

JISC

# JISC Conference 2007





# OpenAthens and the future of access and identity management

JISC Conference 2007



## About Eduserv

- We are a registered charity
- Dedicated to realising the benefits of ICT for
  - learners
  - researchers
  - institutions that serve them
- In-depth understanding of education
- Driven by the needs of the community
- Governed by trustees (drawn predominately from UK HE)

## About Athens

- Initially deployed in 1996
- Established as the 'standard' for SSO to protect online resources in HE and the NHS
- 4 million users in 100 countries
- Access to resources from around 180 leading service providers
- Delivered over 99.999% availability since 1998
- Up to 10,000,000 authentications per month



## The big picture...

- How are we going to better manage online identities for users?
- How are AIM architectures going to evolve?
- What are the important standards and technologies?
- We need to consider scenarios of how we might get there
  - in the short term
  - in the long term

## The picture in HE/FE

- In the short-term, institutions need to consider their options for joining the Federation
- In the longer term
  - AIM technologies will continue to evolve
  - need to support multiple federations
  - supporting multiple technologies and federations over the long term will be costly
- Shared service solutions offer significant benefits - how can we help?
  - OpenAthens provides a cost effective and proven outsourced strategy for joining the Federation, and
  - for the long-term provision of AIM solutions



## Short term issues

- Options for joining the Federation described in the JISC roadmap
  - *become a full member of the UK Access Management Federation, using community-supported tools*
  - *become a full member of the UK Access Management Federation, using tools with paid-for support*
  - *subscribe to an 'outsourced Identity Provider' to work through the Federation on your behalf, such as continued use of Athens with the gateways*
- Note that institutions adopting the third option are still **full members** of the Federation
- And that even within the Federation you may have to broker bi-lateral agreements with content suppliers



## How can we help?

- OpenAthens is a cost-effective and proven mechanism for joining the Federation right now
- Allows you to outsource the technical and policy infrastructure needed to take part in the Federation



## Longer term issues

- User expectations are changing
- Growing demand for lifelong identities
- People will enter education (certainly HE) with an existing identity
  - in the same way that they enter with an existing email address currently
- They will not want to be forced to have an education-specific identity
- They will not want different identities as they move from school to college to university

## Longer term issues (2)

- Users will not want different identities if they are affiliated to multiple institutions
- They will not want to be forced to use different identities for accessing educational and non-educational services (e.g. Web 2.0 services)
- They will want identities that work well for
  - delivery/uptake of course modules at multiple institutions
  - research collaborations across multiple institutions
  - both potentially happening on an international basis

## Technology in flux

- We know that rate of technology change is accelerating
  - AIM technologies continue to evolve over time
  - Federations will come and go (particularly in international context)
  - Institutions will need to keep up with such changes or risk being left behind
- OpenID and MS CardSpace are good examples of how things are changing
  - indicative examples of where things are going
  - not necessarily **the** solution, but things that many institutions will probably have to think about

## OpenID – key features

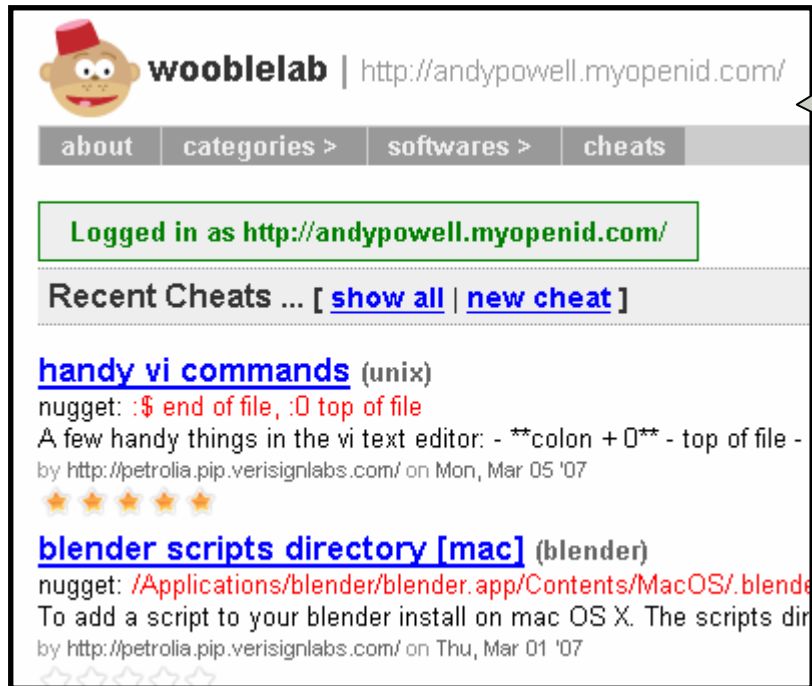
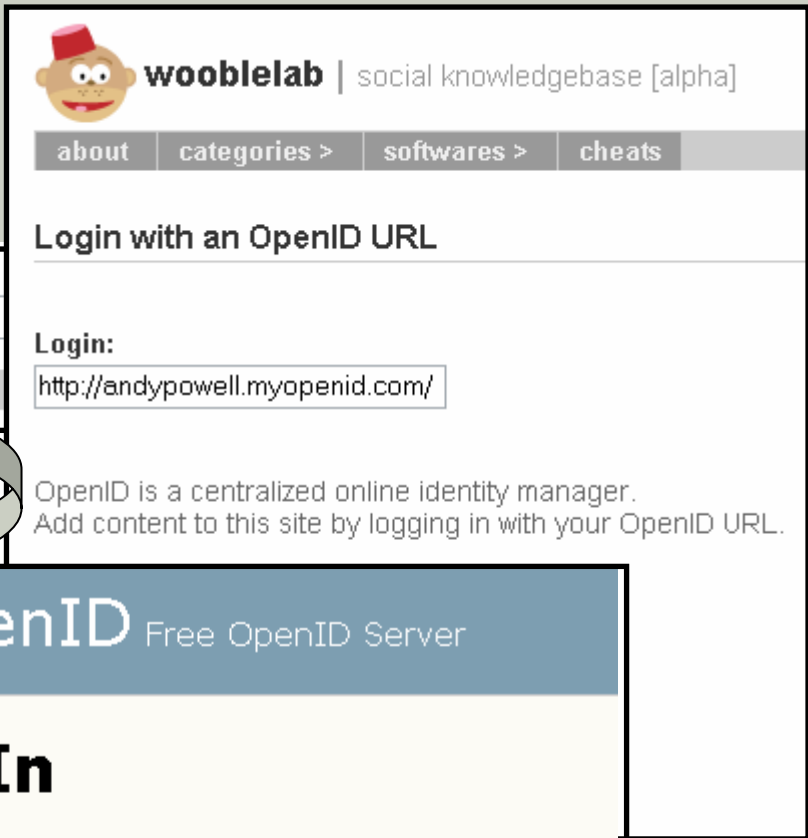
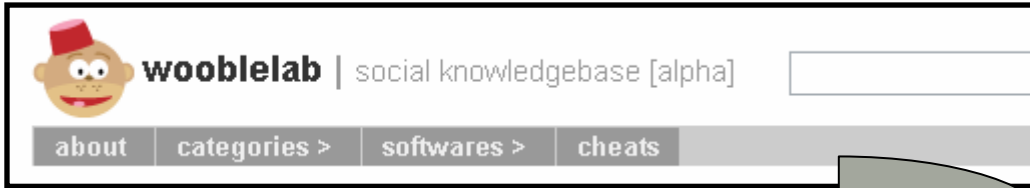
- Born out of a Web 2.0 need
- SSO to blogs, i.e. using a single identity to
  - write to your own blog
  - comment on others' blogs
- However, much wider applicability than that and now being adopted across wide range of 'Web 2.0' services
- Relatively lightweight in technical terms
- An authorisation and attribute exchange mechanism (but not trying to solve everything – trust, authorisation, etc.)



## OpenID – key features

- The identifier is a URI (typically a URL)
  - e.g. mine is <http://andypowell.myopenid.com/>
- This is convenient for a number of reasons, but especially because it removes the need for a WAYF service
  - the OpenID directly provides the location of the Identity Provider (IdP)
- Issues to be solved – e.g. around phishing (spoofing the IdP)
- Still a work in progress, see <http://openid.net/>
- However, widespread interest

# OpenID example



## Microsoft CardSpace

- A client-side Windows application for managing multiple user-centric identities...
  - and implementing the protocol transactions needed to inter-work with server-side (Web) applications
- Sits within high-level open framework known as the 'Identity Metasystem'
- Perceived as a more open replacement for MS's failed 'passport' initiative
- Builds on WS- stack – so not lightweight
- But joint commitment between MS and OpenID leading players to work together



## How can we help?

- the agenda doesn't stop when you join the Federation
- OpenAthens provides a future-proofed, cost-effective technical and policy infrastructure for
  - engaging with multiple federations and
  - dealing with new developments in technology



# The future of Access & Identity Management...



## To recap...

- Users already operating in an increasingly complex online world
  - Many service providers, multiple identities
- Increased move towards user-centric AIM
- Multiple standards which are still evolving
- High rate of technology change
- High costs of implementation, management & support



## Building for the future

- We need new ways of supporting high volumes of users, with diverse needs because
  - Users have multiple online persona and affiliations
  - Higher levels of B2C transactions
  - Organisations still need to be able to manage access control
- Integrated security environments are needed
  - To support trust across multiple federations
  - Addressing needs of IdPs, SPs and end users
  - Expose users rights but maintain privacy
  - Manage complex policy/decision making



## What is Eduserv doing?

- Developing new technology to meet the needs of a rapidly changing AIM environment
- Specifically, creating
  - UK federation ready software and services
  - New tools and services for users, organisations and service providers
  - New architecture to support AIM in a multi federation environment
- This drives Eduserv's AIM vision

# OpenAthens

- A new AIM framework
  - software tools/libraries, utilities, GUI's and services
- Underpinned by a new standards based open architecture
- Securely connecting users with resources

**Anyone to Anything from Anywhere**



## Design principles

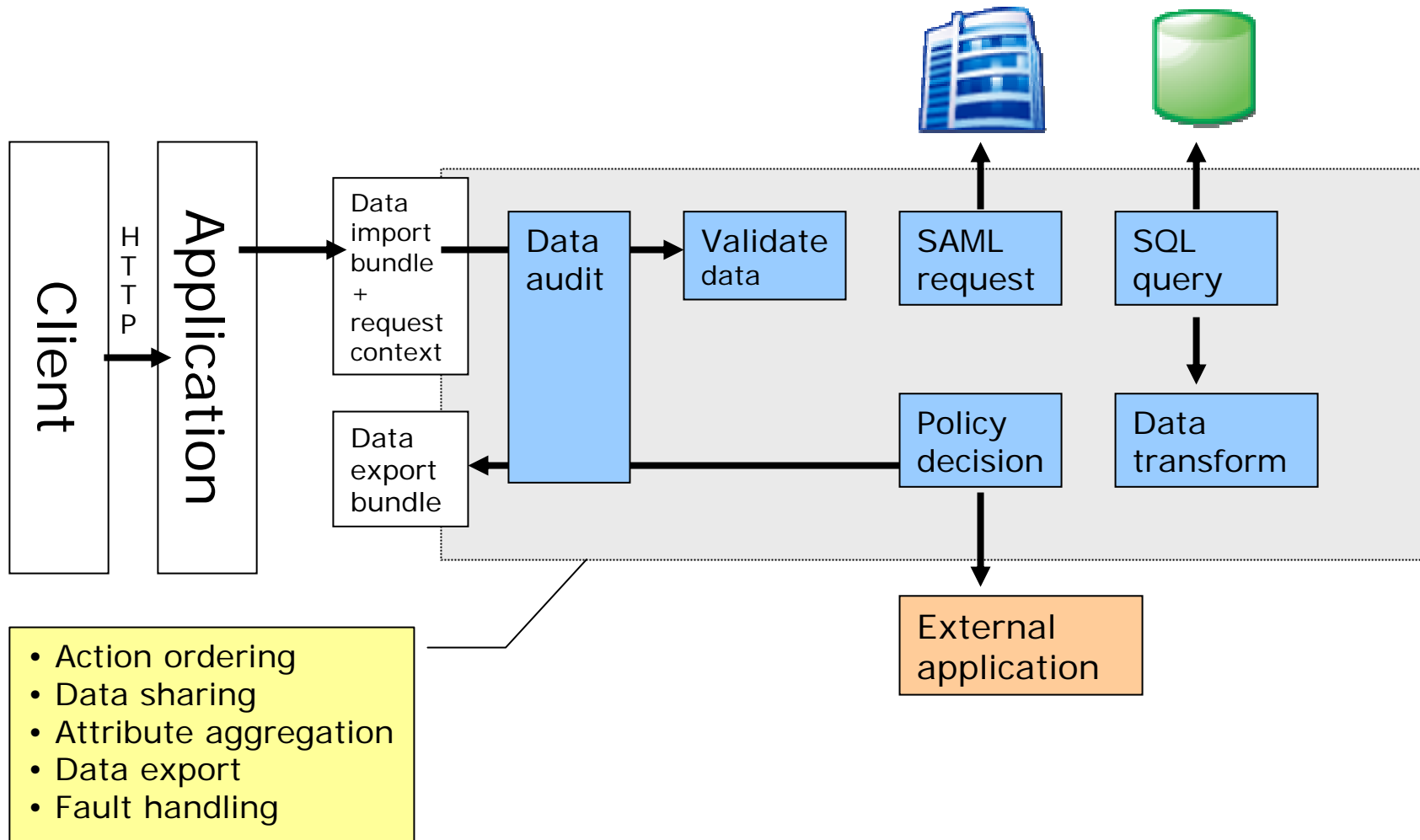
- Open architecture and extensible platform
- Support for multiple federations and federation methods
- Compliant with international standards/protocols
- Seamless migration for existing Athens users
- Future proof



## OpenAthens framework is

- Modular, portable, extensible architecture, embeddable
- Enabling process flows and data to be managed
- Delivering a range of AIM services
  - Outsourced IdP (connect to the UK Federation)
  - SSO, user provisioning/de-provisioning, administration, policy management
- Bridges, gateways, attribute transformations, API's

# OpenAthens workflow example





## Why this architecture?

- Keeps integration simple and static
  - Allows easy upgradeability
  - Can adapt to changing requirements
- Modules provide specialist functionality
  - Easier development model than 'monolithic' approach
- Allows re-use of 'information flow' between applications
- Embeddable & can bind to other languages
  - Multi-language modules
- Find out more about the technical stuff at
  - <http://labs.eduserv.org.uk/aim>



# OpenAthens – the User experience

- Multiple identities – joined up experience
- Users can have 1 or more linked user names
  - OpenID, Athens and others
  - Connect to resources in multiple federations
- Enhanced user experience
  - Multiple ID's map to single login thru account linking
  - Multi factor authentication
  - Manage personal attributes & attribute release policies to enhance privacy
- Single point of identity management – web GUI

## OpenAthens – the Institution view

- Comprehensive administration of users
  - Integrate with local resources
  - Integrate with local Directory services or,
  - Shared identity provider service
  - GUI's to manage users & monitor usage
- Facilitates resource sharing
  - Institutions can be both identity (IdP) and resource (SP) providers
- Flexible suite of software and GUI's that can be used by IT staff and libraries
- Integrated Security Environment
- Flexible, low cost and future proof



# OpenAthens – for Service Providers

- Service Providers (SP)
  - multiple federation methods are supported in a single platform
  - OpenAthensSP beta S/W available since Oct 2006
- Support for
  - Shibboleth 1.3 - UK Federation
  - SAML 2.0
  - OpenID 1.1
  - Microsoft InfoCard (TBA)
- Migration path from Athens technology



## What does OpenAthens do today

- Allows users to connect directly to the UK Federation
  - Quickest, easiest and lowest cost way
- Connects users to resources in Shibboleth, SAML and Athens federations
- Allows Service Providers to use latest technology for connecting to multiple federations
- Protects local resources
- Resource proxy gateway



## OpenAthens development roadmap

- Supporting multiple federation methods
  - SAML 2.0
  - Shibboleth
  - OpenID consumer (available by Summer 2007)
  - CardSpace, GeoIP, Others TBA
- During 2007
  - New end user tools & GUIs
    - Including customisable end-user portal
    - Lifelong identity management
  - Role based authorisation
  - Security enhancements
- In 2008
  - Identity provider tools using the latest architecture

Attribute release management



## What about Athens?

- All Athens subscribers will migrate to OpenAthens platform
  - Some sooner, some later
  - Migrate when you're ready policy
- Seamless migration to OpenAthens



# What will OpenAthens cost?

- Free to HE/FE until Aug 2008
- Thereafter annual subscription will be graduated according to JISC bands (A-J)
- Provisional pricing for the OpenAthens (to be finalised by Aug07)
- Defined Service Levels
- Low cost

Band	Price
A	9500
B	8500
C	7500
D	6500
E	5500
F	4500
G	3500
H	2500
I	1500
J	800

## Summary

- OpenAthens design philosophy – open and extensible framework
- OpenAthens provides a cost-effective technical and policy infrastructure for
  - engaging with multiple federations
  - engage with new standards and technologies as they emerge
  - quickest, easiest and lowest cost way of joining the UK Federation?
  - continued access to Athens and Shibboleth resources
- Connecting

**Anyone to Anything from Anywhere**

JISC

# JISC Conference 2007

