



# Local Authentication Integration Standards

1.0

---

## Eduserv Athens

**Authored by:** Lyn Norris

**Date:** 28 June 2005

---

**Revised by:**

**Revised date:**

---

*Eduserv Athens is a service of Eduserv Technologies Ltd.*

## Changes to this document

<b>Date</b>	<b>Version</b>	<b>Author</b>	<b>Summary of changes</b>
28 <sup>th</sup> June 2005	1.0	Lyn Norris	First version

## Copyright notice

Copyright 2005 Eduserv. All rights are reserved. No part of this documentation or software may be reproduced in any form or by any means or used to make derivative work without prior permission from Eduserv.

Eduserv periodically changes the information in this documentation; changes are incorporated into new editions. Eduserv reserves the right to change product specifications without notice. Eduserv shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the use of this material. Athens is a registered trademark of Eduserv.

- 1. Introduction ..... 4
- 2. Legal Requirements ..... 4
  - 2.1. Licences and Terms & Conditions ..... 4
  - 2.2. Upgrades ..... 5
- 3. General considerations ..... 5
  - 3.1. User identifiers ..... 5
  - 3.2. Terminating Athens sessions ..... 6
- 4. Athens testing ..... 6
- 5. Specific tests ..... 7
  - 5.1. Security ..... 7
  - 5.2. General ..... 7
  - 5.3. Attributes ..... 7

## 1. Introduction

If an organisation already has an established set of usernames and passwords, it may make sense to enable these accounts for access to Athens-protected resources, rather than create a new set of usernames and passwords in Athens (classic Athens).

The policies for issuing, managing and securing these local usernames must meet the Athens guidelines for the secure management of usernames and passwords. Also, the organisation must agree to the [Athens Terms and Conditions](#) which require the organisation to guarantee that users will only be permitted access to Athens-protected resources to which they are entitled under the terms of the licence of the resources.

There are a number of ways in which a local authentication system can be integrated with Athens:

- Using Shibboleth protocols (see [Shibboleth to Athens Integration Guide](#). For more information please go to [our Athens & Shibboleth page](#))
- Using SAML (see [Athens/iChain](#))
- Using Athens Devolved Authentication (AthensDA) (see [AthensDA](#))

This document describes the implementation standards that any local integration of Athens must meet when accessing Athens-protected resources through the Athens UK Federation.

For more information, see [http://www.athensams.net/local\\_auth/](http://www.athensams.net/local_auth/).

## 2. Legal Requirements

### 2.1. Licences and Terms & Conditions

The following licences and terms and conditions are relevant for organisations using Athens Local Authentication facilities:

- The licence for the organisation's use of Athens, which may be an umbrella licence e.g. for JISC supported organisations or NHS England, or a separate licence for the organisation
- The organisational and user Terms and Conditions as described at [http://www.athensams.net/terms\\_and\\_conditions.html](http://www.athensams.net/terms_and_conditions.html)
- The username password policy for this Local Authentication system

A summary of the requirements is as follows:

- The organisation must take reasonable steps to:

- Ensure that access to an Athens-protected resource is only given to individuals who are authorised to access that resource under the terms of the licence for the resource
- Terminate access for Athens enabled accounts promptly when appropriate
- Keep Athens-enabled usernames and passwords confidential
- Ensure that information provided about Athens enabled account holders is accurate
- Investigate cases of suspected abuse
- Users must:
  - keep the account confidential and not permit any third party to use it
  - use it for the purpose for which it was issued by the organisation
  - accept the terms of the Eduserv Athens Privacy Policy

## **2.2. Upgrades**

Note that the standard Athens organisational [Terms and Conditions](#) require an organisation to upgrade their Local Authentication implementation within three months of notification by Eduserv; and to implement security fixes to the protocol within 24 hours.

## **3. General considerations**

### **3.1. User identifiers**

The protocol requires that a user identifier is passed to Athens for each Athens session. This is used to identify the session, and in cases of suspected abuse will be used to identify the user. Organisations are required to provide an audit trail of such identifiers so that the individual can be identified.

The user identifier is also used by Athens-protected resources to provide a key to user profile information within a target application. Although a persistent identifier may not be required by an Athens resource, failure to pass one to Athens may cause access to be denied by a resource provider, or at the very least mean that information relating to given users (such as personalisation) within a given application may not be available. Athens therefore strongly recommends persistent user identifiers.

Implementers should be aware that any change to user identifiers will cause loss of personalisation for users. Unfortunately this also applies to a move from classic Athens accounts to local accounts.

### **3.2. Terminating Athens sessions**

When a user logs out of his local authentication system, the Athens session should also be terminated. The simplest way to achieve this is to forward the user to the following page:

[https://auth.athensams.net/?ath\\_action=ssologout](https://auth.athensams.net/?ath_action=ssologout)

This would leave the user at our page. If you specify our return URL parameter, we will direct the user back to a page of your choosing. This parameter needs to be URL encoded (see <http://tools.devshed.com/webmaster-tools/url-encoding/> for a web based encoder). The final URL you would need to use, assuming you want to redirect users back to "http://lib-mlsfx.lancs.ac.uk:8331/V" would be:

[http://auth.athensams.net/?ath\\_action=ssologout&ath\\_returnurl=%22http%3A%2F%2Flib-mlsfx.lancs.ac.uk%3A8331%2FV%22](http://auth.athensams.net/?ath_action=ssologout&ath_returnurl=%22http%3A%2F%2Flib-mlsfx.lancs.ac.uk%3A8331%2FV%22)

## **4. Athens testing**

A local authentication system will not be made live with Athens protection unless it has been successfully tested against these Integration Standards. Sufficient time must be scheduled to allow the Athens team to test the integration, and for any problems to be corrected. The organisation must check that the service meets the test criteria by checking it against these standards. As soon as the Athens team receives written confirmation that the system passes the tests, they will carry out final testing. When this has been successfully completed, the service will be officially signed off and the organisation can then proceed to use the system for access to Athens-protected resources.

The test federation – touchstone – is available for organisations to trial their integration and for the Athens team to execute their testing. No Local Authentication system will be accepted into an Athens production federation until it has been successfully tested against the test federation.

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

Organisations are obliged to provide the Athens team with the necessary credentials to enable them to fully test the Local Authentication system. Generally this means that Athens should be provided with usernames, passwords and suitable attributes for test purposes. These credentials should be retained as long as the organisation uses Athens authentication, as this will enable the Athens team to perform diagnosis of user problems at any time.

## **5. Specific tests**

### **5.1. Security**

- All usernames and passwords must be encrypted when transferred over the Internet
- Each identifier supplied to Athens must uniquely identify an individual
- An audit trail must exist to allow an individual to be identified by your organisation when given the identifier passed to Athens and a timestamp
- Your systems must be synchronised with the Network Time Protocol (ntp) to ensure that the timestamps in your logs are close to those in the Athens logs
- The unique Local Authentication Identifier as supplied by Athens must be passed in every authorisation call.
- It must be possible for users to terminate their Athens session.

### **5.2. General**

- A successful organisation login must provide access to the correct Athens-protected resources
- An unsuccessful organisation login must not allow access to any Athens protected resource
- An unsuccessful organisation login must provide a sensible error message to the user
- You must be able to remove access to an Athens-protected resource for a single individual to be used in cases of suspected misuse

### **5.3. Attributes**

- Attributes passed to Athens must comply with the [Eduserv Athens Attribute Schema](#)
- No personal information as defined by the UK Data Protection Act should be passed by you in attributes without the express permission of the individual