group Contributors

Executive Summary

Following is a summary of the work of the InCommon Technical Advisory Committee's Alternative Identity Providers Working Group . It describes alternative strategies for deploying an Identity Provider (IdP) in a variety of campus IT environments with the goal of providing solutions for institutions that do not have the expertise and resources to operate a Shibboleth IdP locally, the strategy most deployed within the InCommon Federation as of this writing.

While a locally -operated Shibboleth Identity Provider (IdP) continues to provide the greatest capability and flexibility for an institution's current and future federation needs, there are alternatives that may be better suited to a specific institution's:

- computing environment (e.g., Java, LAMP, Active Directory)
- available resources and expertise, and strategy with respect to insourcing or outsourcing of IT infrastructure.

This paper describes and assesses several alternative strategies institutions may choose to deploy, depending on local circumstance. For example, an institution with a Java environment will likely choose a Shibboleth--based strategy, whereas a Microsoft--centric environment might choose an ADFS-based strategy. Additional considerations are outlined in the body of the report.

When configuring an in-house solution, or selecting a specific outsourced solution, careful consideration of the criteria described in this paper, in the light of both current and future needs, is very important. InCommon and other higher education identity federations are evolving rapidly, and what you do not need today may become a necessity without much warning over the next few years.

This paper closes with a set of recommendations to InCommon, TIER, and Internet2 with respect to actions the work group believes are important to facilitate the deployment of IdPs within higher education. In summary, these are:

- Create appliances for insourced operation including CANARIE/SWAMID IdP Installer tool with configurations pre-built for InCommon.
- Conduct outreach to those institutions that are not engaged in federation and would not know that alternatives for an IdP exist.
- Develop a mentor program for InCommon Members to help campuses get started.
- Develop criteria for assessing of IdP service vendors.
- Author a cookbook on deploying the IdP strategies, including technical architecture, vendor selection, user support, operation, etc. It would be valuable to work with other federations on this project, as these are common issues internationally.

The Group's Approach

The Working Group began its work by identifying a number of alternatives that can be effectively deployed today. These alternatives are:

IdP Strategy	Description
In-House Strategies	
Shibboleth IdP	Integrated with the local IdMS and operated locally, the baseline for comparison
SimpleSAMLphp IdP	An open source IdP written in PHP, integrated with the local IdMS and operated locally
ADFS IdP	Microsoft's SAML implementation for Active Directory, operated locally
Outsourced Strategies	
Outsourced Shibboleth IdP	Shibboleth, integrated with the local IdMS and operated by a third party
Outsourced Vendor IdP	A non-Shibboleth SAML IdP, integrated with the local IdMS and operated by a third party, such as Ping Identity
CAS (local) with Outsourced IdP	A SAML IdP, either Shibboleth or vendor, integrated with the local IdMS and operated by a third party, that uses a local CAS deployment for authentication
Google Apps Gateway	An OIDC-to-SAML gateway, often operated by a third party, for institutions that make use of Google Apps for Education
Insourced IdP with Vendor Support	An IdP run on a locally-supported platform, but with vendor support for the IdP itself.
Hub and Spoke (or Trusted Third Party) IdP	Likely used by systems such as community colleges, K-12, network providers, where individual constituents don't want to run their own IdP. The IdP is located at the Hub and users enter local credentials for authentication. Attributes are passed on from the home institution to the Service Provider.

We also considered the following strategies, but did not do full assessments for the reasons given below.

- Identity as a Service. This is potentially a good strategy for an institution wishing to outsource its entire IAM system, but our group's charge is restricted to IdP only.
- CAS Gateway. The group decided that this does not offer advantages over the "CAS (local) with Outsourced IdP" strategy.
- Google Apps Gateway. This is potentially a good strategy for an institution that has registered all of its community members with Google Apps for Education. The group did not have time, however, to assess this strategy.

Each of these strategies were assessed according to the following criteria:

Criteria	Description
Technical Capabilities	
Support for Recommended Technical Basics for IdPs	Support for InCommon's published recommended practices for IdPs
Support for Attribute Release	Support for attribute release from the campus IdMS
Support for Entity Categories (R&S)	Support for release of attribute bundles for specific entity categories like the Research and Scholarship Category
Support for Multiple AuthN Contexts for MFA and Assurance	Support for orchestration among multiple authentication methods to enable, e.g., multi-factor authentication for high-risk services
Support for ECP	Support for ECP to enable authentication for services that are not web-based
Support for User Consent	Support for release of attributes only after explicit user consent
Operational Criteria	
Expertise Required	In-house expertise required
Resources Required	Resources required, particularly human resources
Upkeep and Feeding Required	Overall operations effort required
Applicable Environments	Types of campus computing environments where the strategy is valuable

Pros / Benefits	Positive aspects of the strategy
Cons / Risks	Negative aspects of the strategy

Fact finders were assigned to investigate each of these alternatives. See Appendix A for detailed assessments of each of the alternative strategies. These assessments can also be found in the work group's wiki space at Alternative IdP Strategies and Assessment Criteria , along with meeting notes and other materials.

Applicability of the Strategies to Campus IT Environments

The following sections discuss the applicability of these strategies in multiple campus environments.

In-House Strategies

Operating an IdP in-house provides the greatest control and flexibility to a campus. That, however, comes at the price of infrastructure and of recruiting and retaining staff with the necessary skills. The following are recommendations for different types of campus environments.

Java Capable Campuses (with a Linux affinity)

Shibboleth is the gold standard for SAML implementations, both IdP and SP. It supports all of our criteria, with the addition of plugins, and is highly conformable to many computing environments. Shibboleth does, however, require specialized knowledge of Java application containers (e.g., Tomcat or Jetty) and XML that may not be among the core competencies of many IT organizations in higher education. Multiple WebSSO systems, such as CAS, can be integrated with Shibboleth. While such containers can be run on top of any operating system platform, the Shibboleth community is largely Linux-centric, so it is helpful to be able to "speak Linux." For IT organizations with that expertise, Shibboleth provides the greatest flexibility for adapting to changing requirements in the future.

Active Directory Centric Campuses

For campuses with identity management based on Microsoft's Active Directory, ADFS is a potential alternative to Shibboleth, particularly when Java is not a core competency. It satisfies today's basic requirements for federation, assuming the deployment of open source scripts. ADFS does not, however, have support for coming requirements like configurable multi-factor authentication, ECP, and user consent. For this reason, a local implementation strategy to use ADFS should be considered transitional, perhaps with outsourcing as a long-term strategy.

LAMP-capable Campuses

SimpleSAMLphp is a potential alternative for campuses with a LAMP (Linux, Apache, MySQL, and PHP) infrastructure. SimpleSAMLphp supports most of our criteria, with the exception of entity categories, configurable multi-factor authentication, and old versions of the SAML protocol. While an institution using SimpleSAMLphp should continue to monitor for long-term strategies with increased capability (perhaps as

enhancements to SimpleSAMLphp), it is certainly a viable solution for institutions with currently simple needs for federation.

Outsourced Strategies

Outsourced IdP services for campuses that do not fit the environments mentioned above are becoming available in the marketplace from multiple vendors. They are based on various technologies, including Shibboleth, SimpleSAMLphp, and proprietary software. We expect the capabilities provided by those vendors to evolve rapidly. The following is a snapshot of some of those services.

Outsourced Shibboleth

There is currently a limited number of vendors that offer Shibboleth as a cloud service, most notably Fischer Identity and Gluu. There are schools within OARnet that are using Fischer Identity's offering.

Campus Environments Based on Google Apps for Education or CAS

Cirrus Identity offers a SimpleSAMLphp-based IdP that can be configured to support campus IAMSs based on Google Apps or CAS; OAuth2, OIDC, and SAML are also supported. Cirrus Identity's offering supports our criteria, except for entity categories, ECP, and full configurability of multi-factor authentication; user consent is planned. This offering is certainly a viable option for campuses without a need to support ECP.

Insourced IdP with Vendor Support

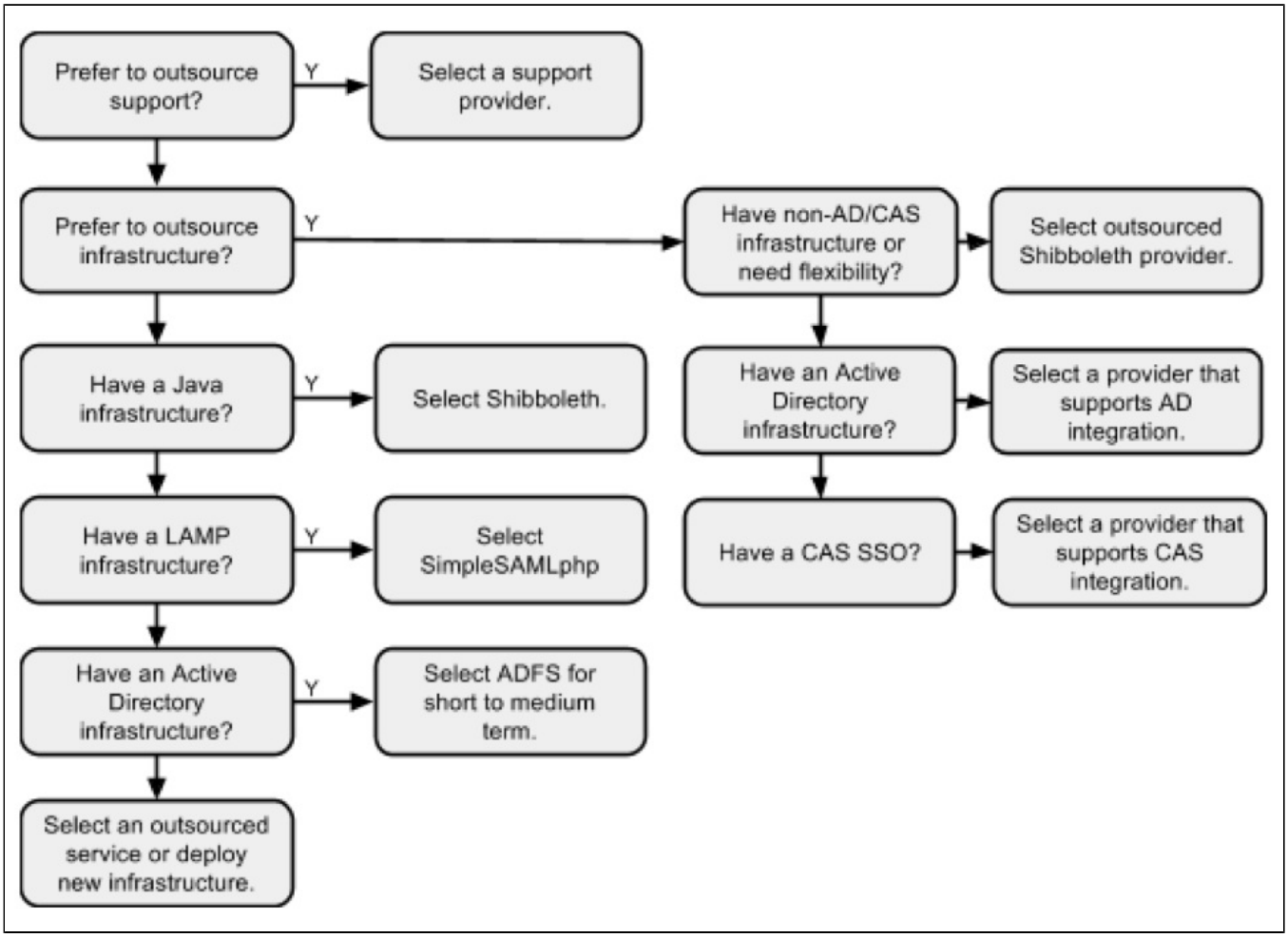
In this strategy, the IdP runs on a locally-supported platform with vendor support for the IdP itself. The hardware and operating system must still be maintained by the institution, but this strategy can facilitate quick deployment of the IdP and its required Java environment with options for the long term. The platform can be on-campus servers or utilize cloud infrastructure such as AWS or Azure. A number of vendors provide such support services; the Shibboleth Consortium maintains a list at http://shibboleth.net/community/consultants.html.

State Systems

State systems and other higher education consortia may choose to use the Hub and Spoke strategy, an insource/outsource hybrid sharing a single IdP instance operated for the entire consortium, supporting multiple scopes to represent the distinct members of the consortium. Additionally, a Shibboleth "multi-scoped" IdP may be a simpler alternative. Selection of the specific technology platform in this environment would be based on the same criteria as described above.

Selecting a Strategy

Choosing an IdP strategy for an institution will be based on many factors, most very unique to the institution. The following decision tree is intended help navigate the options:



Prerequisites for the IdP Strategy

Independent of how IdP service is deployed for a campus, there are a number of other issues that campus must address.

Manage the IdP Service Offering

Even when operation of the IdP is outsourced, it is still necessary to manage the service offering and the vendor providing that service.

Operate an IAMS

The campus must operate (or contract for operation of) an identity and access management system that tracks the lifecycle of community members' affiliation with the campus. This includes maintenance of various information about those community members: name, addresses, affiliations, group memberships, record of identity proofing, entitlements, authentication credentials, etc.

Identity Management Policy

The campus must develop and maintain policy governing identity management functions. This is includes eligibility for campus affiliation, requirements for identity proofing, assurance requirements for services, etc.

Governance

The management structure and funding for identity management must be understood to assure alignment with campus management overall.

Recommendations for Future Work

The group considered several potential activities for future work by InCommon, TIER, and/or community members. These are listed here.

1. **Activities for the InCommon administration or TIER.**

1.1. Deploy or contract for a fully- functional, outsourced Shibboleth blessed by InCommon with InCommon participating in the management of the solution.

1.2. Establish a process for certifying IdP support vendors blessed by InCommon.

1.3. Create appliances for insourced operation including the CANARIE/SWAMID IdP installer tool with configurations pre-built for InCommon. These would likely be distributed as virtual machine images.

1.4. Identify ways to facilitate InCommon members getting consultant help without a lot of administrative overhead. This might be combined with a mentor program.

1.5. Conduct outreach to those institutions that are not engaged in federation and would not know that alternatives for an IdP exist.

2. **Community solutions with InCommon coordination**.

2.1. Discuss ways to outsource an institution's IdP to other InCommon members hosting the IdP.
2.2. Develop a mentor program for InCommon Members to help campuses get started.

3. **Second phase of the Alternative IdPs Working Group or another chartered group**.
These solutions would have high value to the constituent group that the working group was tasked in addressing, i.e., institutions that do not have local resources, yet the work effort would not be as high as the recommendations above.

3.1. Develop criteria for assessing of IdP service vendors.
3.2. Identify and assess vendors. This would have to done repeatedly in order to keep current and provide value.

3.3. Author a cookbook on deploying the IdP strategies, including technical architecture, vendor selection, user support, operation, etc.

Of these, we recommend the following actions be taken as next steps:

- Create appliances for insourced operation including the CANARIE/SWAMID IdP installer tool with configurations pre-built for InCommon. Explore the method for easiest and most sustainable install possible which may be virtual machine, image, or simply the InCommon enhancements to the IdP Installer tool. (1.3)
- Conduct outreach to those institutions that are not engaged in federation and would not know that alternatives for an IdP exist. (1.5)
- Develop a mentor program for InCommon Members to help campuses get started. (2.2)
- Develop criteria for assessing of IdP service vendors. (3.1)
- Author a cookbook on deploying the IdP strategies, including technical architecture,vendor selection, user support, operation, etc. (3.3)

Notes

- Items 1.1 (Deploy or contract for a fully-functional, outsourced Shibboleth blessed by InCommon with InCommon participating in the management of the solution) and 1.2 (Establish a process for certifying IdP support vendors blessed by InCommon.) are considered to be important tasks, but they rely on prior completion of 3.1 (Develop criteria for assessing of IdP service vendors).
- Item 1.5 (Reach out to those institutions that are not engaged in federation and would not know that alternatives for an IdP exist) is of particular importance as the target audience for these activities is institutions that do not currently participate in InCommon. Some of the ways in which outreach can be done include:
    - Publish case studies to make a basic case for federation and describing the benefits of being a participating member of the InCommon federation
    - Compile a list of organizations to target
    - Conduct interviews of CIOs from institutions who are not members of InCommon
    - Create a "road show" for higher education venues, such as:
        - Consortia like the Consortium of Liberal Arts Colleges (CLAC)
        - The National Association of College and University Business Officers (NACUBO)
        - Regional R&E network providers and The Quilt
        - EDUCAUSE
        - InCommon affiliated vendors (to tell their higher ed clients about InCommon, as well as federating their own services. They would first need to see the value of federation)

Appendix A: Alternate IdP Strategy Assessments

To review the assessments of the various IdP strategies considered by the working group please see:

- The Alternative IdP Strategies and Assessment Criteria (wiki page)
- Full Report (PDF)

Appendix B: Alternative Identity Providers Working Group Contributors

Shaun Abshere, WiscNet
David Alexander, IDM Integration
Mark Beadles, OARnet
Steve Carmody, Brown University
Alex Chalmers, Ball State University
Dedra Chamberlin, Cirrus Identity
Emmet Culley, California Community Colleges
Lou Delzompo, California Community Colleges
Janemarie Duh, Lafayette College, Chair
Mike Grady, Unicon
Mark Jones, University of Texas Health Science Center at Houston

Scott Koranda, Spherical Cow Group
Chris Phillips, CANARIE
Ben Poliakoff, Reed College
Tom Scavo, Internet2
Mark Scheible, MCNC
David Walker, Internet2
Dan Zweifel, Washington University in St. Louis