Akenti Access To Zetoc

A. Apps, W.T. Hewitt, M.A.S. Jones, R. MacIntyre, A. Sanders, A. Weeks The University of Manchester

Keywords: Akenti, Community Authorisation, Social Science, Distributed Administration

Abstract

With more services populating the UK's Grid with strict access control policies and users in multi-levelled organisations with multi-lateral collaborations, there is a real need for careful control of access to data and resources. A2Z is an ongoing JISC funded project to investigate the use of Akenti (development authorisation software from Laurence Berkeley Laboratory) to control access to British Library data in the form of an existing service Zetoc, run by MIMAS at the University of Manchester.

A2Z uses UK 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 r&#65533;le) 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 complex authorisation rules required to access the library's data via zetoc. 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 zetoc service

The zetoc service[1] comprises of two user interfaces, a search web page and an alert web page. The search page provides an interface to search through the British Library's Table of Contents Data. The resulting information can be formatted by the institute to which the user is a member. The Alert page is an individually configurable watchdog. It monitors new releases of journals and proceedings for user specified editions and/or keywords, and sends out a table of contents for each match.

Access to both services is currently controlled firstly by IP and if this fails by Athens which presents a username password challenge to the user. This is evaluated remotely. Three letters from the username identify the institute the user belongs to.

Akenti

Akenti[2] 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, resource’s use-conditions, user attributes, and delegated authorization. It makes decisions based on policies split among on-line and off-line entities.

A2Z

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.

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.

When the A2Z web server in figure 2 receives a request to access either of the zetoc services, 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'. 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 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 (below and right) 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.

Distributed Access Control

Authority to use zetoc is governed by two stakeholders:

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. The British Library owns the data.

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 or Affiliates with a Licence and any member of the NHS in the UK with a regional licence. JISC are the stakeholders for the machine and support.

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 stake holders 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.

myGrid Integration – the next step

myGrid[3] aims to provide a virtual laboratory workbench. Access to zetoc via A2Z through myGrid is the next phase of the project. We will create a web service for both zetocs, implementing zetoc Alert as an OGSA notification port type with a UDDI-M registry entry.

Summary

A2Z highlights how Akenti can be employed to describe and evaluate the complex authorisation rules required to access services such as zetoc with minimal impact to the end user.

References

[1] http://zetoc.mimas.ac.uk/
[2] http://www-itg.lbl.gov/Akenti/
[3] http://www.mygrid.info/