



Eduserv Athens Implementation Standards

1.6

Eduserv Athens

Authored by: Eduserv Athens

Date: 26/11/04

Revised by: Tom Demeranville

Revised date: 29 March 2005

Eduserv Athens is a service of Eduserv Technologies Ltd.

1.	Introduction.....	3
2.	Legal Requirements	3
3.	Login /Logout.....	3
4.	Authorisation.....	4
5.	Personalisation.....	5
6.	Statistics	6
7.	IP address handling.....	6
8.	Athens testing.....	6
9.	General.....	7

1. Introduction

The Athens system provides an Access Management System to enable very large numbers of users to access multiple and distributed data services. Athens provides registered users with a single username/password combination for access to one or more distributed services, each service being provided by a Data Service Provider (DSP). The full range of facilities provided by Athens is described on the AthensAMS website – www.athensams.net.

The DSP must integrate the Athens Agent technology within the DSP's service software. The method of integration varies according to the server type, and these are described in the Athens DSP Integration Guide and corresponding Agent guide.

This document describes the implementation standards this integration must meet when implementing version 3.6.x of the Athens agent.

2. Legal Requirements

This section repeats sections of the Athens licence which are relevant to implementers:

- The DSP must make reasonable endeavours to implement new versions of the Athens software within one month of notification of the new version.
- The DSP must make best endeavours to implement service/security upgrades within 24 hours of notification.
- The DSP must formally report bugs as soon as they become apparent.
- The DSP must not modify or alter in any way the code Eduserv supplies, unless they have written permission from Eduserv.
- The DSP must only use the Athens software for the resources for which they have been licensed.
- A link to the Athens Authentication point must be provided on the service's main login page.

3. Login /Logout

The DSP should register with Athens a URL that takes the user directly to the Athens Authentication Point. Our preferred method is that a page for each Athens-authenticated service is created on the DSP's server that redirects users to an AAP.

The DSP should also ensure that the main login page for the DSP's service provides a means for an Athens user to login. This should provide a link to the Athens Authentication Point.

The DSP will be able to tailor the AAP to match their own service style. However the Athens reserved tags must be retained within this page.

If the service has a Logout function, then this must use the Athens logout template.

4. Authorisation

Athens users without access to a specific resource must not be able to access it. Further access decisions (such as those based on a users organisational identity, as discussed in section 6) can then be made independent of the users access rights.

In all cases the DSP must provide a clear error message describing a failure to authorise, in particular when users with valid Athens accounts are refused. The use of the Authentication Point for displaying error messages is encouraged for standard messages.

The DSP must ensure that targets within the service are also protected by Athens, and that any user going directly to a target within the service is unable to view the target without logging in beforehand.

Links to pages within a service must result in the target page being reached after authorisation. This is sometimes referred to as 'deep linking'.

5. Personalisation

If your service(s) offer personalisation features (e.g. saved searches, alerts, etc), only the Athens Persistent UID should be used to associate any local data with the user. This is because:

- some consortium-type organisations such as the NHS move their Athens accounts between organisations as employees move from one trust to another. Using the organisation ID or prefix/site code as part or all of the mapping causes these preferences to disappear
- some Athens organisations re-use account usernames, causing personalisation features to transfer to the new owner

The Athens Persistent UID is guaranteed to be unique for every user within an Athens federation.

6. Organisation identities

Checking the three character username prefix must not be relied on to identify a users organisation. In many cases, prefix checking does not differentiate between sub-organisations, and a proportion of users do not have an organisational prefix. A users home organisation is an attribute which can be queried using the Athens Agent.

The DSP cannot assume that because the user has a valid Athens user account, the user is from a certain sector (e.g. higher education, or the health service). The users organisation type can be discovered using the Athens agent, and the relevant installation guides illustrate how this can be achieved.

Athens will offer users the ability to link two or more user accounts, for instance an HE account and an NHS account. In these situations, the user will have multiple organisational attribute values and DSPs will have to cater for the receipt and processing of multiple values, particularly for organisation identity.

The Organisational identity is guaranteed to be unique within an Athens federation.

7. Federation Identities

Athens is introducing the concept of multiple federations within its namespace to facilitate the large scale adoption of Athens in the US. Organisation identities and persistent user identifiers will now only be unique within a single Athens federation and must be associated with a federation identity for uniqueness. Initially there will be two federations, one for the current set of Athens organisations, known as AthensUK and a new federation for the US called AthensUS. The federation identity is an attribute of the organisation and will be available to resources via the current attribute delivery mechanisms i.e. `read_personal_profile` for Java and C agents; and via environment variables in plug-ins.

8. Statistics

Once a user has been successfully authorised to use the resource or resources, then a call to the Athens agent statistics function should be made for these resources. The DSP must not log resources that the user is not authorised to use, or that the user has not logged in to use (i.e. for resources that are associated with another service that the DSP hosts). The user's IP address should also be included in the call to the Athens agent statistics function.

9. IP address handling

DSPs must submit the user's IP address with:

- the authentication call made by the agent
- the logging of Athens usage statistics

The hostname is not necessary.

10. Athens testing

A service will not be made live with Athens protection unless it has been successfully tested against the Athens Validation Tests. Sufficient time must be scheduled to allow the Athens team to test the implementation of the Athens agent, and for any problems to be corrected. The DSP must check that the service meets the test criteria by checking it against the validation tests which can be found by logging into the Athens DSP Administration at https://www.athensams.net/dsp_area/ and selecting the 'Documentation' link. As soon as the Athens team receives written confirmation that the service passes the validation tests, they will carry out final testing. When this has been successfully completed, the service will be officially signed off and the DSP can then proceed with the allocation of the resource sites.

Eduserv Athens reserves the right to decline acceptance of an Athens implementation if it is deemed to be unsatisfactory for any reason.

DSPs are obliged to carry out any necessary internal procedures to enable the Athens team to fully test their service. That is, Athens should be able to log into the service using the Athens team's own accounts. Please ensure that the appropriate Athens organisation ID for the Athens team accounts (3032813) is entered into your customer

records. Athens would request that these test accounts are retained as long as the DSP uses Athens authentication, as this enables the Athens team to perform diagnosis of user problems at any time.

11. General

If an Athens protected resource denies access for other reasons, such as:

- use of a particular browser
- cookies enabled
- registration needed

then these reasons must be clearly explained to the user when access is denied.

DSPs must support the use by users of both 'personal' and 'access' accounts, unless they have been given specific written permission to the contrary from Eduserv.