

1 Introduction

1.1 The Identity Project Background

The Identity Project addressed the current practice and future needs of UK academic institutions in Identity Management ([IdM](#)). The [IdM](#) issues which were investigated included Grid use, Shibboleth installations of varying degree of maturity, collaborative courses and other long term inter-institutional collaborations, internal and shared dynamic virtual organisations, classes of users other than standard staff/student mix, library access schemes, and NHS involvement.

Partners in the project are:

- [Cardiff University](#) (project lead partner)
- [London School of Economics & Political Science](#) (leading the case studies work package)
- [Birkbeck College](#)
- [Goldsmiths College](#)
- [Imperial College London](#)
- [Queen Mary University of London](#)
- [Royal Holloway College](#)
- [School of Oriental & African Studies](#)
- [University College London](#)
- [University of London](#) (associate partner, not funded by the JISC)

Each partner carried out an audit of their [IdM](#) processes, as described in the [Audit final report](#). A large part of this was concerned with issues surrounding membership of an institution. The project also ran a wide-ranging survey, circulated to every HE institution in the UK, which also addressed these issues; this is described in the [Survey final report](#). This report is based on the information gathered through these activities.

The project started on 1 November 2006 and ended on 31 October 2007. The project was funded under the JISC [e-infrastructure programme](#).

Further information about the project generally can be found via the [project web site](#).

The primary focus of this report is on examining current technologies available to institutions to assist with IDM within, and between, institutions. This is an important area to investigate as many institutions do not have a clear idea of the range and abilities of such technologies available.

1.2 Market definition

Before assessing the commercial products and community projects available to assist the various tasks associated with Identity Management, some market definitions are required. This is particularly the case in this sector since the term Identity Management has been used by vendors as a marketing buzzword rather than as a description of a technology. What one vendor means when referring to Identity Management can be very different to another.

The following areas are all considered part of identity management by one vendor/project or another:

- User account provisioning
- User account management
- Authentication
- Authorisation
- Federated Authentication
- Federated Authorisation

None of these represents Identity Management in isolation, but each can form part of an overall Identity Management solution. Authentication and authorisation are sometime collectively referred to as Access Management.

2. The identity problem

In Identity Management, user accounts are usually considered synonymous with identities. This may be sufficient for many implementations, but conceptually an identity should exist independent of an account. Accounts imply rights to do something, identities imply a relationship with an organisation. These are not the same. For example, an applicant for a IT support post at an organisation has a relationship with that organisation, and probably exists in some form in an HR system. However, the applicant would not normally require an account before actually joining. However, it may be that an Identity Management system needs to be aware of the applicant before the join date in order to link the HR details to a separate system responsible for sending out corporate literature.

Dealing with identities defined thus is not the primary function of most identity management software, which is primarily account based. However, this is a concept that can be included in the design of an Identity Management solution.

3 Usage scenarios

It is useful to consider identity management from two points of view: that of an organisation whose primary “resource” is people; and that of an organisation whose primary “resource” is information. The focus of identity management in these two organisations will be different.

The first organisation (A) will be concerned primarily in ensuring that systems become aware of people who require access to them at the right time, and so will be concerned in some form or another with account provisioning and management. In addition, they it will be concerned with how these users prove who they are when challenged by various systems.

The second organisation (B) will be more concerned with how it can securely grant access to the information to people who are not directly employed by it. These people may be members of the first organisation and have accounts there.

Federated authentication links the two organisations by defining (and providing) a mechanism for the organisation A to verify the identity of their members to the satisfaction of the organisation B. This verification will normally occur when a person from organisation A requests access to information at organisation B. Federated authentication requires that the authentication is performed by organisation A and that organisation B trusts this. It removes the requirement for users to have accounts at organisation B.

4 Project/project selection

The commercial products and community projects included in this section do not comprise an exhaustive list. The main criteria are that they should be in widespread use, or targeted for widespread use, within the UK academic community. In addition, in most cases beta software has been excluded.

4.1 Project/project functionality summary

The products/projects listed below have assessed at how they fit into the definitions in the previous section. These are abbreviated as:

- User account provisioning: UAP
- User account management: UAM
- Authentication: AuthN?
- Authorisation: AuthZ?
- Federated Authentication: fAuthN
- Federated Authorisation: fAuthZ

For each category, each product project is shown with either P if the category is its primary function (or one of them), or S if it has functionality that is relevant to the category, but it is not its primary functions. If it has no relevant functionality, the cell is left blank.

Name	Type	UAP	UAM	AuthN	AuthZ	fAuthN	fAuthZ
Novell Identity Manager	Commercial	P	P				
Sun One Identity Manager	Commercial	P	P				
Microsoft IIS (Identity Integration Server)	Commercial	P	P				
Oracle Identity Manager	Commercial	P	P				
Grouper	Open source				P		P
Signet	Open source				P		P
Penrose	Open source			S	S	S	S
PERMIS	Restrictive license				P		P
Shibboleth	Open source					P	P
SPML	Specification	P					
SAML	Specification					P	P
Liberty	Specification					P	P
WS*	Specification			P	P	S	S
SourceID?	Specification					P	P
OpenID?	Specification					P	P
Bandit	Open source	P	P	P	P		

As can be seen from the above, commercial products tend to concentrate on organisations (which have budgets!), whereas the specifications and open source projects concentrate more on the community with federated functionality.

5 Product descriptions and assessments

This section contains descriptions of the products and projects listed above. These include descriptions sources from the vendors or project team, comments based on testing within this project, and categorisation and assessment on the following criteria:

- Functionally
- Ease of installation
- Ease of configuration
- Ease of maintenance

5.1 Novell Identity Manager

Product home page: <http://www.novell.com/products/identitymanager/>

5.1.1 Vendor description

“Using Identity Manager, you can provision new employees 95 percent faster, and eliminate those tedious, labor-intensive manual procedures that usually accompany the hiring process. And at the other end of the spectrum, Identity Manager lets you revoke access immediately upon their departure from your enterprise. Best of all, everything is verifiable, so you can both enforce and prove compliance with all the security policies in place at your company”

5.1.2 Our comment

A mature and capable infrastructure for synchronising data between linked systems. Has Novell eDirectory at its core, which brings reliability and scalability, and uses an event driven model (with a fall-back to polling) to enable near real-time data synchronisation between systems. A web-based provisioning application is available, which includes work flow functionality. Also integrates with Novell Nsure Audit for compliance reporting. Highly customisable in the right hands. Also integrates with Novell Access Manager in an overall IDM solution.

5.1.3 Functionality

Supports links to a wide range of applications and systems:

Applications:

- Baan, HP Service Desk (Partner Developed Driver), J.D.Edwards, Lawson, Oracle, Peoplesoft, SAP HR, SAP R/3 4.6 and SAP Enterprise Systems (BASIS), SAP Web Application Server (Web AS) 6.20, Siebel, Sugar CRM (Partner Developed Driver)

Databases:

- IBM DB2, Informix, Microsoft SQL Server, MySQL[?], Oracle, Sybase, JDBC

Directories:

- Critical Path InJoin[?] Directory, IBM Directory Server (SecureWay[?]), iPlanet Directory Server, Microsoft Active Directory, Netscape Directory Server, NIS, NIS +, Novell eDirectory, Oracle Internet Directory, Sun ONE Directory Server, LDAP

E-mail systems:

- Microsoft Exchange 2000, Microsoft Exchange 5.5, Novell GroupWise[?], Lotus Notes

Mainframe:

- RACF, ACF2, Top Secret

Midrange:

- i5OS (OS/400)

Operating systems:

- SUSE Linux Enterprise, Debian Linux, FreeBSD[?], HP-UX, IBM AIX, Microsoft Windows NT Domain, Red Hat AS and ES, Red Hat Linux, Solaris, UNIX Files - /etc/passwd

PBX:

- Avaya PBX, Asterisk - (Partner Developed Driver), VoiceRD[?] - (Partner Developed Driver)

Other:

- Command Line Scripts, Delimited Text, Health Level 7 (HL7) - (Partner Developed Driver), DSML, Java Messaging Services (JMS) and IBM WebSphere[?] MQ, Identity Manager Driver for RSA - (Partner Developed Driver), Remedy (for Help Desk), Schools Interoperability Framework (SIF), SOAP, SPML

5.1.4 Ease of installation

Dependent on eDirectory, and effective implementation of IDM requires careful planning and installation and of multiple OS, Directory and Application elements. Therefore ease of installation rated low.

5.1.5 Ease of configuration

Standard Novell documentation of implementation scenarios mean that simple configurations can be simple to implement. However, any customisation increases the difficulty significantly, therefore rated medium.

5.1.6 Ease of maintenance

Standard Novell support available for core drivers, but customisations not supported by Novell. Solution support may be available from a Systems Integrator or Consultant. Rated medium.

5.2 Sun One Identity Manager

Product home page: <http://www.sun.com/software/products/identity/offerings.jsp>

5.2.1 Vendor description

“Sun's comprehensive portfolio of identity management solutions can help you manage, protect, store, verify, and share identity data throughout the enterprise and across extranets.”

5.2.2 Our comments

A suit of products covering account management and provisioning, authentication and access control and federation. Marketed squarely at US corporates and their requirement to comply with the Sarbannes Oxely act. As such it has a very strong audit and compliance infrastructure. Links with a large number of shrink wrapped products for provisioning, and has a choice of directories that can be used as the back end. Would require significant commitment and investment to deliver a solution.

5.2.3 Functionality

Supports links to a wide range of systems:

Standards:

- SPML, WfMC?, SPML

Applications:

- Oracle E-Business Suite, PeopleSoft? HRMS, SAP R/3 Enterprise, SAP Enterprise Portal, Siebel CRM, Virsa Access Enforcer, Bridgestream SmartRoles?

Directory servers:

- Sun Java System Directory Server, Lightweight Directory Access Protocol (LDAP) v3, Microsoft Active Directory, Novell eDirectory, OpenLDAP?

Databases:

- IBM DB2 Universal Database for Linux, UNIX, and Microsoft Windows, Microsoft SQL Server, Microsoft Identity Integration Server (MIIS), MySQL?, Oracle, Sybase Adaptive Server

Help Desk:

- Remedy Help Desk

Message platforms:

- Lotus Notes, Microsoft Exchange, Novell GroupWise², Blackberry RIM Enterprise Server, Sun Java System Messaging and Calendar Service, Java Message Service (JMS) Message Queue

Security managers:

- CA-ACF2, CA-Top Secret, IBM RACF, RSA SecurID², ActivIdentity², Natural, INISafe Nexess, Passlogix v-GO

Web access control platforms:

- Sun Java System Access Manager, IBM Tivoli Access Manager, CA eTrust SiteMinder², RSA ClearTrust²

5.2.4 Ease of installation

A complex system with many interacting elements. Rated low.

5.2.5 Ease of configuration

Out of the box configurations are relatively easy to achieve, anything further requires significant understanding and effort. Rated low.

5.2.6 Ease of support

Support for base product set available from Sun. Solution support may be available through Systems Integrators or Consultants

5.3 Microsoft IIS (Identity Integration Server) – note, this is scheduled to be replaced by the Identity Lifecycle Manager 2007, so a full assessment has not been carried out.

Product home page: <http://www.microsoft.com/miis/default.aspx>

5.3.1 Vendor description:

“Microsoft Identity Integration Server (MIIS) 2003 is a centralized service that stores and integrates identity information for organizations with multiple directories. The goal of MIIS 2003 is to provide organizations with a unified view of all known identity information about users, applications, and network resources.

MIIS 2003 helps improve productivity, reduce security risk, and reduce the total cost of ownership associated with managing and integrating identity information across the enterprise.”

5.3.2 Our comments

Fairly new, and reliant on partners to provide user-focussed functionality. Unusually in this field it uses a database as the backend rather than a directory, and confusingly refers to all connected systems as “databases” even though some may be directories.

Not assessed in detail since it is scheduled for replacement – if you are a Microsoft shop, wait for Identity Lifecycle Manager before assessing the project. The related add-on for Windows server

2003 provides some basic functionality which may still be of interest though.

5.3.3 Functionality

Syncs Active Directory/ADAM, NT 4.0, Exchange Global Address Lists (GAL), Novell eDirectory, Oracle 8i and 9i, Lotus Notes/Domino, SQL 7/2000, SunOne?/iPlanet/Netscape, IBM Informix, dBase, DSML, csv files

Also Identity Integration Feature Pack for Windows Server 2003, providing account provisioning, directory synchronization and identity integration between AD/ADAM and Exchange databases

5.3.4 Ease of installation

Not assessed

5.3.5 Ease of configuration

Not assessed

5.3.6 Ease of support

Not assessed

5.4 Oracle Identity Manager

Product home page: <http://www.oracle.com/products/middleware/identity-management/identity-manager.html>

5.4.1 Vendor description:

“The rights and attributes of each person who accesses your IT system continually change as roles, rules, and policies evolve within your enterprise. The challenge is compounded during mergers and acquisitions, and when sharing IT privileges with business partners and customers. Add to that, the burden associated with meeting regulatory and privacy requirements such as SOX, HIPAA, HSPD12, and many others. Oracle Identity Manager is a best-in-class user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories; and improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a stand-alone product or as part of Oracle's award-winning Oracle Identity & Access Management Suite.”

5.4.2 Our comments:

Oracle Identity Manager is part of a suite of products which together provide all aspects of identity management, such as federated authentication and authorisation. It claims to introduce a new paradigm of Application centric identity management, where applications have the ability to consume and provide identity centric data built into them. This fits into an overall services-based architecture. This appears to be an aspiration since the technical documentation describes a central repository, linked to various applications.

5.4.3 Functionality:

Synchronises a wide range of databases, directories and applications through standards-based or application specific connectors.

5.4.4 Ease of installation

A complex system with many interacting elements. Rated low.

5.4.5 Ease of configuration

Out of the box configurations are relatively easy to achieve, anything further requires significant understanding and effort. Rated low.

5.4.6 Ease of support

Support for base product set available from Oracle. Solution support may be available through Systems Integrators or Consultants

5.5 Grouper

Project home page: <http://middleware.internet2.edu/dir/groups/grouper/>

5.5.1 Project description

“As a result of initial investigations by the MACE-Dir-Groups Working Group, Grouper was developed as an open source toolkit to address the needs of managing groups. Grouper is designed to function as the core element of a common infrastructure for managing group information across integrated applications and repositories. Grouper combines multiple sources of group information, both automated and manual, in managing memberships and other group information in a Groups Registry, a central information asset complementary to a site's Person Registry. A few of the benefits of a groups management service, such as Grouper, include:

- a common user interface and standard API for managing groups
- the same groups are made available to many applications
- distributed authorities are able to directly manage access information
- sophisticated group management capabilities, such as subgroups and composite groups, to support many access management needs.

In addition to basic group management and search capabilities, Grouper's design includes support for: basic group management by distributed authorities; subgroups; composite groups (whose membership is determined by the union, intersection, or relative complement of two other groups); custom group types and custom attributes; traceback of indirect membership; delegation.”

5.5.2 Our comments

An Internet2 project, the function of Grouper is simply to organise “things” into groups. These “things” can be users, existing groups, or other objects such as computers. They can exist in data sources external to Grouper, including LDAP directories and databases. The groups that Grouper groups these “things” into are stored in a database dedicated to Grouper, as are the membership of these groups. Fairly sophisticated concepts, such as group intersection (membership of two groups) are supported by Grouper.

The idea is that other applications (such as Shib) can query Grouper to determine group membership for someone (or something) requesting access and do something useful with this information. A weak point of Grouper is that there is no method of interfacing with it in real time that applications could be expected to support without development. Current methods include export of data from Grouper in XML format, or command line. If a real-time interface were implemented to a standard that meant it could be queried easily, the usefulness of the software would increase.

5.5.3 Ease of installation

Requires some knowledge of Tomcat and Java to get it working, otherwise very easy. Rated high.

5.5.4 Ease of configuration

All configuration beyond the initial configuration is preformed in the web-based UI. Initial configuration is held in Apache Ant build scripts. Documentation is targeted at developers, and is lacking in some areas. Rated medium.

5.5.5 Ease of support

as an open source project, community support is available. Rated medium.

5.6 Signet

Project homepage: <http://middleware.internet2.edu/signet/>

5.6.1 Project description

“Core middleware services such as identity management, directory, and authentication provide a foundation for secure, manageable applications throughout an institution. Even with this foundation, as systems and applications proliferate it becomes more and more difficult to manage user access consistently and cost-effectively. A privilege management service is a relatively new component of campus middleware that addresses this problem by providing centralized management of user privileges across a range of applications.

The benefits of this service include:

- a standard user interface for privilege administrators
- consistent, simplified policy definition, via roles and integration with core campus organizational data
- improved visibility, understandability, and auditability of privilege information
- standard interfaces to other infrastructure services and to application systems to support integration “

5.6.2 Our comments

An Internet2 project. Signet is targeted at the same problems as Grouper (permissions control), but with a different emphasis. It seeks to map permissions that are defined in a store such as Grouper with what this practically means within applications and systems. For example membership of one group may represent read permission over student records, and another write permission. Signet is intended to make is easier to map application specific permissions to facts about users' accounts, such as group membership.

As with Grouper, Signet lacks an interface whereby an application can use it to decide what a user can do. There is a Java API, but, if it were used, this would require development in each application that is to support it. If a standards-based interface can be developed, then the project looks useful.

5.6.3 Ease of installation

Requires a little knowledge of Tomcat and Java to get it working, otherwise very easy. Rated high.

5.6.4 Ease of configuration

Documentation is targeted at developers, and is lacking in some areas. Rated medium.

5.6.5 Ease of support

As an open source project, community support is available. Rated medium.

5.7 Penrose

Project homepage: <http://docs.safehaus.org/display/PENROSE/Home>

5.7.1 Project description:

“Penrose is a java-based virtual directory server. Virtual directory enables federating (aggregating) identity data from multiple heterogeneous sources like directory, databases, flat files, and web services - real-time - and makes it available to identity consumers via LDAP”

5.7.2 Our comments

A virtual directory, based on Apache Directory and potentially a very useful project. It is capable of providing a virtual view, linking a variety of back end data stores together (including directories and databases) and presenting the consolidated data as a single directory accessible via LDAP. Could jump-start identity management projects, but could also be difficult to maintain as changes in the structure of directories and databases to which it provides a view would need to be tracked. Also needs testing for performance, reliability and scalability. For the latter synchronisation of virtual data to a real LDAP directory is supported.

Also see MyVirtualDirectory? (<http://myvd.sourceforge.net/>) which is similar to Penrose, but in Beta.

5.7.3 Ease of installation

Installation of Penrose server and the Eclipse-based Penrose studio is reasonably straightforward – rated high.

5.7.4 Ease of configuration

The complexity of configuration depends on your requirements. However, much of the documentation of the actual configuration steps is in the form of screencams, which may not be to your taste. Rated medium.

5.7.5 Ease of support: as an open source project, community support is available. Rated medium.

5.8 Permis

Project homepage: <http://sec.cs.kent.ac.uk/permis/>

5.8.1 Project description

“There are two separate aspects to securing access to your computer based resources: determining who the users are, and determining what they are allowed to do. The first of these is called authentication, the second is called authorisation (or privilege management). PERMIS is an authorisation system that complements your existing authentication system.

So...

What does PERMIS do for you?

- It helps to control access to your computer resources
- When users request access to your resources, PERMIS makes the access control decisions for you based on your access control policies and the roles of the users
- It uses only your policies, and makes sure they have not been tampered with first
- It allows you to delegate to trusted individuals the ability to assign roles to users on your behalf
- It makes sure that the trusted individuals do not exceed their delegated authority
- It supports dynamic delegation of authority, which allows any user with a role to delegate it to other users in the same group

...and

What do you have to do for PERMIS?

- Define who your users are, by defining the user groups and the roles that users can have
- Write your authorisation policy
- Assign roles to users or delegate this task to others
- Establish agreements with other service providers, so that your users can use their resources and their users can use your resources

You will also need

- An Authentication scheme, for example, username/password, Kerberos, PKI, etc.
- PERMIS provides you with the software that makes access control decisions, and also gives you the tools for managing your policies, your role assignments, and * delegations between users.”

5.8.2 Our comments:

A complex Access Management tool, based around a policy engine. Attributes can be either X-509 based credentials or unsigned depending on the scheme in use. It is relevant for both service providers and identity providers, providing the basic infrastructure for complex policy based authorisation decisions.

Its modular architecture means it can be integrated with Apache, Shibboleth, Globus Toolkit, .Net and Python. Its main strength is that it doesn't tie you to a single authorisation and authentication architecture.

It is released under a restrictive license which allows use of the software solely for Academic Research and teaching and does not allow changes to documentation or code. A BSD-licensed community version is also available at <http://www.openpermis.org/>.

5.8.3 Ease of installation

A complex, multi-stage installation. Rated low.

5.8.4 Ease of configuration

Configuration will normally depend on multi-party service agreements, which is likely to add to complexity. Rated low.

5.8.5 Ease of support

A mailing list and bug tracker exist on the project website. Rated medium

5.9 SPML

Home page: <http://www.oasis-open.org/specs/index.php#spmlv2.0>

Service Provisioning Markup Language is an Oasis XML standard for managing the provisioning and allocation of identity information and system resources within and between organizations. It is implemented by many products and can help with account provisioning in a heterogenous environment.

5.10 Shibboleth

Project home page: <http://shibboleth.internet2.edu/>

5.10.1 Project description:

“The Shibboleth software implements the OASIS SAML v1.1 specification, providing a federated Single-SignOn and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the Attribute information being released to each Service Provider. Using Shibboleth-enabled access simplifies management of identity and access permissions for both Identity and Service Providers. Shibboleth is developed in an open and participatory environment, is freely available, and is released under the Apache Software License. The Shibboleth Roadmap and timeline are available here. Detailed information about Shibboleth is available here.”

5.10.2 Our comments

An Internet2 project which provides federated access management functionality using a subset of SAML, wrapped in a robust, scalable protocol. Selected for the UK Academic federation. The underlying workings of the protocol are complicated, but these are hidden from the user. Conceptually it is fairly simple, but personal experience with a small number of people in UK HE and FE suggests that it is poorly understood.

5.10.3 Ease of installation

Some understanding of the underlying concepts is required, but installation of the java-based identity provider is relatively straightforward. The Apache module service provider element is more challenging, and required compilation on the target platform. Rated medium.

5.10.4 Ease of configuration

This will depend on the federation and how well documented its setup is. For UK academic use this is rated medium.

5.10.5 Ease of support

An active support mailing list, and fairly comprehensive WIKI. Rated as high.

5.11 SAML

Homepage: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Security Assertion Markup Language – is an OASIS standard for federated collaboration which securely exchanges XML messages regarding authentication and authorisation . The recent version 2 extended functionality and we are likely to see convergence on the use of SAML across a range of products and packages in this area.

5.12 Liberty

Homepage: <http://www.projectliberty.org/>

An industry initiative that has its roots in a response to the ill-fated Microsoft Passport programme. It defines open standards-based specifications for federated identity and identity-based web services. Essentially now an implementation of SAML with extensions. These extensions make it incompatible with SAML on the wire.

5.13 WS*

Specifications for authentication and authorisation included in the web services standards initiative. Microsoft and IBM are primarily behind the WS* initiative, but the standards are published and implementable by third parties.

5.14 SourceID?

Homepage: <http://www.sourceid.org/>

Provides a layer which enables multi-protocol federated access management. These protocols include SAML, Liberty, WS-Federation and CardSpace?. Potentially very useful in a heterogeneous environment, but needs testing.

5.15 OpenID?

Homepage: <http://openid.net/>

A highly publicised initiative which provides a means for individuals to assert their own identities through a simple, personalised URL. At its most basic, it assumes that self-validated assertions are sufficient, but institutional-level validation can be added, allowing organisations such as AOL to become OpenID? providers. Conceptually similar to Shibboleth, but differs through not using the SAML security model. However, only authentication is currently supported, although work is under way to extend into authorisation functionality.

5.16 Bandit

Homepage: http://www.bandit-project.org/index.php/Bandit_Summary

“A set of loosely-coupled components that provide consistent identity services for Authentication, Authorization, and Auditing. The Bandit project creates a community that organizes and standardizes identity-related technologies in an open way, promoting both interoperability and collaboration.”

The only beta grade project in this list, but included as it has a strong architecture and should be monitored.

6 Applying products/projects/specifications to real-world scenarios

The following scenarios are intended a rough guides as to where the products and projects described above fit into common requirements of organisations. They are not blueprints or system designs.

6.1 Organisation wanting internal Identity management

Consider packaged product such as Novell Identity Manager, Sun One Identity Manager, Microsoft

IIS (Identity Integration Server) and Oracle Identity Manager. These may require serious commitment to a wider suite of products to deliver real value. Also consider their suitability as point solutions, supplemented by existing or new applications and processes. Use of standards, such as DSML and SAML will assist in interoperability.

For an open source solution, keep an eye on Bandit.

6.2 Organisation wanting to be a Shibboleth IDP

Use of the official Shibboleth software should be considered, although it has been implemented independently (e.g. Guanxi at <http://www.guanxi.uhi.ac.uk/index.php/Guanxi>).

An authoritative authentication provider will be required for a Shibboleth implementation. You can have more than one authentication provider, but duplication across many leads to problems (such as: which username/password should a user who exists in more than one use?). If you don't already have a consolidated one in directory or database form, then consider using the Penrose directory to present a virtual view of various providers. Also consider synchronising the various providers into a single repository using an a product from a major vendor (as listed above). Penrose is likely to offer quick wins, but the latter may be more reliable, but take longer to implement. For this reason, Penrose may be suitable as a proof-of-concept.

You will also need a single source of attributes about people who have authenticated. This can be in the form of a single database or directory.

If complex authorisation policies are required, consider the use of Grouper, Signet or Permis.

6.3 Service provider wanting to be FAM compliant

Consider whether to implement a consolidated solution which closely integrates service provider with identity provider, versus a modular solution which emphasises interoperability. Consider Permis as the core authorisation engine. Consider standardisation on standard protocols in widespread use – Shibboleth for the educational community, or SAML for more widespread use and support in packaged products.

6.4 Set of organisations wanting to start a federation

Consider where the products and projects appear to be converging. At the moment SAML (or a subset of it with Shibboleth) appears the best bet for “managed” federations, and OpenID? for more informal federations.