Hellenic Academic Libraries Link

HEALLINK

Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Authentication and Authorization Infrastructure AAI

Shibboleth.

HEAL-Link Federation

Higher Education & Research

Exhibit – 2

Technical Specifications

&

Attribute Specifications

Trust Relationship

Trust relationship among the federation, federation members and federation partners is based on X.509 Public Key Infrastructure (PKI) technology, which enables mutual authentication. This is based on use of the SSL/TLS protocol and XML digital signatures using keys contained in X.509 certificates, conventionally obtained from Certification Authorities (CAs) that are recognized by HEAL-Link Federation.

Concerning the use of commercial Certificate Authorities for federation members should not be the only solution. Most of the federation members have their own Certificate Authorities due to various services they provide to their members. These CAs are acting according to service requirements set by the academic community. Besides that, there is a big cost in retrieving the certificates from a commercial Certificate Authority.

Therefore, HEAL-Link Federation will take into account the policies of the mentioned Certification Authorities and integrate them into the list of trusted Certificate Authorities.

Digital Certificates

HEAL-Link Federation; Certificate Roles

The protocols and profiles used by the federation make extensive use of X.509 certificates to carry the public keys used for various purposes. These certificates can be broken down into two main classes:

- Browser-facing certificates are visible only to a user's browser. Certificates from any certification authority (CA) may be used here; the main constraint being that the CA is accepted as trusted by the user's browser. The browser-facing certificates are:
  - o The identity provider's SSL server certificate seen by browsers (for example, on a user login page).
  - o The service provider's SSL server certificate seen by browsers (for example, on actual site pages being protected by Shibboleth and at assertion consumer service endpoints).
  - o Any SSL server certificates seen by browsers during the discovery process (for example, on local WAYF servers or at institutional portals).
- Trust fabric certificates are visible only to the identity provider and service provider software; the user's browser never sees them. Only certain certificate products are acceptable for this purpose; see below. The trust fabric certificates are:
  - o The certificate for the identity provider's XML signing key pair for SAML services.
  - o The certificate for the identity provider's SSL server key pair for SAML services.

- The certificate for the service provider's SSL client key pair for SAML services.
- The certificate for the service provider's XML signing key pair for SAML requests.

Software set-up is simplest when it is possible to choose the same certificate for use in all roles for a given entity. In this case, the browser-facing certificates and trust fabric certificates are combined.

Attribute Specifications

The AAI Attribute Specification is very important for the exchange of data among HEAL-Link Federation and Federation Participants. This document standardizes the attributes among all participating organizations. The format of the attribute definition is close to the LDAP syntax. This specification started with a basic set of attributes and is based on work of [Internet2] for the [eduPerson] specification. The set of attributes might get further extended in future versions, depending on attribute requirements of consumers (the resources) and the possibilities of the attribute providers (the home organizations) to supply them.

The home organization administrator's and resource owner's most important duty regarding attributes is the respect of privacy and data protection. Users perceive many of the attributes specified in this document as very sensitive information All people getting in touch with these attributes must fully respect user privacy and the relevant data protection laws and regulations which define how to deal with personal data.

Revealing attribute values can be a security risk. A good example to show that aspect is the unique identifier 'uid'. It could provide valuable information to a malicious third party. Its intended semantics is to be a user's identifier for authentication (aka login), possibly also on the home organization. It is thus security sensitive and home organization administrators should ponder carefully the decision to release the uid attribute to any resource, even within their organization. Conversely, resource administrators should not require the uid attribute unless they have a bilateral agreement with the home organization administrators. Note that Shibboleth is designed to not release the credentials used for the authentication at the home organization. Whenever information is handed out to third parties, the security risk involved must be carefully considered.

Home Organizations and Attributes

Home organizations collect and maintain the information, which should be made available through attributes. It is stored in a user directory, which can either be implemented using an LDAP compatible directory (e.g. OpenLDAP or Active Directory) or an SQL database. The home organization is responsible for **proper identity management** and **up-to-date personal data**. In

addition, it is also responsible for proper configuration of the Shibboleth Attribute Release Policy (ARP) defining which attributes may be released to which resources in order to protect the privacy of its users. Each home organization participating in HEAL-Link Federation has to implement at least the mandatory attributes as they are defined in this document.

Resource Owners and Attributes

The set of attributes needed by a resource depends on the service it offers to its users. The set may be minimal for anonymous services and rather large for highly personalized services with granular authorization. One thing that should be followed is that: according to the data protection principles, as few as possible personal data should be processed!

In addition, a resource owner should carefully consider which information to store across user sessions. The less information is stored, the smaller impact a potential misuse has in case of an incident. So it is the duty of the resource owner to specify which attributes are **really required** to offer the service and which **additional desired attributes** might allow him/her to offer optional advanced services. When defining their attribute requirements, resource owners should always check the attribute implementation status of HEAL-Link Federation. If a resource requires an attribute not (yet) implemented in the home organization of its prospective users, these users will not be able to access the resource. Therefore in case of an update at their required attributes, resource owners should notify HEAL-Link Federation in due time, in order for the proper action to be taken for the implementation of the new attribute.

The minimal requirements for users of HEAL-Link Federation in attributes are described below.

Mandatory Attributes for HEAL-Link Federation Participants

Entitlement (eduPersonEntitlement)

- Description
    - URI (either URL or URN) that indicates a set of rights to specific resources.
    - A simple example would be a URI for a contract with a licensed resource provider. When a principal's home institutional directory is allowed to assert such entitlements, the business rules that evaluate a person's attributes to determine eligibility are evaluated there. The target resource provider does not learn characteristics of the person beyond their entitlement. The trust between the two parties must be established out of band. One check would be for the target resource provider to maintain a list of subscribing institutions. Assertions of entitlement from institutions not on this list would not be honored.
    - This attribute is suitable when a home organization knows to which resources a

certain set of their students, staff etc. should have access to. The home organization knows their users and can therefore add a specific entitlement value to the entries of entitled users.

- Permissible values
    - *urn:mace:dir:entitlement:shared:common-lib-terms*
- Typical usage
    - authorization
- Origin
    - [eduPerson]
- OID
    - 1.3.6.1.4.1.5923.1.1.1.7
- LDAP syntax
    - Directory String

Optional Attributes for HEAL-Link Federation

TargetedID (eduPersonTargetedID)

- Description
    - A unique identifier for a person, mainly for inter-institutional user identification on personalized services.
- Semantics
    - <unique-local-ID> (local part)
    - It is an ID uniquely allocated by the home organization for a user that has been authenticated according to the local authentication policy. It has to be unique. It MAY NOT be reassigned, also if the former user left the home organization.
    - A home organization has to be able to identify the person matching that <unique-local-ID>.
    - TargetedID should not be exposed to end users; especially require a user to provide it manually.
- Typical usage
    - Personalization, authorization
- Origin
    - [eduperson]
- OID

- o   1.3.6.1.4.1.5923.1.1.1.10
- LDAP Syntax
  - o   Directory String
- Notes
  - o   It MUST NOT exceed 256 characters in length.

This Document is based on the corresponding documents of **JISC (UK federated access management)** and **SWITCHaai (Authentication and Authorization Infrastructure AAI Federation, Switzerland).**