The ‘A2Z Project’: Akenti Access to zetoc

Report 1: Results of the trial implementation of the authorisation software, Akenti, for the bibliographic reference and notification service, zetoc.

Authors: Ross MacIntyre(1), Mike Jones(2) and Ashley Sanders(1)

Affiliations:
(1) MIMAS, Manchester Computing, University of Manchester
(2) ESNW (E-Science Centre North West), Manchester Computing, University of Manchester.

Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.7</td>
<td>Nov 2003</td>
<td>Draft for discussion with LBNL</td>
</tr>
<tr>
<td>0.8</td>
<td>Dec 2003</td>
<td>Incorporated comments from LBNL</td>
</tr>
<tr>
<td>1.0</td>
<td>Dec 2003</td>
<td>Final version submitted to JISC</td>
</tr>
<tr>
<td>1.1</td>
<td>Dec 2003</td>
<td>Revision to Observation concerning PERMIS</td>
</tr>
</tbody>
</table>

Acknowledgements
The authors acknowledge the assistance of the following members of staff in the work associated with this report:
Manchester Computing: Andrew Weeks and Geoff Lane
ESNW: Stephen Pickles
Lawrence Berkeley National Laboratory[LBNL]: Mary Thompson and Abdelilah ‘Abdou’ Essiari.

A2Z is funded by the Joint Information Systems Committee [JISC] of the UK Higher and Further Education Funding Councils.
Table of Contents

1 Introduction..................................................................................................................3
  1.1 Background
  1.2 Scope
  1.3 Overview

2 Evaluation Environment...............................................................................................4
  2.1 Application
  2.2 System

3 Requirements................................................................................................................6
  3.1 Authentication
  3.2 Authorisation

4 Results..........................................................................................................................7
  4.2 Access Control
  4.3 Application Data

5 Technical Detail..........................................................................................................11
  5.1 Installation of Akenti
  5.2 Configuration of Akenti

6 Observations..............................................................................................................16
  6.1 Manchester Computing
  6.2 Response from LBNL

7 References..................................................................................................................18

Appendices
A1 Successful Access Messages.....................................................................................19
A2 Unsuccessful Access Attempt..................................................................................20
A3 Apache-created Environment Variables.................................................................21
A4 Configuration Files for the A2Z Web Site...............................................................24
A5 Configuration Files for the JISC TAU
   Academic Attribute Certificate Generator ...............................................................32
A6 Example Institutional Attribute Certificate..........................................................35
A7 Example JISC TAU Academic Attribute Certificate.............................................36
The ‘A2Z Project’: Akenti Access to zetoc

1 Introduction

1.1 Background

In response to the JISC Circular 6/02: JISC Programme in Authentication, Authorisation and Accounting, Manchester Computing (MC) and the e-Science Centre for the North West (ESNW), both at the University of Manchester, proposed the implementation and technical evaluation of the authorisation system, Akenti [Akenti].

The authorisation evaluation would be conducted in the context of an existing current awareness service zetoc [zetoc], hosted by MIMAS [MIMAS], a section within MC. The system would be made accessible, firstly as a web server (through digital certificates embedded in the user’s web browser along side traditional Athens authentication) and secondly as a web service (using GSI authentication).

The aim being to evaluate Akenti in a ‘real’ service environment; exploring some of the technical and managerial issues associated with an authorisation system for an environment consisting of distributed resources, used by distributed users.

The proposal was discussed with the Akenti Development Team, led by Mary Thompson, Secure Grid Technologies, Lawrence Berkeley National Laboratory, California, USA[LBNL].

The EPSRC-funded e-Science pilot project myGrid [myGrid] would provide the environment for evaluating the interoperability with praxis gaining currency in the UK e-Science programme.

1.2 Scope

This report documents the results of the first stage of the project, the implementation and configuration of Akenti for zetoc.

1.3 Overview

A2Z uses UK eScience [eScience] X509 certificates to identify people via the same zetoc web interface familiar to the user, minus the username password authentication step. Behind the scenes, complex sets of rules exist some of which are issued, signed and maintained by people representing the British Library (stakeholder for the data) and others by people representing JISC (stakeholder for the storage and service delivery mechanism). Users are issued with Attribute Certificates (i.e. certificates which tie an X509 certificate to an attribute e.g. group or rôle) which the stakeholders may wish to require as part of their access policy.

This paper highlights how Akenti has been employed to describe and evaluate the authorisation rules required to use the zetoc service. It highlights the minimal impact to the user and shows how a resource such as this can be controlled in a highly distributed framework.
The ‘A2Z Project’: Akenti Access to zetoc

2 Evaluation Environment

2.1 Application

The zetoc service provides (z39.50-compliant [z39.50]) access to the British Library's Electronic Table of Contents (ETOC) database. This contains over 20 million records corresponding to journal articles and conference papers going back to 1993. They cover 20,000 current journals and 16,000 conference proceedings published per year covering all subjects in science, technology, medicine, engineering, business, law, finance and the humanities. Around 100,000 of the journals included are available for electronic data delivery (EDD) download. The database is updated daily with approximately 10,000 new records. Copies of all the articles and conference papers listed on the database can be ordered online from the British Library's Document Supply Centre.

The service can be viewed as consisting of two types of function: Search and Alert. Each has slightly different requirements, due to its functionality, described below.

zetoc Search provides a search interface accessible as a web form (or via the z39.50 target). Access is controlled firstly by an IP-check of permissible network addresses and domains. If a corresponding site is recognised as being eligible, access is granted and a site identifier passed to the application. Should this check fail, the user is prompted to enter their Athens [Athens] username and password. If successful, access is granted and a site identifier passed to the application. In both cases, this site identifier is the unique three-character identifier allocated by Athens, e.g. ‘man’ = University of Manchester. This site-id is subsequently used by the application to test for institutional-specific settings and preferences.

zetoc Alert is a current awareness service which will email a user the table of contents from particular journals and/or details of articles or conference papers which match some pre-defined search criteria, such as an author's name or keywords from the title. Users may create multiple Alerts. These email Alerts are sent on the day the new matching data is loaded into the database. As these lists need to be associated with a particular user, some form of persistent, derivable identifier is required, to allow subsequent access for update by the user. For this reason, Athens login is mandatory. The Athens username is used to identify all associated Alerts. (There are some functional differences depending on whether the Athens username is a ‘Personal’ or ‘Access’ account, but they are not relevant to this particular project.)

The zetoc data is received in SGML format via ftp from the British Library, converted, then loaded into an OpenText BRS/Search database. zetoc Search cgi-script and its z39.50 origin and target are all written C. zetoc Alert is written in C++.

2.2 System

The service runs on ‘Irwell’, a shared server comprising of a Sun E6500 running Solaris 8. This hardware is used to host many services, principally for the UK Higher and Further education communities. It was funded by the JISC and is located in the Kilburn building at The University of Manchester. Services installed currently range
The ‘A2Z Project’: Akenti Access to zetoc

from data accessible directly through the operating system and the packages available to analyse these data to online services available via web delivery.

During the first stages of the project a copy of the Apache web server (version 1.3.23) was set up. There are many instances of this software running on the server for other online services. The web server was installed along with the mod_SSL[modssl] module to allow secure access: mutual authentication and encrypted data transfer. It is only the Authentication that is of interest to this project.
The ‘A2Z Project’: Akenti Access to zetoc

3 Requirements

3.1 Authentication

Akenti requires the use of X509 digital certificates.

3.2 Authorisation

The access policy for zetoc offers an interesting model as it must reflect and satisfy the requirements of a number of stakeholders, users and support organisations:

1) The British Library ‘own’ the data. They have licensed it, at zero cost, for use by the UK’s Higher and Further Education communities, UK Research Councils and other sites served by JISC. Also, subject to a non-zero licence fee, to the English and Scottish NHS Regions (discussions with the NHS in Wales and N.Ireland have not concluded). They have also stipulated that access should be granted to zetoc Search for BL-registered readers whilst they are physically in the BL Reading Rooms.

2) JISC funded the server and support costs. They have licensed zetoc, at zero cost, to JISC-Supported sites (see Note below), but impose a non-zero licence fee for all eligible non-JISC supported sites, such as Research Councils, Irish Higher Education Institutions, CHEST Associates (see Note below) and the NHS.

3) MIMAS developed, host and support the service. MIMAS invoice institutions on JISC’s behalf, keep a record of subscriptions and maintain data integrity and personalised functions.

4) Institutions who have licensed zetoc. They may specify configuration settings, for example relating to mediated Document Supply.

Note: JISC-supported sites are those sites for which JISC receives government funding (via relevant official funding councils) to provide services. A list of these sites is maintained by their Technical Advisory Unit [TAU]. CHEST [CHEST] negotiate agreements on behalf of JISC. The agreements are usually also available to a slightly wider group of CHEST ‘Associate’ sites. NHS = UK National Health Service, consisting of regions grouped by the 4 nations England, Scotland, Wales and N.Ireland.
The ‘A2Z Project’: Akenti Access to zetoc

4 Results

4.1 Summary

Akenti is a security model and architecture that aims to provide scalable security services in highly distributed network environments.

It makes use of digitally signed certificates capable of carrying:
- user identity authentication,
- resource usage requirements ("use-conditions"),
- user attribute authorizations ("attribute certificates"),
- delegated authorization;

and makes decisions based on policies split among on-line and off-line entities.

A2Z uses UK eScience X509 certificates over https to identify people via the same zetoc web interface familiar to the user (figure 1). This does away with any username password step.

Figure 1 The zetoc Search interface via A2Z (Note some certificate data is deliberately being displayed.)

The zetoc Alert interface via A2Z has not been altered, however, the method by which the user’s Alert lists are identified was altered, as documented in 4.3.

Behind the scenes, complex sets of rules exist (see figure 2). These rules are issued, signed and maintained by the stakeholders. Users are issued with Attribute Certificates (mapping their X509 certificate to a rôle or a group). The stakeholders may require these as part of their authorisation policy.
Figure 2 Akenti Authorisation

When the A2Z web server in figure 2 receives a request to access either of the zetoc services (i.e. Alert or Search), it checks the https connection for a recognised valid certificate. If no certificate is presented the user cannot get any further and is told so.

If authentication is successful the user’s X509 certificate and IP address are passed to the ‘Authentication Black-box’ (see Figure 2 above). This will return one of three options:

- **read** – access to the data,
- **write** – the user may customise the interface for other users,
- **neither** – authorisation cannot be found for that user.
The ‘A2Z Project’: Akenti Access to zetoc

The ‘Black-box’ decides this using a capability certificate issued by the Akenti engine. It invokes the Akenti engine with the user’s X509 certificate. Akenti reads and verifies its Root Policy and user certificate. It then collects and verifies use condition certificates that the policy directs it to. The use conditions specify the location of attribute certificates and other requirements e.g. location or receipt of fees. The engine evaluates all attribute certificates and any X509 based constraints and returns a capability certificate containing full or conditional rights.

Finally, the ‘Black-box’ is left to evaluate any conditions on the returned capability before it grants or denies access.

4.2 Access Control

Authority to use zetoc in A2Z has been implemented based on meeting the requirements of the two primary stakeholders:

1) The British Library’s use conditions allow access to readers in the Reading Room, anyone from UK academia, anyone from NHS Scotland providing a licence has been paid or NHS England.

2) JISC’s use conditions allow access to British Library readers, UK academics from the ‘TAU’ list: Higher/Further Education and Research Councils which must have a licence, ‘CHEST’ Associates with a Licence and any member of the NHS in the UK with a regional licence.

Due to the large number of institutes on the JISC TAU list it was necessary to create a further Akenti-based service. This is an automated web-based interface that generates a TAU attribute certificates upon the successful evaluation of attributes issued at the institute level.

Akenti has been designed to use use-conditions with a high level of granularity. The aim is to allow stakeholders to add and remove authorisation on a condition-by-condition basis. Conditions may be marked as “critical” or “non-critical”. If a condition is critical it must be satisfied.

This basis is not suitable for the zetoc service where a condition from the British Library and a condition from JISC must be satisfied. Therefore A2Z bundles all Library conditions into one large critical use condition and does the same for all JISC conditions.

4.3 Application Changes

The changes to the zetoc search for A2Z were fairly simple.

After the normal checking for valid IP addresses and Athens a check is made to see if the network connection to the user is via https (rather than http.)
The ‘A2Z Project’: Akenti Access to zetoc

If it is https, then check made if the SSL_CLIENT_S_DN and SSL_CLIENT_I_DN environment variables have been set by Apache. An error is reported if they are not set and access is denied.

If the variables are set and this is the start of a new session, then a call is made to the ‘Black-box’ script and check its return value. If the ‘Black-box’ says this user is okay, then note is taken of their SSL_CLIENT_S_DN against this session and the user continues.

If the ‘Black-box’ says the user is not okay, they are shown a screen saying they are not authorised and access is denied.

On second and subsequent access to this session the SSL_CLIENT_S_DN variable is checked against the one stored for the session and access is only allowed if they are identical. This saves having to call the ‘Black-box’ for every web page displayed to the user.

Changes were also made to allow the users certificate details be displayed on the main zetoc search page.

4.4 Application Data

The Alert has to be associated with the individual, so a persistent identifier had to be found. This may change in future to be an attribute passed post authorisation, but will initially be the user’s distinguished name (SSL_CLIENT_S_DN).

e.g. SSL_CLIENT_S_DN= 
"/C=UK/O=eScience/OU=Manchester/L=MC/CN=ross macintyre"

No one else should have that name, as only UKeScience Certificates are supported for this project and the policy of the certificate authority (CA) dictates that the CA will not issue two certificates with the same DN at the same time (plus some other constraints) It was therefore safe to use SSL_CLIENT_S_DN to Identify an individual. If it was decided to accept other CAs then SSL_CLIENT_I_DN would also be needed to establish the correct context.

Appendix 3 shows the environment variables available. Conveniently, the string could be used to directly create subdirectory structures within the Unix environment. This would not be sufficient in a live environment, as there may be eScience certificate holders who are not members of an eligible institution.

Within zetoc Search a number of application settings are institution-specific. For the purposes of this evaluation, the IP address is checked to determine the institution. This would not be suitable for a live environment. This is a follow-on from the generic ‘Where Are You From?’ (WAYF) issue.
The ‘A2Z Project’: Akenti Access to zetoc

5 Technical Detail (and additional commentary)

The following section has been structured to mirror that of the PERMIS/Akenti Comparison report by Chadwick [Chadwick].

5.1 Installation of Akenti

5.1.1 Code download

Both Akenti Version 1.1 and version 1.2a were downloaded at times of their release. Obtaining the software was straight forward. Software is located on the LBNL web server [http://www-itg.lbl.gov/Akenti/](http://www-itg.lbl.gov/Akenti/) The software was, at this time, available in source and binary versions. Binary versions were available for Solaris and for i386.

It was noted that the Akenti software required many other items of software as prerequisites:

- Java JDK>=1.3 (JDK 1.3.1 available on Target Machine)
- OpenSSL (Already available on Target Machine)
- OpenLDAP download from [http://www.openldap.org/](http://www.openldap.org/)
- Xerces version 2 (obsolete) downloaded from [http://archive.apache.org/dist/xml/xerces-c/Xerces-C_2_0_0/](http://archive.apache.org/dist/xml/xerces-c/Xerces-C_2_0_0/)
- Java security packages jsse, jce, the Java LDAP classes, jndi downloaded from [http://java.sun.com/products/OV_stdExt.html](http://java.sun.com/products/OV_stdExt.html)
- Mod_akenti was also downloaded (requiring Akenti v1.1)

5.1.2 Setting up environment

Machine: irwell.mcc.ac.uk a 24 processor Sun E6500 running Solaris 8.

A user was created under whose UID all the relevant configuration was controlled. An Apache (1.3.23) webserver with mod_SSL[modssl] was installed:

The domain name a2z.mimas.ac.uk was registered as an alias for irwell.mcc.ac.uk. The Apache server was configured to listen for requests to this host.

A UK eScience server certificate was obtained with the distinguished name:

```
/C=UK/O=eScience/OU=Manchester/L=MC/CN=a2z.mimas.ac.uk/Email=mike.jones@man.ac.uk/
```

During the SSL handshake this identifies the web server to the user and guarantees its authenticity. The UK eScience Certificate Authority runs a non-standard practice whereby it issues certificates with the locality field ‘L’ containing information to identify the authorising Registration Authority not the Geographical location of the owner of the private key. The “Email” flag (aka “emailAddress”) is a requirement under the UK eScience CA’s CPS for all non-personal certificates.

The web server was configured to accept https connections. After the server has identified itself the user may identify themselves by using their certificate in the same SSL handshake. A secure context is then set up and if the user presented a certificate s/he is then able to use the web pages as though they had passed a username password challenge.
The ‘A2Z Project’: Akenti Access to zetoc

To identify the user the web server needs to relate the user’s certificate to a CA’s public key. The UK eScience CA’s root certificate was installed into the corresponding configuration of the SSL enabled web server. A cron job was also set up to download, verify and install the UK eScience’s Certificate Revocation List. The CRL contains a list of certificates issued by the CA that it believes it can no longer guarantee the authenticity of the possessor.

The web server was set up to allow Common Gateway Interface programs to be executed.

Akenti was installed in the directory $HOME/akentiDist and the policies were stored in a directory structure under $HOME/A2Z. A copy of the zetoc software was installed in the same location as the apache software $HOME/apache

5.1.3 Installing the software

Installing the software was not trivial. During the compilation of the source various bugs were found. Most of these related to the Java Version and generated Makefiles. The installer was not a Java expert and it was envisaged that deployment in the field would not require in-depth Java knowledge.

Akenti version 1.1 was downloaded and was found to require many prerequisites not already installed on the server. Most notable a deprecated version of Xerces which was not easy to find. Open LDAP and its prerequisites were then downloaded and installed. Even this installation was not without difficulty.

An attempt was made to compile Akenti 1.1 which produced many errors based upon the installation environment. The binary version was then downloaded and installed. This was done to get an idea of configuration of the Java environment. It was not used as part of this evaluation other than for this reason.

Akenti version 1.2a was downloaded and was found not to compile ‘out of the box’.

The second stumbling block was that our user environment was not large enough to contain Akenti and all its prerequisites. The directory was then stripped down leaving only the required libraries and include files. During the compilation phase, on at least three occasions an increase of quota had to be requested from the system administrators (a process by which one’s request joins a queue of administrative tasks to be approved then executed). The user space quota eventually was increased to 1GB. Akenti occupies approximately 650MB and the non-system prerequisite software a further 50MB

At this point Abdelilah Essiari from LBNL arrived and debugged A2Z’s version of the Akenti code as follows:

1. Noting the errors in the compilation referring to Unrecognised use of Java Exceptions for the version of Java used: The exception statements were located and removed from code.
The ‘A2Z Project’: Akenti Access to zetoc

2. Found not to compile due to Makefile references pointing to files in incorrect places; too many "../" in a number of Makefiles. Symbolic link were created in AKENTI_HOME/../ When found to compile, the relevant Makefiles were found and modified.

Akenti v1.2a was finally installed and working on March 27.

5.2 Configuration of Akenti

5.2.1 Using the software

Two methods were available to configure Akenti once installed: using the java/swing Graphical user interface, and/or using command line. The GUI would be the preferred method to use in the field. However, various bugs and features made the use of this interface difficult in our case. zetoc required complex logical expressions in the use conditions (described below). The GUI was not able to express these in an intuitive way and a syntax mismatch caused difficult to spot errors. – During the LBNL visit to Manchester these were discovered and our version of Akenti was patched to deal with this.

Due to the complex nature of the policies required the editing of these policies in raw XML and their signing via the command line tools were the preferred method.

There is one caveat with the command line option. Signing actually produces an encoded Akenti certificate which is tagged onto the end of the XML file. It cannot then be altered and resigned without first removing the Akenti component as the Akenti component is not in XML format.

A second security issue was noticed in that the signing tools of Akenti would only allow the password of the encrypted signer’s key to be passed on the command line. Therefore during the signing process (the order of a few seconds) the password protecting this private key is visible to any user at the time logged onto the system.

5.2.2 Making the Authorisation Decision

At the start of this project it was envisaged that Mod_Akenti would be used to evaluate the underlying authorisation challenges. However, it turned out that Mod_Akenti only works with Version 1.1 of Akenti which we could not compile. Therefore we chose to invoke the Akenti engine via a CGI perl program called blackbox.pl.

The Akenti engine returns a Capability Certificate that only Akenti knows how to decode, verify and evaluate. This is useful for systems where this evaluation takes place in a different location to the service requiring the authorisation decision. A2Z however, makes a decision in the same place as the request is generated. Therefore a second tool was used to interrogate the certificate issued locally by the engine. The result is a quantity of text which is parsed by the blackbox.pl using regular expressions. At this point a tool converting the Certificate to XML would have been preferred.
5.2.3 Creating a basic policy

The policy is made up from a root policy and use conditions.

5.2.4 Creating a root policy

This is essentially the configuration of who is allowed to issue use-conditions and what Certificate Authorities are trusted. This policy can also contain information describing where to find policies and also attributes. In this case JISC and the British Library were allowed to create policies and a list of certificates was allocated the right to sign these policies.

The template for this file was taken from the included example Authorisation model supplied with the Akenti installation. The final root policy file is shown in Appendix 4.

5.2.5 Creating Use Condition Policies

It was discovered that the logic of combining these policies did not allow for either the British Library’s or the JISC’s to be split into more convenient smaller multiple conditions files. Two monolithic use conditions files were constructed and signed to reflect the policies described in section 3. The current use condition files are shown in appendix 4.

5.2.6 Creating attribute certificates

Attribute certificates as used by Akenti are signed XML documents. These map the User’s authentication credentials to a role or an attribute. In this project the Attributes convenient for evaluating the conditions imposed by the JISC and the British Library are Attributes mapping an individual to:

1. a membership of an academic Institute (from the TAU list)
2. a membership of a CHEST organisation
3. a membership of an NHS authority

Example Attributes are shown in Appendix 6 and 7.

2 and 3 above are straight forward as there are only a small number of such entities. The number of Academic Institutes however tops six hundred. For ease of use for the user it was decided to run Akenti in pull mode (where Akenti is set up to retrieve attribute certificates rather than push mode where the user supplies the relevant attributes). In pull mode Akenti has no other information than the CA and the Distinguished name of the user. It must then check up to six hundred locations for an attribute before returning its authorisation answer. If these locations are online this could take some considerable time. (In fact when tried, the process failed after approximately 448 checks).

To solve this, a separate Akenti based authorisation service was created to allow a user to request an attribute certificate mapping their DN to membership of “a TAU
The ‘A2Z Project’: Akenti Access to zetoc

listed academic institute”, via a web site. This attribute is signed by an entity representing the JISC, automatically on the retrieval of a valid attribute mapping the user to membership of an academic institute. The root and use condition policies for this service can be found in Appendix 5.

5.2.7 Documentation

The main documentation available was on how to interact with the API. This project however decided to use the tools provided. There was little documentation at the time on how to use these tools. At the time of this installation there was very little in the way of installation instructions.
6 Observations

6.1 Manchester Computing

The project was able to successfully implement an access policy that reflected the requirements of the stakeholders and functioned as intended.
The software was implemented and configured as intended. However, a number of workarounds and compromises had to be included.

The support for distributed attribute certificates and use conditions were appealing.
Only the root policy itself was tied to the system.

At the time of evaluation, the Akenti software (version 1.2) was at a maturity level suitable for a development project, but not a production service.
(The same could be said of the GLOBUS toolkit). As noted above, there were a number of build errors, which were circumvented, but only by commenting out commands from the source code. There were also some incompatibilities that came to light. It is acknowledged that a subsequent release (version 1.3) was made available in late April 2003, which included a number of fixes, but was not evaluated.

It is unlikely that implementation (using v1.2) could be accomplished without the involvement of the Akenti development team.
The planned visit by Senior Akenti Developer, Abdou Essiari, was very productive. He provided specific advice and resolved a number of implementation issues.

The integration work required was very limited and straight-forward.
The software was implemented with only minor changes to the application. This contrasts favourably with an authorisation system that required API function calls, for example.

Checking access using user assertions failed.
It was not possible to model a user asserting their institutional affiliation, i.e. rather than checking all possible affiliations. The 'check access' command with user assertion (-b option) failed with a segmentation error.

Limited modelling within use conditions was possible.
It proved impossible to implement the full logical model as a constraint in one use condition and an additional Akenti server was required.

A limit on the number of attribute checks was hit.
In order to check for the relevant affiliation, identifying the signed attribute, a long list of potential locations had to be checked. The size of the check list (over 600) appeared to 'break' the system and the Akenti server was reconfigured to check on subsets of the eligible institutions separately.

Akenti certificates contain both XML and non-XML data.
In the version evaluated, the certificates contained both XML and PEM-encoded data. It is understood that this is being rationalised and only XML data will be present in some future release.
The ‘A2Z Project’: Akenti Access to zetoc

The use of eScience Certificates introduced additional complexity.
The eScience certificate contains location information relating not to the individual user, but to the Registration Authority. This prevented location data being used to limit the checking performed by Akenti. This is a shortcoming of the eScience implementation and nothing to do with Akenti.

6.2 Response from LBNL

The report was discussed with Mary Thompson and Abdelilah Essiari at LBNL on 25th November and the following email response received from Abdelilah Essiari on 26th November 2003:

“Thank you for the feedback. We have already corrected some of the problems you have encountered.”

“We are now linking all the tools to dynamic libraries. We will in the near future have a C++ tree and a Java tree. This should make the disk space requirements more reasonable.”

“Also we have moved to the newest XERCES library.“
“I have to say here that apache made a huge design change from the previous version. No wonder they buried the old version. The old design actually was using C++ techniques to manage memory. Users did not need to worry about deleting memory. We are doing the same in the Akenti code. But from some reason they moved to C style way of managing memory and they did not even bother to explain why. In any case, the switch was done over the summer and of course we had to make sure that we were freeing memory at the right time and at the right place.”

“We have also made some fixes to the Java GUI in response to the feedback from the PERMIS people. The other issues will also be tackled as for the most part they do not involve much work.”

“Now on the more serious issue of the Akenti model not allowing UseCondIssuersGroups to make sure that at least one of their Use Conditions must be satisfied, I can see two solutions. One is we add this to Akenti. But for the time being, this could easily be handled outside of Akenti by viewing the resource as two resources. One will be handled by the BL, the other by JISC. The enforcer will then simply make two calls to the Akenti Engine and make sure that both parties are happy.”

“We have also started to look at things differently when dealing with applications. We now try to determine the needs of an application and then we develop a GUI to generate Akenti Certificates. This GUI though is different from our present GUI in that it hides the fact that Akenti is being used.”

“We can talk more about this at some point. But we have successfully done this for a peer-to-peer application being developed by Karlot Berket here at LBL. And we have another application coming. Yours could be the third. But the main idea is that you
could switch to a different authorization system without having to change the GUI. This work will obviously be done on your side, but we will help in design.”

“To conclude it was nice working with you and I must say that I am quite impressed with the progress you made with Akenti.”
The ‘A2Z Project’: Akenti Access to zetoc

7 References


[JISC] http://www.jisc.ac.uk


[zetoc] http://zetoc.mimas.ac.uk

[MIMAS] http://www.mimas.ac.uk

[myGrid] http://mygrid.man.ac.uk/

[eScience] http://www.grid-support.ac.uk/ca/

[z39.50] http://www.loc.gov/z3950/agency/

[Athens] http://www.athens.ac.uk

[modssl] www.modssl.org

[TAU] http://www.jisc.ac.uk/index.cfm?name=collections_banding_information

[CHEST] http://www.chest.ac.uk

[Chadwick] http://www.jisc.ac.uk/uploaded_documents/AkentiPERMISDeskComparison2-1.doc
The ‘A2Z Project’: Akenti Access to zetoc

Appendices

Appendix 1 Successful Access Messages

1) Successful certificate check:

“Checking for existing JISC H/FE certificate

You already have a valid JISC certificate please go straight to the zetoc A2Z interface [https://a2z.mimas.ac.uk/].

2) Subsequent Screen <https://a2z.mimas.ac.uk/>

“A2Z

This is the secure a2z server.

Start a zetoc session.
Appendix 2 Unsuccessful Access Attempt

1) Unsuccessful (2-stage) certificate check:

“Checking for existing JISC H/FE certificate

I can't find a JISC Certificate for you Therefore I will attempt to find a H/FE Attribute Certificate. If successful I will generate a JISC H/FE Attribute certificate, store it here and show it below.

Checking for HE Attribute Cert

... Checking for Attribute certificates from our list of institutions. This could take some time if I had a large list ...

Can't find any Attribute certificate in order to issue you with a JISC H/FE certificate. Please contact your institute's rep for an institute attribute certificate.”

2) Authorisation failure when attempting access directly from [https://a2z.mimas.ac.uk/](https://a2z.mimas.ac.uk/)

“zetoc - Authorisation failure

Unfortunately you are not authorised to access the zetoc database. Only users from the UK academic community are allowed free access to this database.”
The ‘A2Z Project’: Akenti Access to zetoc

Appendix 3 Apache-created Environment Variables

```
DOCUMENT_ROOT="/home/unixusername/apache/secure/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTPS="on"
HTTPS_CIPHER="RC4-MD5"
HTTPS_EXPORT="false"
HTTPS_KEYSIZE="128"
HTTPS_SECRETKEYSIZE="128"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint,
application/msexcel, application/x-shockwave-flash, */*
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-gb"
HTTP_CONNECTION="Keep-Alive"
HTTP_HOST="a2z.mimas.ac.uk"
HTTP_USER_AGENT="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
.NET CLR 1.0.3705)"
PATH="/usr/ucb:/usr/bin:/bin"
QUERY_STRING=""
REMOTE_ADDR="130.88.201.24"
REMOTE_HOST="rmac.mcc.ac.uk"
REMOTE_PORT="1361"
REQUEST_METHOD="GET"
REQUEST_URI="/cgi-bin/printenv"
SCRIPT_FILENAME="/home/unixusername/apache/cgi-bin/printenv"
SCRIPT_NAME="/cgi-bin/printenv"
SERVER_ADDR="130.88.203.233"
SERVER_ADMIN="unixusername@irwell.mimas.ac.uk"
SERVER_NAME="a2z.mimas.ac.uk"
SERVER_PORT="443"
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE="<ADDRESS>Apache/1.3.27 Server at a2z.mimas.ac.uk
Port 443</ADDRESS>
"
SSL_CIPHER="RC4-MD5"
SSL_CIPHER_ALGKEYSIZE="128"
SSL_CIPHER_EXPORT="false"
SSL_CIPHER_USEKEYSIZE="128"
SSL_CLIENT_A_KEY="rsaEncryption"
SSL_CLIENT_A_SIG="md5WithRSAEncryption"
SSL_CLIENT_C="UK"
SSL_CLIENT_CERT="-----BEGIN CERTIFICATE-----
MIIFJzCCBA+gAwIBAgICApAwDQYJKoZIhvcNAQEEBQAwDgYDVR0PBEIwIwIB
7OJcJUG/CGwGCSqGSIb3DQEBCwUAAwIBAQBUDg19iJG62vRzZVQYlSsJZ5tnC
mXzNvQ28+KZafE0U4fXzAkNAKgCQF1XfBzSdA5w3LQeXzKnWiU/gCQFvXfBzSd
-------------
END CERTIFICATE-----
"n
SSL_CLIENT_CERT_END="Jun 18 10:22:03 2004 GMT"
SSL_CLIENT_CERT_SERIAL="0790"
SSL_CLIENT_CERT_START="Jun 19 10:22:03 2003 GMT"
SSL_CLIENT_CN="ross macintyre"
SSL_CLIENT_CN="CA"
```

Page 22 of 37
The ‘A2Z Project’: Akenti Access to zetoc

SSL_CLIENT_IDN="/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk"
SSL_CLIENT_IEMAIL="ca-operator@grid-support.ac.uk"
SSL_CLIENT_IO="eScience"
SSL_CLIENT_IOU="Authority"
SSL_CLIENT_I_DN="/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk"
SSL_CLIENT_I_DN_C="CA"
SSL_CLIENT_I_DN_email="/cA-operator@grid-support.ac.uk"
SSL_CLIENT_I_DN_O="eScience"
SSL_CLIENT_I_DN_OU="Authority"
SSL_CLIENT_KEY_ALGORITHM="Not supported by mod_ssl"
SSL_CLIENT_KEY_EXP="Not supported by mod_ssl"
SSL_CLIENT_KEY_SIZE="Not supported by mod_ssl"
SSL_CLIENT_L="MC"
SSL_CLIENT_M_SERIAL="0290"
SSL_CLIENT_M_VERSION="3"
SSL_CLIENT_O="eScience"
SSL_CLIENT_OU="Manchester"
SSL_CLIENT_SIGNATURE_ALGORITHM="md5WithRSAEncryption"
SSL_CLIENT_S_DN="/C=UK/O=eScience/OU=Manchester/L=MC/CN=ross macintyre"
SSL_CLIENT_S_DN_C="UK"
SSL_CLIENT_S_DN_CN="ross macintyre"
SSL_CLIENT_S_DN_L="MC"
SSL_CLIENT_S_DN_O="eScience"
SSL_CLIENT_S_DN_OU="Manchester"
SSL_CLIENT_VERIFY="SUCCESS"
SSL_CLIENT_V_END="Jun 18 10:22:03 2004 GMT"
SSL_CLIENT_V_START="Jun 19 10:22:03 2003 GMT"
SSL_EXPORT="false"
SSL_KEYSIZE="128"
SSL_PROTOCOL="SSLv3"
SSL_PROTOCOL_VERSION="SSLv3"
SSL_SECRETKEYSIZE="128"
SSL_SERVER_A_KEY="rsaEncryption"
SSL_SERVER_A_SIG="md5WithRSAEncryption"
SSL_SERVER_C="UK"
SSL_SERVER_CERT="-----BEGIN CERTIFICATE-----
MIIFUDCCBDigAwIBAgICAMwwDQYJKoZIhvcNAQEEBQAwcDELMAkGA1UEBhMCVUsxETAPBgNVBAoTCGVTY2llbmNlMRIwEAYDVQQLEwlBdXRob3JpdHkxCzAJBgNVBAMT
..." 
Pq6kCFCc8C4m4vpaNaQvExbJV7CzwkJ/5rmpfoCDG+7r6rEP7sPc7X/nfzhj25b70/m58

SSL_SERVER_CERTFILE="Not supported by mod_ssl"
SSL_SERVER_CERTIFICATE="-----BEGIN CERTIFICATE-----
MIIFUDCCBDigAwIBAgICAMwwDQYJKoZIhvcNAQEEBQAwcDELMAkGA1UEBhMCVUsxETAPBgNVBAoTCGVTY2llbmNlMRIwEAYDVQQLEwlBdXRob3JpdHkxCzAJBgNVBAMT
..." 
Pq6kCFCc8C4m4vpaNaQvExbJV7CzwkJ/5rmpfoCDG+7r6rEP7sPc7X/nfzhj25b70/m58

SSL_SERVER_CERTIFICATELOGDIR="Not supported by mod_ssl"
SSL_SERVER_CERT_END="Dec 10 13:30:08 2003 GMT"
SSL_SERVER_CERT_SERIAL="CC"
SSL_SERVER_CERT_START="Dec 10 13:30:08 2002 GMT"
SSL_SERVER_CN="/C=UK/O=eScience/OU=Manchester/L=MC/CN=a2z.mimas.ac.uk/Email=mike.jones@man.ac.uk"
SSL_SERVER_EMAIL="mike.jones@man.ac.uk"
SSL_SERVER_IC="UK"
SSL_SERVER_ICN="CA"
The ‘A2Z Project’: Akenti Access to zetoc

SSL_SERVER_IDN="/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk"
SSL_SERVER_IEMAIL="ca-operator@grid-support.ac.uk"
SSL_SERVER_IO="eScience"
SSL_SERVER_IOU="Authority"
SSL_SERVER_I_DN="/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk"
SSL_SERVER_I_DN_C="CA"
SSL_SERVER_I_DN_CN="a2z.mimas.ac.uk"
SSL_SERVER_I_DN_O="eScience"
SSL_SERVER_I_DN_OU="Manchester"
SSL_SERVER_SESSIONDIR="Not supported by mod_ssl"
SSL_SERVER_KEYFILE="Not supported by mod_ssl"
SSL_SERVER_KEYFILETYPE="Not supported by mod_ssl"
SSL_SERVER_KEY_ALGORITHM="Not supported by mod_ssl"
SSL_SERVER_KEY_EXP="Not supported by mod_ssl"
SSL_SERVER_KEY_SIZE="Not supported by mod_ssl"
SSL_SERVER_L="MC"
SSL_SERVER_M_SERIAL="CC"
SSL_SERVER_M_VERSION="3"
SSL_SERVER_O="eScience"
SSL_SERVER_OU="Manchester"
SSL_SERVER_SIGNATURE_ALGORITHM="md5WithRSAEncryption"
SSL_SERVER_S_DN="/C=UK/O=eScience/OU=Manchester/L=MC/CN=a2z.mimas.ac.uk/Email=mike.jones@man.ac.uk"
SSL_SERVER_S_DN_C="UK"
SSL_SERVER_S_DN_CN="a2z.mimas.ac.uk"
SSL_SERVER_S_DN_Email="mike.jones@man.ac.uk"
SSL_SERVER_S_DN_L="MC"
SSL_SERVER_S_DN_O="eScience"
SSL_SERVER_S_DN_OU="Manchester"
SSL_SERVER_V_END="Dec 10 13:30:08 2003 GMT"
SSL_SERVER_V_START="Dec 10 13:30:08 2002 GMT"
SSL_SESSION_ID="ED5A1176121443892C65344B16DFE15D2013983DF7A7F9717729A9D2A8780796"
SSL_SSL_VERSION="OpenSSL/0.9.6e"
SSL_STRONG_CRYPTO="Not supported by mod_ssl"
SSL_VERSION_INTERFACE="mod_ssl/2.8.12"
SSL_VERSION_LIBRARY="OpenSSL/0.9.6e"
UNIQUE_ID="P6D6RoJYy4IAAEbyPlI"
downgrade_1_0="1"
force_response_1_0="1"
nokeepalive="1"
ssl_unclean_shutdown="1"
Appendix 4 Configuration Files for the A2Z Web Site

The configuration file for Library data (which is read first by the Akenti engine: $HOME/A2Z/akentiConfLibrary_Data

# Akenti server may be providing access
# control to several independent resources.
# So for each top level resource we must
# specify a base which must be an absolute path.
RootResourceName library_data /home/unixusername/A2Z
# The name of policy files.
# PolicyFileName .htauthority
# # SignCerts [on, off] Signing capability and cached certs.
SignCerts off
#

BEGIN CACHE CONFIG
#
#
# Caching Parameters:
#
# Caching [on, off]
# CacheType [server, file]
#
# If we are using a server to cache the certs
# CacheHost hostname
# CachePort port
#
# If we are caching directly in the file system
# CacheBase a directory pathname
# CacheDIRName the name of the caching directory
#
# Caching off
CacheType file
#
# Server CacheMechanism
CacheHost
CachePort
#
# File Cache Mechanism
CacheDir /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../../resourceTree/cache
#
# END CACHE CONFIG
#
#############################################################
#
BEGIN AUTH SERVER INFO

# SSLMode [on, off] Use SSL
# AkentiPort default secure port 8443
# default unsecure port 8444
# ServerCertFile server's certificate pathname
# ServerKeyFile server's private key pathname
# CertificateAuthorityPath dirpath to trusted CAS
# CertificateAuthorityFile file containing trusted CA
#
The ‘A2Z Project’: Akenti Access to zetoc

# SSLMode        off
ServerCertFile /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../../resourceTree/idCerts/serverCert
ServerKeyFile /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../../resourceTree/idCerts/serverKey
CertificateAuthorityPath
CertificateAuthorityFile /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../../resourceTree/idCerts/caICert
# # END AUTH SERVER INFO
#

BEGIN LOGGING CONFIG
# Type of logging desired
# Logging  [off, file, server, stdout, stderr]
# Setting the logging level
#   LogLevel [1, 2, 3, 4, 5]
#   Only logs with a level <= LogLevel will be logged
# Logging to a file:
#   TempLogDir  temporary storage
#   MonitorLogFile permanent storage
# Logging to a server
#   MonitorServer   server's hostname
#   MonitorPort     server's port
# Logging file
LogLevel 5
# File Logging Mechanism
TempLogDir /tmp
MonitorLogFile /home/unixusername/A2Z/logs
# Server Logging Mechanism
MonitorServer
MonitorPort
# # END LOGGING CONFIG
#

$HOME/unixusername/A2Z/library_data/.htauthority:

<AkentiCertificate>
  <SignablePart>
    <Header Type="Policy" Version="2" CanonAlg="Ak1CanAlg"
SignatureDigestAlg="RSA-MD5">
      <UID>irwell#38432341#Wed May 14 03:23:24 2003</UID>
      <Issuer>
        <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    </Issuer>

Page 26 of 37
The ‘A2Z Project’: Akenti Access to zetoc

<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CADN>
</Issuer>
<ValidityPeriod End="040513032324Z"
Begin="030514032324Z"/>
</Header>
</PolicyCert>
<ResourceName>library_data</ResourceName>
</CAInfo>
<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CADN>

<X509Certificate>MIIE5TCCA82gAwIBAgIBADANBgkqhkiG9w0BAQQFADBwMQs
520AKzbkqZ81s9mQfEedrdqZplGStiQQ9x1yNodglvNa3u6LU28uBUzNHk6gKTOzOMRMl31ZMlad3c</X509Certificate>
</IdDirs>
</CAInfo>
</UseCondIssuerGroup>
<Principal>
<UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michaeljones</UserDN>
</Principal>
</UseCondIssuerGroup>
<AttrDirs>
<URL>file:/home/unixusername/A2Z/JISC/HE</URL>
<URL>file:/home/unixusername/A2Z/JISC/FE</URL>
<URL>file:/home/unixusername/A2Z/JISC/RC</URL>
</AttrDirs>
<CacheTime>3600</CacheTime>
</PolicyCert>
The ‘A2Z Project’: Akenti Access to zetoc

</SignablePart>

<Signature>TTbt0McdnuyLsPtaAXL71kKKzCjA4x15obPSxPSog65+9v+8S1T0Dj
AkS5x/E/BQv
c5RPmgzXl/vmLykj9Czk7BzHuHzQ0FCVqEg2ydb1UN/jvC0ewVG9iUFaRmGivj6/
qEOr6Vnhw2ZGFP42KUWN9v9DEBtx5nr/6TrCh/CsaVQ=/</Signature>

-----BEGIN AKENTI POLICY CERTIFICATE-----

-----END AKENTI POLICY CERTIFICATE-----

$HOME/A2Z/JISC/UseCond.test.xml.38432341

<AkentiCertificate>
  <SignablePart>
    <Header Type="UseCondition" Version="2"
      CanonAlg="Ak1CanAlg" SignatureDigestAlg="RSA-MD5">
      <UID>irwell#38432341#Wed Jul 30 15:51:07 2003</UID>
      <Issuer>
        <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael
          jones</UserDN>
        <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-
          operator@grid-support.ac.uk</CADN>
      </Issuer>
      <ValidityPeriod End="040729155107Z"
        Begin="030730155107Z"/>
    </Header>
    <UseConditionCert scope="sub-tree" critical="true">
      <ResourceName>library_data</ResourceName>
      <Condition>
        <Constraint>( Location = ReadingROOM ) || ( JISC =
          HE ) || ( JISC = FE ) || ( JISC = RC ) &&& ( LicenceRC =
          PAID ) ) || ( Chest = yes ) || ( NHS = England ) &&& ( Licenc
          en = Scot) &&& ( LicenceSNHS = PAID ) ) || ( NHS = Wales ) &&& ( L
          icenceWNHS = PAID ) ) || ( NHS = N Ireland ) &&& ( LicenceNINHS =
          PAID ) )</Constraint>
        <AttributeInfo type="SYSTEM">
          <AttrName>Location</AttrName>
          <AttrValue>ReadingROOM</AttrValue>
        </AttributeInfo>
        <AttributeInfo type="AKENTI">
          <AttrName>JISC</AttrName>
          <AttrValue>HE</AttrValue>
        </AttributeInfo>
        <Principal>
          <UserDN>/C=UK/O=es-
            grid/OU=mvc.mcc.ac.uk/CN=Michael AS Jones</UserDN>
        </Principal>
      </Condition>
    </UseConditionCert>
  </SignablePart>
</AkentiCertificate>
The ‘A2Z Project’: Akenti Access to zetoc

</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>JISC</AttrName>
  <AttrValue>FE</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=es-grid/OU=mvc.mcc.ac.uk/CN=Michael AS Jones</UserDN>
    <CADN>/C=UK/O=es-grid/CA</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/JISC/FE</URL>
  </AttrDirs>
</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>JISC</AttrName>
  <AttrValue>RC</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=es-grid/OU=mvc.mcc.ac.uk/CN=Michael AS Jones</UserDN>
    <CADN>/C=UK/O=es-grid</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/JISC/RC</URL>
  </AttrDirs>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>LicenceRC</AttrName>
  <AttrValue>PAID</AttrValue>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>Chest</AttrName>
  <AttrValue>yes</AttrValue>
</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>NHS</AttrName>
  <AttrValue>England</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    <CADN>/C=UK/O=eScience/OU=Authority/CA/emailAddress=ca-operator@grid-support.ac.uk</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/NHS</URL>
  </AttrDirs>
</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>NHS</AttrName>
  <AttrValue>Scotland</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    <CADN>/C=UK/O=eScience/OU=Authority/CA/emailAddress=ca-operator@grid-support.ac.uk</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/NHS</URL>
  </AttrDirs>
</AttributeInfo>
The ‘A2Z Project’: Akenti Access to zetoc

<AttrDirs>
  <URL>file:/home/unixusername/A2Z/NHS</URL>
</AttrDirs>
</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>NHS</AttrName>
  <AttrValue>Wales</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-operator@grid-support.ac.uk</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/NHS</URL>
  </AttrDirs>
</AttributeInfo>
<AttributeInfo type="AKENTI">
  <AttrName>NHS</AttrName>
  <AttrValue>N Ireland</AttrValue>
  <Principal>
    <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-operator@grid-support.ac.uk</CADN>
  </Principal>
  <AttrDirs>
    <URL>file:/home/unixusername/A2Z/NHS</URL>
  </AttrDirs>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>LicenceENHS</AttrName>
  <AttrValue>PAID</AttrValue>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>LicenceSNHS</AttrName>
  <AttrValue>PAID</AttrValue>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>LicenceWNHS</AttrName>
  <AttrValue>PAID</AttrValue>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
  <AttrName>LicenceNINHS</AttrName>
  <AttrValue>PAID</AttrValue>
</AttributeInfo>
</Condition>
<Rights>read</Rights>
</UseConditionCert>
</SignablePart>

<Signature>gajUVU4ivJ4vwdI+bNm/SBWrS+T5IMrHovhYxNS14vuXucIw75M6h+pJMs/chdt
hV4K6/axAg2NDAq89T5enBCQt5g5BoI0MP2ZSk9oEdV+r/XKYu5Xb+ag3K62fX9g
AQlUg9m5apM+2ganler+klvt7F3b0ldq4csKrcDXAAc=</Signature>
</AkentiCertificate>
The ‘A2Z Project’: Akenti Access to zetoc

-----BEGIN AKENTI USECONDITION CERTIFICATE-----
VXNlQ29uZGl0aW9uIFYyIGlyd2VsbCMzODQzMjM0MSNXZWRcIEp1bFwgMzBcIDE1
OjUxOjA3XCAyMDAzIC9DPVVLL089ZVNjaWVuY2UvTlU9TWFuY2hlc3Rlc3MPU1D
89T5enECQG5g5BoI0MPZSk9oEdV+r/XKYu5Xb+ag3K62fX9gAQIUgWm5apM+2gan
ler+klvt7F3b0ldq4csKroDXAAc=
-----END AKENTI USECONDITION CERTIFICATE-----

$HOME/A2Z/BL/UseCond.test.xml.38432341

<AkentiCertificate>
  <SignablePart>
    <Header Type="UseCondition" Version="2"
      CanonAlg="Ak1CanAlg" SignatureDigestAlg="RSA-MD5">
      <UID>irwell#38432341#Fri Aug 01 18:59:44 2003</UID>
      <Issuer>
        <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael
        jones</UserDN>
        <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-
        operator@grid-support.ac.uk</CADN>
      </Issuer>
      <ValidityPeriod End="040731185944Z"
        Begin="030801185944Z"/>
    </Header>
    <UseConditionCert scope="sub-tree" critical="true">
      <ResourceName>library_data</ResourceName>
      <Condition>
        <Constraint>( Location = ReadingROOM ) || ( IP =
        ac.uk ) || ( ( NHS = England ) && ( LicenceSNHS = PAID )
        ) || ( ( NHS = Scotland ) && ( LicenceSNHS = PAID )
        )</Constraint>
        <AttributeInfo type="SYSTEM">
          <AttrName>Location</AttrName>
          <AttrValue>ReadingROOM</AttrValue>
        </AttributeInfo>
        <AttributeInfo type="SYSTEM">
          <AttrName>IP</AttrName>
          <AttrValue>ac.uk</AttrValue>
        </AttributeInfo>
        <AttributeInfo type="AKENTI">
          <AttrName>NHS</AttrName>
          <AttrValue>England</AttrValue>
          <Principal>
            <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael
            jones</UserDN>
            <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-
            operator@grid-support.ac.uk</CADN>
          </Principal>
          <URL>file:/home/unixusername/A2Z/NHS</URL>
        </AttributeInfo>
        <AttributeInfo type="AKENTI">
          <AttrName>NHS</AttrName>
          <AttrValue>Scotland</AttrValue>
          <Principal>
          </Principal>
        </AttributeInfo>
      </Condition>
    </UseConditionCert>
  </SignablePart>
</AkentiCertificate>
The ‘A2Z Project’: Akenti Access to zetoc

<UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>

<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-operator@grid-support.ac.uk</CADN>

</Principal>
<AttrDirs>
<URL>file:/home/unixusername/A2Z/NHS</URL>
</AttrDirs>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
<AttrName>LicenceENHS</AttrName>
<AttrValue>PAID</AttrValue>
</AttributeInfo>
<AttributeInfo type="SYSTEM">
<AttrName>LicenceSNHS</AttrName>
<AttrValue>PAID</AttrValue>
</AttributeInfo>
</Condition>
</Rights>
</UseConditionCert>
</SignablePart>

<Signature>pighB45Hb4r5w9DnP0gLHPa208c1XYFAgZqE/X5VFTiFrLZLToop2zGLrzV/1
DgdsusPR7UTpuYGVDvX/RGJXQx3eYyfYXbxVgLw81zALAO+D02q69CQj0NdmQ
0YHvsagNvaShiKtH80CEEpFqadGbPE2f5JqXSlqVgs==</Signature>
</AkentiCertificate>

-----BEGIN AKENTI USECONDITION CERTIFICATE-----
VXNlQ29uZGl0aWwuAFtyIGlyd2VsbCMzODQzMjM0MNSNGcm1cIEF1Z1wgMDpcIDE4
OjUSOj0XCAyMDAzIC9DPVVLL089ZVNjaYWVuY2UvTl9TWFuY2hlc3Rci9MPU1D
VgLw81zALAO+D02q69CQj0NdmQ0YHvsagNvaShiKtH80CEEpFqadGbPE2f5Jq
XS1qVgs=
-----END AKENTI USECONDITION CERTIFICATE-----
The ‘A2Z Project’: Akenti Access to zetoc

Appendix 5 Configuration Files for the JISC TAU Academic Attribute Certificate Generator

SHOME/A2Z/JISC/akentiConfJISC:

# Akenti server may be providing access
# control to several independent resources.
# So for each top level resource we must
# specify a base which must be an absolute path.
RootResourceName HE /home/unixusername/A2Z/JISC
# The name of policy files.
# PolicyFileName .htauthority
# # SignCerts [on, off] Signing capability and cached certs.
SignCerts off
#
#BEGIN CACHE CONFIG
#
# Caching Parameters:
# #
# Caching [on, off]
# CacheType [server, file]
#
# If we are using a server to cache the certs
# CacheHost hostname
# CachePort port
#
# If we are caching directly in the file system
# CacheBase a directory pathname
# CacheDIRName the name of the caching directory
#
Caching off
CacheType file

# Server CacheMechanism
CacheHost
CachePort

# File Cache Mechanism
CacheDir /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../../resourceTree/cache
#
# END CACHE CONFIG
#
#BEGIN AUTH SERVER INFO
#
# SSLMode [on, off] Use SSL
# AkentiPort default secure port 8443
# default unsecure port 8444
# ServerCertFile server's certificate pathname
# ServerKeyFile server's private key pathname
# CertificateAuthorityPath dirpath to trusted CAS
# CertificateAuthorityFile file containing trusted CA
The ‘A2Z Project’: Akenti Access to zetoc

# # # SSLMode off
ServerCertFile /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../resourceTree/idCerts/serverCert
ServerKeyFile /home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../resourceTree/idCerts/serverKey
CertificateAuthorityPath
CertificateAuthorityFile
/home/unixusername/akentiDist/build/sun-sol-gcc/testcase/libsrc/shared/../resourceTree/idCerts/caICert

# # END AUTH SERVER INFO
# # #
# # #

BEGIN LOGGING CONFIG
# Logging parameters:
# # Type of logging desired
# Logging [off, file, server, stdout, stderr]
# # Setting the logging level
# LogLevel [1, 2, 3, 4, 5]
# Only logs with a level <= LogLevel will be logged
# #
# Logging to a file:
# TempLogDir temporary storage
# MonitorLogFile permanent storage
# #
# Logging to a server
# MonitorServer server's hostname
# MonitorPort server's port
# #
# Logging file
LogLevel 5
# File Logging Mechanism
TempLogDir /tmp
MonitorLogFile /home/unixusername/A2Z/logs
# Server Logging Mechanism
MonitorServer
MonitorPort

END LOGGING CONFIG
# #
# #

$HOME/A2Z/JISC/HE/.htauthority

<AkentiCertificate>
  <SignablePart>
    <Header Type="Policy" Version="2" CanonAlg="Ak1CanAlg"
SignatureDigestAlg="RSA-MD5">
      <UID>irwell#761c78bc#Fri Aug 01 19:02:51 2003</UID>
    </Header>
  </SignablePart>
</AkentiCertificate>
The ‘A2Z Project’: Akenti Access to zetoc

<UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CADN>
</Issuer>
<ValidityPeriod End="040731190251Z" Begin="030801190251Z"/>
</Header>
<PolicyCert>
<ResourceName>HE</ResourceName>
<CAInfo>
<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/EmailAddress=ca-operator@grid-support.ac.uk</CADN>
<X509Certificate>MIIE5TCCA82gAwIBAgIBADANBgkqhkiG9w0BAQQFADBwMQswCQYDVQQGEwJVSzER
urlkEM7Q+kWb1bUtgoBaU0b7Pxtn3OmtO10sdU1pZPZzJy+HYcoi5esbfbOS7CoRU520AKzkbkZ81s9mQfEedrdgZplGSiQQ9xlYNogd1vN4a3u6LU28uBUzNHk6gKTOz0MRML3ZMlad3</X509Certificate>
<IdDirs>
<URL>file:/home/unixusername/A2Z/IdDir</URL>
</IdDirs>
</CAInfo>
<UseCondIssuerGroup>
<Principal>
<UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
<CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CADN>
</Principal>
<URL>file:/home/unixusername/A2Z/JISC/UseConditions</URL>
</UseCondIssuerGroup>
<AttrDirs>
<URL>file:/home/unixusername/A2Z/Manchester</URL>
<URL>file:/home/unixusername/A2Z/York</URL>
<URL>file:/home/unixusername/A2Z/Salford</URL>
</AttrDirs>
<CacheTime>3600</CacheTime>
</PolicyCert>
</SignablePart>

<Signature>b2VXag2PG/TcFUn8ngwkap/7Sh10MC19I2McfFrVe/RjL/r+kYscPH3Mz7aojvYSAuDLrVPRXrXvYNh9kVhVMNy0lroB/Mr/RviU23PPfd7c+fILrZ4WR4zHhXMPFIZM9IUvDx+Lmja+9pKQnt45TdsFQwRa9J9u+lbxta307V0==</Signature>

-----BEGIN AKENTI POLICY CERTIFICATE-----
UG9saWFsIFoSFy1GLy202vbsCM3njJfJNzhiYyNgcm9cIgF1Z1wMDFcIDE50jAyOjUXCAYMDAIC9DPVVLLO89ZVNjaWVuY2YvT1U9TFWuy2hlc3Rlcj9MPU1DL0NOPW1p
GxiGH2RN8Y3LSWuGh+avK9FwJThbc8993tz58gutnZHjMeFcwU0hlIwwhS8PH4ua
Nz72mA23jL0VJDfr0n276VvQ1rc7tXQ==
-----END AKENTI POLICY CERTIFICATE-----
The ‘A2Z Project’: Akenti Access to zetoc

Appendix 6 Example Institutional Attribute Certificate

/home/unixusername/A2Z/Manchester/rossman.xml.500121fa.0

```xml
<AkentiCertificate>
  <SignablePart>
    <Header Type="Attribute" Version="2" CanonAlg="Ak1CanAlg"
     SignatureDigestAlg="RSA-MDS">
      <UID>irwell#5e3a1cd1#Fri Aug 01 10:56:43 2003</UID>
    </Issuer>
    <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</UserDN>
    <CA DN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CA DN>
    <ValidityPeriod End="040731105643Z" Begin="030801105643Z" />
    <Issuer>
      <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=ross macintyre</UserDN>
      <CA DN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk</CA DN>
    </Issuer>
    <AttrName>University</AttrName>
    <AttrValue>The Victoria University of Manchester</AttrValue>
  </SignablePart>
  <Signature>tWJ5WJWke9IA4+7knIzHOIFeP/dbTUXri8d3yNGSNzg1056pWgE5V
  xayv1HftHt5 2qBBayKKC8p2i0q2fLxM28euOZQzgDcZzySKeHxHlpTShv3mCQbpXy9X3Fwkk+jC
  GXqRq3r+P HHg2kYwbLvjK7kFM72PCCa1/S1qtA=k</Signature>
</AkentiCertificate>

-----BEGIN AKENTI ATTRIBUTE CERTIFICATE-----
QR0cmIdXRlIFFFFyGlyd2VsWbCM1ZTNhMNKnMSNcmlcIEF1Z1wgMDFcIDEwOjU2
OjQzXCAyMDazI9DPVULL089ZVWjaWVuY2UvT1U9TWFuY2hcL3Rci9MFU1DLN0
PW1pY2hhZWxcILpvmXCI9DPVULL089ZVWjaWVuY2UvT1U9QXVoaG9yaXR5LNO
PUNBL0VYWlsPNWhL9wZXJhG9ydQyodaWtc3VwC9G9ydCShYy51ayAwIDAzMDgw
MTEvNU10LmQdMQwNz2xmTAMlJpZmBbzFDMX5BBgCgUtBNLUE1N5AvQ21V59P
PWUTY2l1bnN0LVU1bhnNoZXN0ZTVlTD1NQy9DcJyb3NzXCBtYWNpbnR5c2Nucg
LmNV5UsTzl1U2pN5jZ9PVTV1BdXRob3JpdHkvQ049O8WVW1haw9yY2EtbeB1
cmFob3JA3JpZ2c2XWb3J0IlmFJvFVuaXZlcmNpdHkgV1hXYWlpbnR5c2Ng
YWwgV5dpdMVyc210eVwgb2zcIEhbnNoZXN0ZTVlMCAxMjggtWJ5JWYke91A4+7k
nIzHOIFeP/dbTUXri8d3yNGSNzg1056pWgE5Vxayv1HftHt52qBBayKKC8p2i0q2
fiLxM28euOZQzgDcZzySKeHxHlpTShv3mCQbpXy9X3Fwkk+jCQxQ3r+PHHg2k
YwbLvjK7kFM72PCCa1/S1qtA=k
-----END AKENTI ATTRIBUTE CERTIFICATE-----
```
The ‘A2Z Project’: Akenti Access to zetoc

Appendix 7 Example JISC TAU Academic Attribute Certificate

$HOME/A2Z/JISC/HE/ross_macintyre.xml1.e7f3af3c.0:

```xml
<AkentiCertificate>
  <SignablePart>
    <Header Type="Attribute" Version="2" CanonAlg="Ak1CanAlg"
      SignatureDigestAlg="RSA-MD5">
      <UID>irwell#e7f3af3c#Wed Aug 27 11:28:20 2003</UID>
      <Issuer>
        <UserDN>/C=UK/O=es-grid/OU=mvc.mcc.ac.uk/CN=Michael
          AS Jones</UserDN>
        <CADN>/C=UK/O=es-grid/CN=UK e-Science CA</CADN>
      </Issuer>
      <ValidityPeriod End="040826112820Z"
        Begin="030827112820Z"/>
    </Header>
    <AttributeCert>
      <SubjectAndCA>
        <UserDN>/C=UK/O=eScience/OU=Manchester/L=MC/CN=ross
          macintyre</UserDN>
        <CADN>/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-
          operator@grid-support.ac.uk</CADN>
      </SubjectAndCA>
      <AttrName>JISC</AttrName>
      <AttrValue>HE</AttrValue>
    </AttributeCert>
  </SignablePart>
  <Signature>Vr/uzp4WQcMheshROsCml1TUvPv+cN76t1Boacej02E7Bھ4Hxen3F
    sfGpbrZ92q-
    jrwGRAydTXDteWdJS88QiyyaGE210f4JMrwRloP005b05yyI6fG29upKdTmL1FYVe
    DNtbomnxr28pl82zt+IMT6J/xHP66zG5w/HWEBMr5kg="</Signature>
</AkentiCertificate>
```

```
-----BEGIN AKENTI ATTRIBUTE CERTIFICATE-----
QXR0cmlidXRlIFIFgyIGlyd2VsbCQ1N2zYWYzYyQXZWRcIEF1Z1wgMjdcIDE0
OjIwXCayMDAzIC9PdVVuL089ZXMtZ3JpZC9!PtLQJlMIPFHNjLmNjLmNvL08pU1p
Y2hhZWNzc3EPtXCBKd251cyAvQz1sY9PWWZLWdyaWQvQ049VUtU2Np2Z5j
ZVwqQ0EgMCAwMzA4NjcxMTI4MjBAIDA0MDgyMjExMjgyMjExIGQvQWxQ2Fwu
QS1NjRDUgLOM9VUsVz11U2pZW5jZS9PV1I1NY5jaGVzdGVyLW09TUMvQ049cm9z
clwgbWFjaW50eXJlc3VwcG9ydC5hYy51ayBKSVNDL0VtYWlsPWNhLW9zJnJhG9yQ
QdyaWQtwc3VwcG9ydC5ayBKSNDIeHFDAgMTI4Fa/7s6WeFKHdIXrUT1RqVhUlLz7
/nDe+rZRGQoHo9NhTw+R8Xp9xHzxqW6
2fWavo68BkQmUlw7RMAYuVPEissmhhNtdH+CTMESKDztQWO9Csn10nXtbvjynU5i
9RWFXgzbW6J68dkaYtGBX/iDE+if8Rz+usxucPxlhATK+ZI
-----END AKENTI ATTRIBUTE CERTIFICATE-----
```