



Authenticated Networked Guided Environment for Learning

Authentication: the process of making sure that a user is who he claims to be by asking for proof.

Authorisation: the process of establishing whether an authenticated user is permitted to access a given resource, and what rights they have over that resource (e.g. Read, edit, print etc.).

Authentication and authorisation are separate services, which are often confused as one process. Authentication simply accepts that the identity information given by the user is valid. Authorisation connects the user to the resources he needs. Authorisation often happens implicitly alongside authentication, allowing users to automatically enter an environment where accessible resources are available, and all other resources are hidden. It is perfectly possible (and often desirable) for authorisation to happen on an individual resource level, with right-to-access being established as a user clicks a link.

ANGEL's process of achieving authentication and authorisation.

Angel offers a middleware solution to the problems of authentication and authorisation and has the ability to use a variety of protocols for these purposes. For authentication, a username and password (or certificate where appropriate) can be matched against an institutional network authentication service, or an LDAP server (typically part of a modern e-mail gateway) or against records held by an MIS system or VLE. When the user is found, a list of rights groups for that user is created. This process occurs across a secure connection so that passwords are encrypted. This allows access to permitted users from outside a secure area, thus allowing students to access information from off-campus.

When an authorisation request is received from a resource, ANGEL compares the rights groups list of the user to the rights groups list connected to this resource within the Resource Manager. The appropriate credential for the resource is then created and a response to the authorisation request is generated. This credential is typically a web cookie with a short expiry time.

The ANGEL User Manager is intended as an institutional solution to authentication and authorisation. This gives institutions the freedom to choose a preferred authentication system, or use different authentication services to query different directories of user information. This means that users can be issued with one set of authentication credentials (a username and password, a certificate etc.) and these can be used to access a variety of systems such as the Library patron information system, the institutional VLE / MLE, course portals and initial network log-on.

Using Shibboleth and PAPI

Shibboleth and PAPI are both systems that manage the authorisation of authenticated users, normally to external services. They both utilise certificate and cookie credentials. Use of these credentials for authorisation means that content providers do not need to keep track of users from institutions licensed to use the resource, and allows publishers to move beyond the easy to manage but restrictive IP-based solutions currently in favour. This in turn means that institutions are able to offer users the ability to access resources from home or while abroad.

TECHNICAL BRIEFING ONE THE ANGEL APPROACH TO AUTHENTICATION AND AUTHORISATION



Authenticated Networked Guided Environment for Learning

What is a rights group?

Permission to access a resource is generally assigned to a 'group' rather than an individual, for example access to certain resources may be permitted to postgraduates, but not to undergraduates. A user may belong to many different groups with an educational institution: the undergraduate student group, the English department group, the Victorian Literature course and so on. Information about the group each user is assigned to is generally stored in a student record within an institutional network. When an authentication service queries a directory service (such as the Student Record System) for user information, details about the groups a user belongs to can be returned. This information can be configured as a list of groups to which the user is assigned, thus determining the rights a user has. This has privacy benefits as only non-specific information about the user is passed to services.

Managing electronic identities.

In order for the user to seamlessly access all services which require **authentication**, detailed information about the services the user is **authorised** to access is needed. This requires data to be gathered and stored by institutions in an agreed format. The process also requires the storage of more complex metadata than institutions currently undertake.

In order to achieve this, UK HE and FE communities require a unique namespace to support a range of directory-based applications which involve the sharing of personal data between institutions, and between institutions and data providers (commercial and non-commercial). More information about the use of directories and namespaces can be found in Technical Briefing One: the Middleware Concept.

What is happening to Athens?

Athens authentication is now well-established within UK HE, but the current service does not offer the

functionality required for future national access management services. Currently, Athens is not based on open international standards (its code and protocols remain proprietary to Eduserv). The Athens service is developing a service, Athens Distributed Authentication, to address some of these issues but have not as yet reached a production service. JISC are currently considering the potential of using an Athens system as an authorisation facility for JISC services, whilst using digital certificates as the main credentials for establishing user identity.

Proposed JISC solution

As part of the development of the Information Environment, the JISC faces the problem of creating a national authentication and authorisation service that is maintainable across UK HE and FE, but that allows for flexibility and institutional control. A solution using X.509 certificates has been proposed. This system would allow institutions to continue managing electronic identities for members, but would require the certificate created for each user to be signed by a national JISC service.

How are these developments supported by ANGEL?

The ANGEL project is supporting these developments by:

- ◆ Offering an open source standards-based framework in the form of the ANGEL User Manager that will support a variety of authentication and authorisation procedures, including the opportunity to use X.509 certificates.
- ◆ Testing two of the major authentication schemes available in the form of PAPI and Shibboleth.
- ◆ Working with JISC to establish best-practise scenarios for managing electronic identities within the UK educational sector. This includes the development of a proposed namespace schema for the UK educational community, and analysis of current resource licensing issues.