Identity Provider Strategies for Common Campus Environments

Janemarie Duh, Chair
David Walker
Alternative Identity Providers Working Group

December, 2014

Table of Contents

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

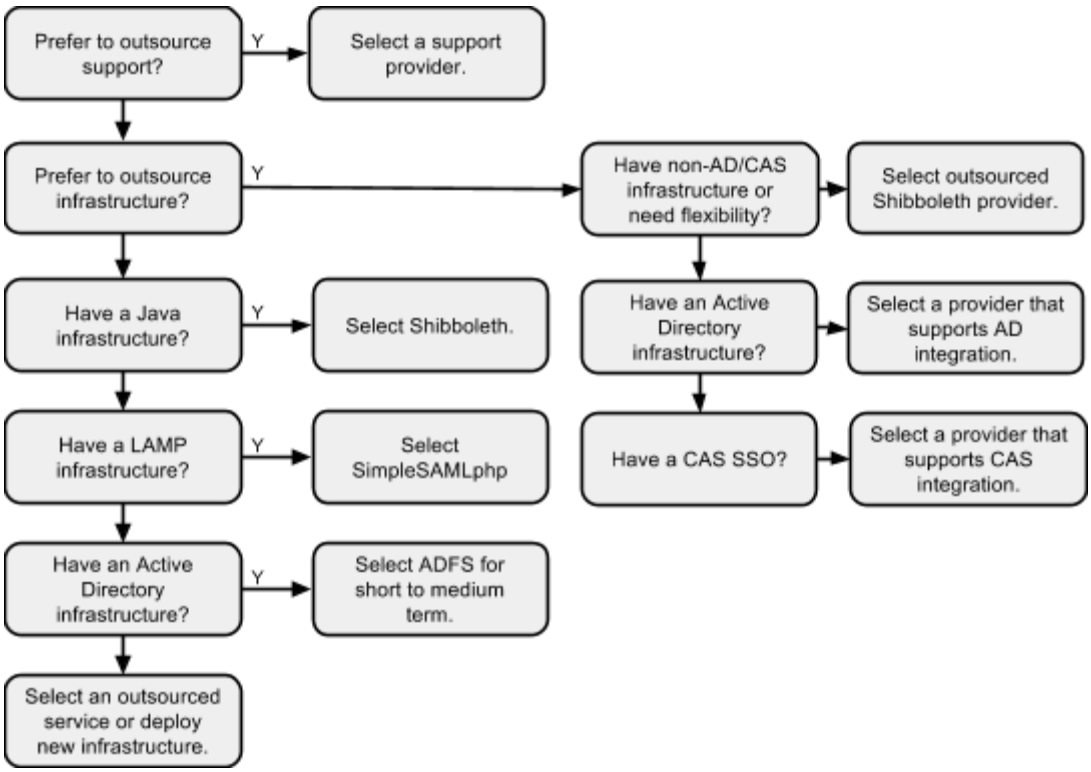
In this strategy, the IdP runs on a locally-supported platform with vendor support for the IdP itself. The hardware and operating system must still be maintained by the institution, but this strategy can facilitate quick deployment of the IdP and its required Java environment with options for the long 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

The following are assessments of the various IdP strategies considered by the work group. These assessments are also available from the Alternative IdP Working Group wiki space at Alternative IdP Strategies and Assessment Criteria.

Shibboleth IdP (local)

Description
The Shibboleth Identity Provider software integrated with the local IdMS and operated locally is presented as a baseline for comparison of all proposed alternative solutions which are not set up, run, and maintained locally by a campus .

Fact Finders
Janemarie Duh (Lafayette College)
David Walker (Internet2)

Example Deployments
Shibboleth is the primary IdP software used in R&E federations.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata
The Shibboleth IdP can be configured to support all recommended technical basics.

Support for Attribute Release
Shibboleth can be configured to release any attributes supported by the IdMS. Attribute filter policies are set on the IdP to release attribute values and done so in a privacy-preserving way.

Support for Entity Attributes/categories (e.g., R&S)
The IdP software supports the release of entity attribute bundles in fixed or dynamic subsets to all SPs or R&S SPs.The benefit of supporting attribute bundles is the decreased administrative overhead. An attribute is configured for the entity category.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Identity assurance. The Multi-Context Broker, an extension to the Shibboleth IdP, supports multiple assurance profiles.
https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker

Support for ECP (Enhanced Client or Proxy)

ECP is a SAML authentication profile for non-browser clients. There is a Java client which is a wrapper around the Apache HTTPClient that provides Shibboleth support.
https://github.com/reckart/shib-http-client

Support for User Consent

User attribute release consent. Technology exists via an extension for Shibboleth IdPs, uApprove, to implement attribute release consent. It also handles Terms of Use.
https://www.switch.ch/aai/support/tools/uApprove.html
There is also current work on a privacy manager through the NSTIC-sponsored Scalable Privacy Project.

Expertise Required

Shibboleth requires expertise in the operation of Java-based services and XML, in addition to general knowledge of federation architecture.

Resources Required

Shibboleth requires a Java servlet container, such as Apache Tomcat. Hardware resources that must be allocated are dependent on load, but are generally low.

Upkeep and Feeding Required

Maintaining an IdP requires keeping up on security patches and advisories for the underlying resources as well as keeping current on the IdP software itself. Site administrators are tasked with maintaining the IdP metadata and monitoring the InCommon NOTICE list in case technical changes are made that require them to take corrective action regarding their IdP and how it operates in a federated context.

Applicable Environments

Shibboleth is highly adaptable to arbitrary environments.

Pros / Benefits

Shibboleth is the mainstream SAML implementation. It is used in the vast majority of federation deployments, and new developments in the use of SAML are usually built for Shibboleth first.

Cons / Risks

Shibboleth requires specialized expertise to operate. This expertise may not already be available in an environment that does not already support Java.

ADFS IdP

Description

Active Directory Federation Services (ADFS) from Microsoft provides users with SSO capabilities in federated environments. ADFS uses a "claims-based" access control authorization model. See:

- http://msdn.microsoft.com/en-us/library/bb897402.aspx
- http://en.wikipedia.org/wiki/Active_Directory_Federation_Services
- https://spaces.internet2.edu/display/InCFederation/Using+Other+Software
- https://wiki.shibboleth.net/confluence/display/SHIB2/MicrosoftInterop
- http://adfstoolkit.org/

Fact Finders

Scott Koranda (Spherical Cow Group)
Alex Chalmers (Ball State University)

Example Deployments

Ball State University (BSU), an InCommon Participant, is an example of an ADFS deployment used for federation in the InCommon context.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

Metadata Consumption

ADFS does not support direct consumption of InCommon Federation metadata. The product focuses on a more point-to-point federation approach where the details for each entity are entered one at a time using a graphical user interface (GUI) better suited for point-to-point federation than a large identity federation like InCommon. To help work around this limitation ADFS deployers have developed pysfemma, "a script that parses a (Shibboleth) federation metadata XML content and creates a pool of metadata files and a powershell script in order to automatically configure and update an Active Directory Federation Services STS (Security Token Service)." We note, however, that there are issues when using pysfemma such as all entities being deleted and then re-populated with each run, and that a run to consume the InCommon metadata can take more than two hours.

As noted above, ADFS does consume per-entity metadata directly without the use of pysfemma or other third-party tools using a graphical user interfaced (GUI) better suited for point-to-point federation.

Scope in Metadata

ADFS does not support the notion of scope as it is normally used in the SAML context. Specifically when ADFS is acting in an SP role it does not check the scope on (scoped) attributes in an assertion from an IdP. There are, however, techniques that ADFS operators can use in combination with pysfemma and other scripts to approximate the handling of scope. See for example this email thread.
Please note that the above concerns ADFS acting in an SP role and not an IdP role, which is the primary focus here. We include these details in order to answer questions posed by readers.
When acting as an IdP ADFS can assert scoped attributes (or claims), such as eduPersonPrincipalName.

X.509 Certificates in Metadata

Older versions of ADFS would not accept 2 relying parties having the same X.509 signing certificate. This is a problem since some SPs operated by the same entity, often logical SPs sharing the same base Shibboleth installation, use the same X.509 certificate in metadata. ADFS update 3 (also known as 2.1 2012) fixes this issue. Note that if the X.509 certificates are part of a PKI infrastructure (not self-signed) ADFS does check the CRLs and other parts of the certificate chain. If the certificates are self-signed they must still be time valid (not expired).

SAML Protocol Endpoints

ADFS does not support SAML 1.1 but does support SAML2 authentication requests via the SAML V2.0 HTTP-Redirect binding. ADFS can protect all endpoints with SSL/TLS.

Support for Attribute Release

With ADFS the accompanying Active Directory (AD) deployment is configured automatically as an attribute store, so it is only necessary to run through a "wizard" to set up attributes. It is also straightforward to use the AD LDAP functionality as an attribute store. ADFS can also pull/resolve attributes from an associated Microsoft SQL Server easily. Other SQL data stores can also be used but require the writing of a plugin and some scripts.
It is, however, important to note that ADFS releases attributes in an undefined format type, whereas in the InCommon Federation relying parties usually anticipate a format type of URI. The ADFS operator can change the format type from undefined to URI relatively simply, but this must be done for every claim (attribute) that it is issuing. It is not uncommon for this to be scripted. The ADFS claim/attribute rule language has the reputation of being arcane and not well documented.

Support for Entity Attributes/categories (e.g., R&S)

ADFS does not support (without use of third-party tools) entity attributes or categories, such as the InCommon R&S entity category. Configuration is per relying party. So for example it is not possible to configure ADFS to release an attribute (claim) such as eduPersonPrincipalName to a set of SPs based on the SPs being tagged in the consumed (InCommon) metadata with the R&S entity category.
An ADFS operator, however, can use third-party tools such as pysfemma and a combination of PowerShell tools to help configure ADFS so that it effectively does release attributes to SPs based on an entity category like R&S.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

ADFS does not support multiple authentication contexts that would allow for easy integration of MFA, InCommon Assurance, and "step up" authentication flows.

Support for ECP (Enhanced Client or Proxy)

ADFS does not support ECP. It only supports the POST, redirect, and artifact bindings and does not support SOAP/PAOS.

Support for User Consent

ADFS does not support "user consent" in the context of a "uApprove like" approach.

Expertise Required

ADFS as a component in a Microsoft Windows server deployment integrates well and does not require expertise beyond that one expects for Windows administrators operating for example AD. Considerable expertise, however, is required when integrating ADFS into a higher education federation like InCommon since it is necessary to "translate" from the language and "culture" of the federation to that of the ADFS environment, and to be able to understand how to use tools like pysfemma to work around some of the limitations of ADFS. This expertise is often hard won and not found with the more "traditional" ADFS administrators.

Resources Required

ADFS is easy to deploy and integrate in an existing AD environment for experienced Windows administrators and does not require any special resources. Note, however, that when federating ADFS with more than 100 relying parties (which is expected in InCommon) it is necessary to use a Microsoft SQL Server database rather than the Windows "internal" database used by default. The SQL server should itself be in a high availability (HA) configuration if ADFS and AD and other components are set up in a HA configuration.

Upkeep and Feeding Required

Once deployed, configured, and integrated with InCommon via pysfemma or the like, ADFS has a reputation for being stable and solid. It is known to scale well.

Applicable Environments

ADFS is used when the existing IdMS is Microsoft Active Directory (AD).

Pros / Benefits

Using ADFS is a natural approach for Microsoft Windows shops and the basic deployment and configuration will be straightforward for experienced Windows administrators. Once deployed ADFS is known to be stable and scale well. High availability (HA) configurations use standard Microsoft Windows server techniques and approaches for HA.

Cons / Risks

Integration with large identity federation environments like InCommon requires additional scripts and supporting infrastructure like pysfemma and a considerable learning curve to acquire the necessary knowledge to "bridge the gaps" between the InCommon environment and the peer-to-peer model or approach that is the norm for ADFS federation.

SimpleSAMLphp IdP

Description

SimpleSAMLphp is a lightweight IDP and SP implemented in (drumroll) PHP. Its development is sponsored/hosted by Uninett, a "state owned company responsible for Norway's National Research and Education Network."

Fact Finder

Ben Poliakoff (Reed College)

Example Deployments

https://simplesamlphp.org/users
Judging from the users enumerated on the above site, most production instances of this software are in European Universities, Federations, and companies serving those entities.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

SimpleSAMLphp supports a subset of the features of the Shibboleth IdP:

- Automated consumption of SAML metadata
- Scope in metadata
- x509 certificates in metadata

- SAML V2.0 Web Browser SSO
- Authentication requests via the SAML V2.0 HTTP-Redirect binding, the SAML V2.0 HTTP-Post binding, and (optionally) the legacy Shibboleth 1.x AuthnRequest protocol
- ECP with a third party patch (not well integrated or tested)
- Does *not* support SAML V1.1 attribute queries
- Endpoint protection protected with SSL/TLS optionally
- Also supports establishing an IdP Proxy.

Support for Attribute Release

The software does support sophisticated attribute filtering, release (including consent, using the bundled consent module).

Support for Entity Attributes/categories (e.g., R&S)

Not currently supported, this is an open issue:
https://github.com/simplesamlphp/simplesamlphp/issues/49

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

The IdP software is quite flexible and extensible, supporting multiple authentication methods (LDAP, Radius, various databases, OpenID, Yubikey, etc) and multiple factors.
I'm not certain about "Assurance".

Support for ECP (Enhanced Client or Proxy)

ECP is supported with a third party patch, not widely implemented.

Support for User Consent

Supported with a bundled extension, https://simplesamlphp.org/docs/stable/consent:consent

Expertise Required

Experience with the deployment of PHP applications is required, including the maintenance and management of associated web server software (Apache, Nginx, etc)

Resources Required

The service itself is quite lightweight, serving as middleware, requiring a web server that can serve PHP. There is, of course, an implicit requirement for a local IdMS. The software is most commonly integrated with LDAP directories.

Upkeep and Feeding Required

As with any of the locally hosted IdPs, the software itself needs to be kept up to date. Additionally the underlying web server must be well cared for.

Applicable Environments

- Organizations with little experience with Java and/or with little desire for hosting Java applications
- Organizations with existing local PHP hosting expertise and/or investment in PHP hosting architecture
- Organizations that might want to quickly extend the functionality of the software by writing PHP extensions and/or patches
- System-wide organizations that have use cases where operating an IdP Proxy to front member organizations IdPs is the best fit.

Benefits

SimpleSAMLphp is easy to deploy in LAMP environments, can be easily extended or patched, has an active development community, and probably starts up about 15 times faster than a Java servlet.

Insourced IdP with Vendor Support

Description

An IdP run on a locally-supported platform with vendor support for the installation, configuration, and operation of the IdP itself. In this assessment, we will assume the IdP software is Shibboleth.

Fact Finder

David Walker (Internet2)
Mike Grady (Unicon, Inc.)

Example Deployments

The University of California Hastings College of the Law (http://www.uchastings.edu) has a Shib IdP that was installed and configured by Unicon on Hastings-managed servers, and the IdP continues to be managed by Unicon on behalf of UC Hastings. More common to date are institutions hiring vendors such as Unicon to install and configure the IdP initially, but then the campus primarily manages it after that, often with a support contract to get vendor help as needed. Servers can be within the institution, or in cloud infrastructure such as AWS or Azure.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

The Shibboleth IdP can be configured to support all recommended technical basics.

Support for Attribute Release

Shibboleth can be configured to release any attributes supported by the IdMS. Attribute filter policies are set on the IdP to release attribute values and done so in a privacy-preserving way.

Support for Entity Attributes/categories (e.g., R&S)

The IdP software supports the release of entity attribute bundles in fixed or dynamic subsets to all SPs or R&S SPs.The benefit of supporting attribute bundles is the decreased administrative overhead. An attribute is configured for the entity category.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Identity assurance. The Multi-Context Broker, an extension to the Shibboleth IdP, supports multiple assurance profiles.

Support for ECP (Enhanced Client or Proxy)

ECP is a SAML authentication profile for non-browser clients. There is a Java client which is a wrapper around the Apache HTTPClient that provides Shibboleth support.

https://github.com/reckart/shib-http-client

Support for User Consent

User attribute release consent. Technology exists via an extension for Shibboleth IdPs, uApprove, to implement attribute release consent. It also handles Terms of Use.

https://www.switch.ch/aai/support/tools/uApprove.html

There is also current work on a privacy manager through the NSTIC-sponsored Scalable Privacy Project.

Expertise Required

Expertise in the installation, configuration, and operation of the hardware and operating system are required. Specific expertise in Shibboleth, however, is provided by the vendor.

Resources Required

Hardware resources that must be allocated are dependent on load, but are generally low. Shibboleth requires a Java servlet container, such as Jetty, which could be provided by the vendor.

Upkeep and Feeding Required

The hardware and operating must be maintained. Upkeep of the IdP itself, and probably the Java servlet container would be the responsibility of the vendor.

Applicable Environments

Shibboleth is highly adaptable to arbitrary environments.

Pros / Benefits

Shibboleth is the mainstream SAML implementation. It is used in the vast majority of federation deployments, and new developments in the use of SAML are usually built for Shibboleth first. Outsourcing support can facilitate quick deployment of the IdP. The outsourced support can be utilized for the long term, or support can be phased over to the institution over time.

Cons / Risks

None were identified by the fact-finders.

Outsourced Shibboleth IdP

Description

Shibboleth, integrated with the local IdMS and operated by a third party.

Fact Finder

Mark Beadles (OARnet)

Example Deployments

1. Shibboleth deployed on server(s) outside the institutional network ("in the cloud") and operated by a third party - Shibboleth in the Cloud

2. Shibboleth deployed on server(s) or appliance(s) within the institutional network and operated by a third party - Shibboleth in a Box

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

As with Shibboleth (local).

Support for Attribute Release

As with Shibboleth (local).

Support for Entity Attributes/categories (e.g., R&S)

As with Shibboleth (local)

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

As with Shibboleth (local), assuming that 1. the third-party operator supports/provides the Multi-Context Broker (https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker), an extension to the Shibboleth IdP and 2. additional integration is performed between the third-party operated server(s) and the institution's authentication providers.

Support for ECP (Enhanced Client or Proxy)

As with Shibboleth (local), assuming that the third party operator has configured and enabled the SAML2 ECP profile (https://wiki.shibboleth.net/confluence/display/SHIB2/IdPEnableECP)

Support for User Consent

As with Shibboleth (local), assuming that the third party operator has configured and enabled an extension such as uApprove (https://www.switch.ch/aai/support/tools/uApprove.html) or equivalent.

Expertise Required

Expertise in Shibboleth, SAML, XML, Java are not required since these are outsourced to the operator. Institution still needs sufficient expertise to run their own IdMS infrastructure.

Resources Required

1. Shibboleth in the Cloud: the main resource requirement is financial, however the institution will need to provide personnel time for integration and testing with the third-party server.

2. Shibboleth in a Box: in addition to requirements for 1, institution will need to provide data center space and potentially server platform for use by the third-party provider.

Upkeep and Feeding Required

Upkeep and feeding of the IdP proper are handled by the third-party operator, however the institution will need to monitor, patch, maintain the IdMS infrastructure.

Applicable Environments

Since the operations are outsourced, this model can work with nearly any environment.

Benefits

Most or all of the benefits of Shibboleth - local, but without the requirement to install, operate, maintain, or have operational expertise in Shibboleth.

Outsourced Vendor IdP (Cirrus Bridge)

Description

A multi-tenant, cloud hosted SAML IdP. The current solution runs on simpleSAMLphp, though that may change over time. The "bridge" can translate OAuth2, OIDC, or CAS to SAML. Ideal for campuses/institutions running GoogleApps or CAS who need a SAML IdP and would prefer not to deploy and maintain one locally.

Fact Finder

Dedra Chamberlin (Cirrus Identity)

Example Deployments

- Cirrus Identity is a GoogleApps business which has a SAML IdP registered in InCommon. We use the Bridge ourselves on a daily basis for access to our SPs which are registered in the InCommon federation
- We have conducted a PoC at a Bay Area university to integrate their local CAS and GoogleApps with Service Now in the cloud using our test Cirrus Bridge for authentication. We are currently seeking permission to release more details about this project.

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

The Cirrus Bridge supports all but item 4 of the “Endpoints in IdP Metadata” section.

Support for Attribute Release

The Cirrus Bridge integrates with a campus IdMS (CAS, GoogleApps, or local LDAP) to manage attribute release.

Support for Entity Attributes/categories (e.g., R&S)

Cirrus Identity does not own the data being released by the campus. Assuming the campus approves the release of R&S attributes and works with Cirrus on one of the attribute release approaches noted above, there is no technical impediment to the release of R&S attributes.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

The Cirrus Bridge will support multiple authentication contexts and can be configured on a per-SP basis, i.e., one SP may require multi factor authentication, while another may not.

Support for ECP (Enhanced Client or Proxy)

The Cirrus Bridge currently does not support ECP.

Support for User Consent

This feature is not currently implemented, but on the Cirrus roadmap. We hope to either implement an attribute release manager or leverage an existing tool with our products.

Expertise Required

- One-time allocation of campus IT staff resource to assist with integrating data with the cloud-hosted Cirrus solution, most likely with expertise in the local attribute store and web SSO solutions.
- Our recent campus PoC took about 5 hours of local staff time for the first integration (ServiceNow), and about 45 minutes for the second (Google Apps).

Resources Required

This solution is cloud-hosted, so minimal local resource is required. Beyond the one-time integration work, local staff may need to assist from time-to-time with trouble-shooting.

Upkeep and Feeding Required

Minimal (see above) unless core local services are changed and additional integration work needs to be completed.

Applicable Environments

- Any institution that wishes to benefit from SAML-enabled applications (particularly cloud-hosted) but would prefer not to run a SAML-IdP locally
- **Particularly well-suited to institutions which already host a credential store and log-in solution, such as CAS and/or Google Apps institutions.**

Pros / Benefits

Designed to be a quick, cost-effective, low-maintenance solution for institutions who need a SAML IdP and would prefer not to incur the cost of standing up an IdP and it's ongoing maintenance.

Cons / Risks

- No endpoint in IdP metadata support as noted above
- No ECP support
- Doesn't yet support user consent for attribute release (though campus can limit which attributes are released to the Bridge)

Hub and Spoke (or Trusted Third Party) IdP

Description

A "Hub and Spoke" strategy would likely be used by a group of organizations that don't want to (each) run their own IdP. Examples would be University or Community College Systems, a group of K-12 school districts (either a regional unit or possibly statewide), or a Regional Network Provider running a Hub and Spoke IdP for its constituents. Additionally, this could be implemented by a vendor providing the service to multiple clients, however, individual client flexibility of the solution is limited. The IdP is located at the Hub, and users would enter their credentials and select their institution (for authentication) when logging in. This allows the "hub" to authenticate the user at their institution and obtain agreed upon attributes which would then be passed on to the Service Provider. Additionally, a centralized User Consent page could also be presented to the user when attempting to access a Service Provider.

Fact Finder

Mark Scheible (MCNC)

Example Deployments

There aren't any known deployments in InCommon, however, there are Hub and Spoke variations in some of Europe's smaller countries - WAYF (Denmark), SURFnet (The Netherlands), FEIDE (Norway). These are used to provide an entire suite of "federation" services.

Support for the Recommended [Technical Basics for IdPs|], including the ability to consume metadata

Since SimpleSAMLphp is frequently used to implement a Hub and Spoke strategy and its variations, these are supported to the extent they're supported by SimpleSAMLphp.

Support for Attribute Release

Attribute release is supported, however, client or spoke organizations may not have the flexibility to choose which attributes to release individually. These may be determined by the organization running the Hub IdP or by a consensus of the client organizations.

Support for Entity Attributes/categories (e.g., R&S)

Not currently.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Multiple authentication methods are supported via SimpleSAMLphp, which allows clients with different authentication implementations (e.g. LDAP, CAS, Active Directory, etc.) to exist in the same configuration.

Support for ECP (Enhanced Client or Proxy)

Via a 3rd-party patch to SimpleSAMLphp

Support for User Consent

Yes, and in a Hub and Spoke configuration it can be centralized, allowing use by all user organizations.

Expertise Required

Depending on the implementation, LDAP experience is required as each organization needs to support some method of authentication used by the Hub. Additionally, some understanding of how the Hub operates and releases (or not) attributes to connected SPs must be understood.

Resources Required

There are two sides of this strategy. From the Hub Organization side, knowledge and expertise in running an IdP (likely SimpleSAMLphp) as well as being able to configure and support any additional services being provided to the “Spoke” Organizations. Spoke Organizations might need few resources beyond maintaining their own campus authentication environment. Spoke SP Organizations (if offered by one of the group members) would likely need to have similar resources to the Hub organization – ability to run an SP, integrated with their service or application being offered to others.

Upkeep and Feeding Required

As stated previously, there is a lot more upkeep required on the Hub side of this strategy than on the Spoke side. Hub organizations need to keep their Client organizations “happy”, keep their data secure, provide Services that are needed by the clients.

Applicable Environments

The Hub and Spoke IdP Strategy is not likely to be implemented by a single organization (unless via a vendor-provided service), but could be a good solution for small groups of organizations (Higher Education "Systems" as mentioned above), particularly for client organizations (spokes) that have limited resources to run their own IdP. However, in a fragmented environment it "might" be implemented to allow access to resources where a central common directory (and person registry) does not exist - e.g. undergraduate student directory, employee directory, alumni directory, distance education directory, standalone guest system, etc.

Pros / Benefits

Biggest benefit to the spoke organizations is that the majority of the work is done by the Hub Organization. Spoke organizations can join with little or no ongoing overhead, once implemented.

Cons / Risks

The Hub organization controls most of the services provided to the client “spoke” organizations and as a result the spoke organizations have less flexibility in attributes released to SPs, or in SPs integrated with the IdP for example.

IdP-Installer Appliance Installation

Description

The IDP-Installer component is a lightweight tool to install both a Shibboleth 2.4 IdP and/or eduroam capable FreeRADIUS installation preconfigured for a given federation.

The design is modular and capable to be tailored for multiple federations of which Sweden's SWAMID and Canada's Canadian Access Federation have builds. It is multi-lingual and available to be tailored by anyone from github.

The process of installing the components is straightforward; an interview process via a bundled local webpage in the installer helps create and manage a configuration file used for input to the installer, the act of doing the installation with said configuration, and some post configuration steps.

The installer out of the box creates a ready dev or test environment in a few minutes and uses self signed certificates and a default installation.

The intent is to provide a rapid test environment and more importantly, a base configuration such that a production installation is a repeatable process with little effort using the configuration file approach.

Fact Finder

Chris Phillips (Canadian Access Federation)

Example Deployments

The IdP-installer has been used by more than 6 institutions in Canada to install their test environment as well as their production environment.

The IdP-Installer home

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

Supported configurations are documented in the bundled documents (single hosts, active-standby production configurations etc) of the installer. It is pre-configured for Canadian Access Federation Metadata.

Support for Attribute Release

Shibboleth can be configured to release any attributes supported by the IdMS. The Shibboleth instance is expected to be pointed at Active Directory.

Attribute filter policies are set on the IdP to release attribute values and done so in a privacy-preserving way.

Support for Entity Attributes/categories (e.g., R&S)

The IdP software supports the release of entity attribute bundles in fixed or dynamic subsets to all SPs or R&S SPs.The benefit of supporting attribute bundles is the decreased administrative overhead. An attribute is configured for the entity category.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Identity assurance. The Multi-Context Broker, an extension to the Shibboleth IdP, supports multiple assurance profiles. See https://spaces.internet2.edu/display/InCAssurance/Multi-Context+Broker

Support for ECP (Enhanced Client or Proxy)

ECP is a SAML authentication profile for non-browser clients. There is a Java client which is a wrapper around the Apache HTTPClient that provides Shibboleth support.

https://github.com/reckart/shib-http-client

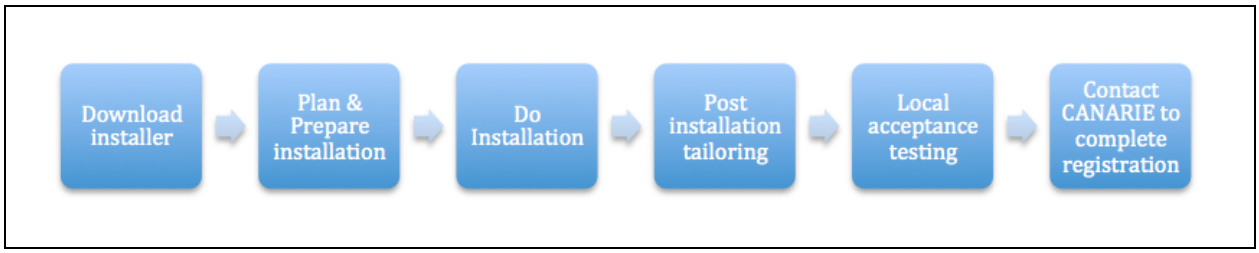
Support for User Consent

Technology exists via an extension for Shibboleth IdPs, uApprove, to implement attribute release consent. It also handles Terms of Use. See https://www.switch.ch/aai/support/tools/uApprove.html. User Consent in the IdP-Installer is not enabled by default.

Expertise Required

The IdP-installer is designed to reduce the required expertise to that of a general system administrator. General knowledge of federation architecture is beneficial but is not required to commence the installation.

Many of the configuration decisions and barriers to implementation are reduced or eliminated via pre-configurations specific to the baseline federation operations and the Q&A interview style process at the beginning of the installation process.



The above is the usual process for using the IdP-Installer with the Canadian Access Federation operated by CANARIE.

Resources Required

The VM with 8gb of memory, 20gb disk, 2 CPUs is sufficient for a small to medium-sized production machine.See Latest IdP-Installer Documentation

The IdP-Installer can also be easily installed in a local virtual box image as described here https://collaboration.canarie.ca/elgg/file/view/1666/configuration-guide-to-setting-up-virtualbox-for-the-idp-installer

Upkeep and Feeding Required

Maintaining an IdP requires keeping up on security patches and advisories for the underlying resources as well as keeping current on the IdP software itself.

The IdP-Installer does not perform 'upgrades' as there is a significant amount of bespoke configuration post installation (specifically around the IdP WAR actually for login page customization etc). The upgrade path is to repeat the configuration in a VM from a base installation and re-configure from there.

It is up to the IdP operator to decide what is a major change that would require a fresh install (which only takes a few minutes) vs a minor change such as attribute release which edits can happen on the existing installation.

Applicable Environments

Shibboleth is highly adaptable to arbitrary environments.

The IdP-Installer also supports the inclusion of an eduroam ready FreeRADIUS server pre-configured for Canadian Access Federation use.

Pros / Benefits

This component has exactly the same benefits as the Shibboleth software selection, but is pre-configured for operation with default metadata settings, directory settings abstracted into a Q&A interview process the installation personnel go through to pre-flight check the installation.

This approach allows for more rapid IdP installation measured in days (for some, minutes) rather than weeks.

By designing for an out of box dev experience, the installer encourages a practice to have a test environment as well as a production environment for those who may not have these practices in place already.

Cons / Risks

The IdP-installer is available in a 'global' configuration and configurations for Canada (CAF) and Sweden (SWAMID), but none are available for inCommon.

While not difficult, no 'lead' or champion in the US space has voiced interest to craft the inCommon 'build' and CAF would be interested in identifying an interested person or group. Guidance on configuration can be provided if some wishes to self identify as interested.

There are two discrete areas for configuration -- Shibboleth and eduroam and tailoring the configuration is not difficult but inCommon specifics are needed for such an action.

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