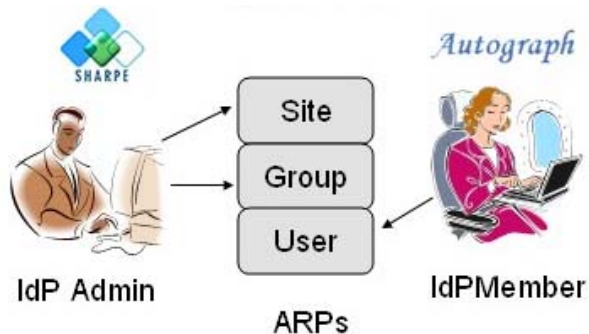


Shibboleth™ Attribute Release Policy Editing Tools



Introduction

Shibboleth provides for privacy protection through Attribute Release Policies (ARPs). Release of user attributes from an Identity Provider (IdP) to a Service Provider (SP) is determined by the IdP's ARPs. ARPs contain a set of rules specifying which attributes to release for institution members in general, or for specific individuals. Currently, editing of these XML files needs to be done manually, an error prone and cumbersome process.

ShARPE and Autograph are two open source applications for managing Shibboleth Attribute Release Policies via a GUI. ShARPE is used by IdP administrators to define site and group ARPs, and Autograph is used by IdP members to define individual ARPs based on individual privacy requirements.

ShARPE and Autograph v0.8 may be installed as part of a new Shibboleth IdP installation or onto an existing IdP.

Additional Features

In order to easily manage a Shibboleth-based Federation, ShARPE and Autograph introduce the following features:

Group ARPs

It is envisaged that agreements or 'contracts' between IdP and SP may be established by specific groups within the institution. ShARPE introduces support for group ARPs. The list of IdP group names and group memberships can be read from the institutional directory or from a flat-file.

Service Description

In order to sensibly decide which attributes to release, IdP administrators and users need to know the attributes and values an SP requires. In addition, releasing more attributes that are personal should give access to more services, and users need to know what they get in return for giving up their privacy.

A Service Description (SD) describes the SP's service and service offerings and attributes (names and values) required. SDs enable comprehensive service information to be provided to IdP administrators and users, and release of only those attributes required to access required service offerings where consistent with privacy requirements.

Federation Manager, a tool for administrators to manage IdPs and SPs entries in the federation, fully supports service descriptions by integrating the entries into the Federation metadata. ShARPE and Autograph are able to process SP's authoritative service description from the Federation.

ShARPE and Autograph may also be applied to existing IdPs which may not have service descriptions for their SP. In this case, attributes need to be manually specified (SP names are obtained from the federation metadata file), but information on

service offerings and attributes required to access services is not available.

Attribute Mapping

Many IdPs will use a custom directory schema hence there needs to be a mechanism to map attributes from the IdP's schema to the schema required by the SP or the Federation.

ShARPE provides attribute-mapping functionality allowing the IdP administrator to express the required mapping using special functions. For example, attributes may be mapped by name (one-to-one or by concatenation), assigned static values, hashed (useful for targetedID implementations).

ShARPE

ShARPE is used by the IdP administrator to:

- Manage users' accesses to SPs via service descriptions
- manage institution-wide ARPs
- manage group ARPs
- specify mappings between the IdP attribute schema and SP schemas

Example Scenario

Consider the case of an IdP wishing to specify institution-wide and group ARPs for a particular service. In this case, the service provider offers a minimally featured 'Read access' service offering to the entire IdP membership, and 'Moderator' service offering to the librarians who have created the appropriate contract with the SP. Firstly, the Service Description for the SP is selected:



Next the IdP administrator ensures that only those attributes required to access the Bronze service offering are released to the SP for the entire IdP membership.

aafl1.mams.local
Physics Repository

Status: **NEW**

Service Offering	Description	Requested Attributes
Moderator	This service offering allows documents to be deleted and new document categories to be established.	Surname Nickname Affiliation
Create access	This service offering allows new documents to be created and added to the repository.	Nickname Affiliation
Read access	This service offering allows all non-classified documents to be searched and downloaded.	Affiliation

Group	Released Attributes	Service Offering Status
all communities		<input checked="" type="radio"/> Moderator <input type="button" value="Enable"/>
all communities		<input checked="" type="radio"/> Create access <input type="button" value="Enable"/>
all communities		<input checked="" type="radio"/> Read access <input type="button" value="Enable"/>

The IdP administrator then creates contract for Librarian group using SHARPE, which ensures that only those attributes required to access the 'Moderator' service offering are released to the SP for the members of the group.

Group	Released Attributes	Service Offering Status
Librarian	Nickname Affiliation	<input checked="" type="radio"/> Moderator <input type="button" value="Enable"/>
		<input checked="" type="radio"/> Create access <input type="button" value="Disable"/>
		<input checked="" type="radio"/> Read access <input type="button" value="Disable"/>

Any users (IdP members) who are also the member of 'Librarian' group will be able to access 'Moderator' service offering on runtime. Other users will only gain 'Read access' service.

Autograph



Autograph allows an IdP member to protect their privacy by providing for control of attributes released to individual service providers.

Autograph is used by IdP members to view attributes released to specific SPs on their behalf, and to deny the release of attributes in accordance with their privacy requirements.

Example Scenario (continued)

Susannah Halmay, a staff member in the physics department, has access to the Moderator service offering by virtue of her membership in the Librarian group. Using Autograph she can select the service and view the attributes released on her behalf when she accesses the service via Shibboleth.

Personal details released:

nickname: Sue

Other details released:

affiliation: staff

given name: Susan

She noted that all service offerings are available to her (as she is a moderator, she is allowed to moderate, create, and read articles).

Available Service Offerings:

- Moderator**
 This service offering allows documents to be deleted and new document categories to be es ...
 - affiliation
 - nickname
 - surname
- Create access**
 This service offering allows new documents to be created and added to the repository.
 - affiliation
 - nickname
- Read access**
 This service offering allows all non-classified documents to be searched and downloaded.
 - affiliation

Due to privacy concerns, however, Sue does not wish to release her "sn" attribute to the service, and is satisfied with not having access to the Moderator level service. She denies release of the "sn" attribute by clicking on the trash-can icon, resulting in the Moderator level service no longer being available.



Attribute surname removed from identity card

The following information will be released when you go to the service "Macquarie

Personal details released:	Macquarie Physics Repository
nickname: Sue	Available Service Offerings: <input checked="" type="radio"/> Moderator This service offering allows c and new document categori <input type="button" value="Enable"/> <ul style="list-style-type: none"> affiliation nickname surname <input checked="" type="radio"/> Create access This service offering allows n created and added to the re <ul style="list-style-type: none"> affiliation nickname
Other details released:	
affiliation: staff	
given name: Susan	
<input type="checkbox"/> Release this information on all future visits to this service provider <input type="button" value="Go to Service Provider"/> <input type="button" value="Simple Display"/>	

ShARPE Development

This software is developed by the Meta Access Management System (MAMS) project at Macquarie University, Sydney, Australia. The MAMS project is funded by the Australian Federal Government's Department of Education, Science, and Training (DEST) as part of "Backing Australia's Ability" program. ShARPE and Autograph have been accepted as part of the National Science Foundation Middleware Initiative (NMI) EDIT software release.



australian access federation



Australian Government
Department of Education,
Science and Training

an initiative of

Backing
Australia's
Ability

The Australian Government's
Commitment to Innovation

References

ShARPE info: <http://www.federation.org.au/ShARPE>

MAMS: <https://mams.melcoe.mq.edu.au>

MAMS Federation : <http://federation.org.au>

NMI: <http://www.nmi-edit.org> & <http://www.nsf-middleware.org>

Contact Mail: sharpe@mams.org.au