PhiloIDG

This documentation will help you integrate your identity services with Philo through Internet2's NET+ program. Associated portions of the NET+ Identity Guidance Services are noted below.

Discovery and Authentication

An implementation of Philo involves hardware on the campus network. Through this, a vanity URL that can be used to invoke the service is created, e.g. philo.school.edu. This directs users specifically to the identity provider associated with the campus(1.1.1).

Discovery can also originate at third-party sites for channels(1.2.1). Users in this situation will have an interface by which they can navigate back to their school's Philo implementation and ultimately their school's identity system.

Attributes

Philo can consume the following attributes in a SAML response:

Philo Attribute	Recommended SAML Attribute Name	Optional
User Identifier	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	No

The user identifier must be understood by both the authentication system and the authorization mechanism in place. It is preferred that the identifier take the form of an email address or user identifier that is human legible in order to better support out-of-band processes.

Mapping of incoming SAML attribute to user identifier can be configured by Philo for each organization.

Privileges

Authorization of a user is performed by back-channel request using the user identifier supplied in the SAML assertion. This is preferentially performed by making a call to a campus authorization service through use of either a custom API or a standard protocol such as SQL or LDAP. Schools that do not have such an authorization system can supply a list of privileged users through another mechanism such as a CSV file or another structured plain text document available for download via FTP, SCP, etc.

Support for an explicit authorization attribute in the front channel and support for different viewership privileges are roadmapped.

Provisioning

Usernames received through authentication events in the front-channel are stored in a user record by Philo that also contains some other information about that user, e.g. an authorization and authentication event history.

User principal names or other personally identifying information is never supplied to any third party organization; a directed, opaque, persistent user identifier semantically similar to a SAML 2.0 persistentID is supplied, associated with privilege information. Philo is able to internally dereference these opaque identifiers to campus identifiers to enable specific workflows such as privilege validation.

These third party organizations may store additional user information, but associated only with the opaque user identifier.

Deprovisioning

Deprovisioning of user records or information contained therein only occurs when specific support requests are made to Philo.

Logout

There is a local logout button on the Philo player that will log the user out of their Philo session. Philo will be able to display custom information on that page.

Implementation

Philo uses samlr, an open sourced SAML library written in Ruby.

Metadata

Philo is an InCommon Federation participant with the entityID `https://sp.philo.com/sp` published in the metadata aggregate. Philo is able to acquire IdP information from metadata, including the InCommon aggregate, but is not able to consume metadata directly yet.

Example Configuration for SAML Implementations

TBD