Shibboleth Interoperability with the Athens Access Management System

David Orrell, EduServ, Queen Anne House, 11 Charlotte Street, Bath, BA1 2NE, UK
Email: David.Orrell@eduserv.org.uk
Keywords: Authentication, Authorisation, Security, Access Management, Shibboleth, Athens

Extended Abstract

Athens is the de-facto standard Access Management System (AMS) used throughout the UK in the Higher Education and Health sectors for Authentication and Authorisation of federated online subscription services (such as online publications and journals). It is developed and maintained by EduServ, a not-for-profit organisation based in Bath, UK. Athens provides single-credential authentication, true single sign-on (AthensSSO) access across multiple services, distributed administration, and statistical usage analysis. In the Athens system, single sign on is achieved by performing all authentications in a single domain (called the 'authentication domain'), via the Athens Authentication Point, and maintaining browser session cookies, tied to this domain. This means that whenever a user requires access to an AthensSSO service, they will traverse the authentication domain, the Authentication Point will recover their session, and transfer them to the service provider by the use of a short-term 'token'.

In Athens, authentication can either be performed via the central Athens database (which currently holds over 2.2 million users), or can be devolved to individual institutions (called AthensDA – Devolved Authentication). Centralised authentication is useful for small institutions, or institutions who do not have the required infrastructure for fully devolved authentication. In this case, user information is held by Athens on behalf of participating institutions, with extensive distributed administration capabilities provided for user management. User attributes are held in a pre-defined format which can be extended through the use of additional user profile data associated with a user account.

Devolved authentication is achieved by institutions authenticating users by a trusted local authentication system (such as an LDAP directory). The user is then assigned a particular role (a set of authorisation permissions) defined in the Athens AMS and this information is passed back to Athens and used in subsequent authorisation requests by service providers. The Athens Authentication Point then creates a 'virtual' Athens account for the user, which possesses the correct authorisation permissions for the particular user.

This paper focuses on the perceived advantages and disadvantages of devolved authentication over the more centralised model traditionally used in the UK. Moreover, the paper discusses in details, the similarities and differences between the architecture and authorisation mechanisms used by both the Athens devolved authentication model and Shibboleth, an emerging standard for user attribute sharing in a federated environment. The conclusion from this comparison is that Athens and Shibboleth have similar high-level architectures, but their emphasis is different. Shibboleth is focused towards attribute release (what information can and cannot be released about a given user), whereas Athens is more focused on providing a comprehensive access management framework. This encompasses both authentication and authorisation mechanisms, in both devolved and centralised scenarios.

As Athens has been in active use for a number of years there are inevitably a number of aspects of the system that are proprietary because they were introduced before suitable standards had been defined and adopted. However, the paper discusses how the existing Athens authorisation mechanism is being developed to interoperate with standards such as those for attribute acquisition defined by Shibboleth. The important advantage of this development in particular is that it will

allow service providers who use Shibboleth to seamlessly integrate with Athens, and conversely give Athens users potential access to services employing Shibboleth as their access control mechanism. Hence, users of Athens will have access to any participating Shibboleth service. This enables Shibboleth to be used to extend the authorisation protocol used between a service provider and the central Athens Database.

The requirements for Athens-Shibboleth interoperability are defined in the paper, and are briefly summarised as follows:

- The Athens Authentication Point (AAP) needs to act as a Shibboleth 'Where Are You From?' (WAYF) service. This is quite easy to achieve as all AthensSSO authentications already pass through the Authentication Point. What's more, AthensDA already has functionality almost identical to that of a WAYF service as part of its architecture. The main requirement for an interoperable system is that Shibboleth service providers have some means to refer users to the Athens Authentication Point. This effectively establishes Athens as a 'Shib-club' in its own right. An alternative mechanism would be to register Athens itself as an institution in an existing Shib-club, if such a club did pre-exist.
- The Authentication Point also needs to act as a Shibboleth Handle Service, and generate and return a handle back to the DSP after the user has been authenticated. This handle is used to identify a user to service providers in pseudonymous manner, similar to an AthensDA virtual account (although the handle shouldn't be persistent between sessions).
- There also needs to be an Athens Attribute Authority which can serve attribute requests for a particular user. This component also needs to perform mapping between user data currently held in the central Athens database, and the requested attributes. This mapping needs to be flexible and tied in to the Athens user profiling system. This would create an adaptable and extendable attribute mapping mechanism which would ultimately be compatible with a variety of different attribute schemas (eg. eduPerson).

The paper also proposes a data flow in an Athens-Shibboleth interoperable system, and defines both the new components of such a system, and modifications to existing components of the Athens AMS in order to achieve interoperability. Moreover, the paper discusses a proposed attribute mapping scheme between attributes held in the Athens database and those requested by service providers who have deployed Shibboleth to protect their content. This allows attribute requests from these service providers to be served on request.

The result of an interoperable system such as this is that it provides additional value to both service providers and Athens users: a user can benefit from being able to access Shibboleth protected services with an Athens account, and a service provider who has adopted Shibboleth can immediately interoperate with the Athens AMS and benefit from its established user base. This mechanism also delivers an additional interface to Athens, while still maintaining its comprehensive and proven range of facilities.

EduServ plan to develop a working demonstrator of an Athens-Shibboleth interoperable system by the end of March 2003.