The UK
Access
Management
Federation
FOR EDUCATION AND RESEARCH

UK Access Management Federation for
Education and Research

Identity Provider Deployment

2 June 2008

Version 1.0

CONTENTS

UK Access Management Federation for Education and Research

Identity Provider Deployment

1 Introduction

This is one of a series of documents covering technical, operational, and organisational issues relevant to the management of the UK Access Management Federation for Education and Research. This document provides advice on the deployment of an identity provider. The latest version of this document can always be found on the UK federation website[1].

Interworking between federation members is based on the willingness of service providers to trust the authentication and authorisation assertions made by identity providers about individual users. This involves two steps:

- a user presents credentials to an identity provider, acquired by the user as part of a registration process (typically, name and password);
- the identity provider makes assertions about the user, on behalf of the member organisation, to the service provider to which the user has requested access.

Each organisation that wishes its users to have access to federation services must decide how its registration and identification processes will operate, and how the identity provider service will be managed. These decisions will be influenced by the licensing and other requirements imposed by the providers of the particular services that users need to access and by the organisation's own organisational and technical resources. In some cases the organisation may decide to outsource either or both the registration and identity provider functions to another organisation by commercial agreement.

2 Methods of user registration

Methods of user registration vary in the cost to the organisation and in the quality of the identity assurance guarantees which they provide. The following approaches are in use:

- *Managed registration*. The organisation administers the issue of credentials to individual users. The user's identity can be verified whenever these credentials are presented to the identity provider, and can be linked to each session where assertions about the user are sent to a service provider.
- *On-site registration*. Where an organisation does not provide its users with individual computer accounts, it may arrange for credentials to be issued to any user who makes a registration request on-site. These credentials may subsequently be used on or off site. This provides anonymous registration with assurance that the user had access to the organisation's secure network when the registration was made.
- *Open access registration.* The user presents self-registered credentials obtained from an off-site supplier. This simply provides anonymous registration.

Only the first of these methods provides user accountability. All, however, enable the user to present a persistent identifier, albeit anonymous in the other two cases.

Methods that do not provide user accountability directly may be strengthened where the service provider operates an additional out-of-band registration process, typically based on a user's email,

[1] http://www.ukfederation.org.uk/content/Documents/Documentation

telephone, or in-person assertion. This can bind an arbitrary name provided by an identity provider to a more reliable form of identification. A method may be strengthened significantly by an in-person assertion of identity backed up with a photo ID, such as a student card.

In general, each identity provider is regarded as operating a single *identity assurance profile*, which describes the management processes it uses for identity assurance. A technical solution is now emerging which enables an identity provider which supports a range of identity assurance profiles to indicate the method used on a per-user or per-session basis. This can be used where different identity assurance methods apply to the enrolment of different individuals or to distinguish the particular authentication method used in this session. Standards approval for this capability should be completed during 2008.

3 User accountability

User accountability, as defined in the Rules of Membership[2], refers to the ability of the identity provider to associate an end-user with a given session where it has provided authentication. This capability is a requirement for many services:

- where the means must exist to investigate any suspected cases of misuse by individuals, such as when commercially sensitive content is involved, or when content is supplied on the condition that it is used for educational purposes only;
- where a closed group of collaborating users wish to preserve the privacy of their work;
- where a teaching resource is part of an integrated product whose operation depends on knowing the actual identity of individual users;
- where a sensitive service operated within the organisation is to be secured.

User accountability is not a service requirement in other cases:

- for resources licensed to all members of the organisation (traditionally these have used IP address checking to verify that the user is present on the organisation's secure network);
- for open services, such as many blogs and wikis, where the only requirement is that the user presents a persistent identifier (a 'handle').

Note that service personalisation can be supported through the use of persistent anonymous identifiers and does not depend on knowing the actual identity of the user.

Where an organisation which employs an outsourced identity provider asserts user accountability, then responsibility for the accuracy of this assertion remains with the organisation and is not transferred to the outsourced provider.

4 Attributes

Service providers within the federation make their services available to users on the basis of attributes about the user asserted by an identity provider. There are two kinds of attribute:

- *Unscoped.* The attribute is a conventional directory attribute; typically a simple text string.
- *Scoped.* The attribute is keyed to the user's organisation. It is common for service providers to offer services on the basis that a user is associated with a particular organisation. The organisation is identified by its *security domain*, also referred to as its *scope*, which is usually the same as the organisation's DNS name. The value of a scoped attribute can be informally represented as *value@scope* (this should not be confused with an email address, which it resembles). To ensure that service providers can rely on scopes to identify real-world organisations, digitally signed metadata published by the federation lists the security domains which each identity provider is entitled to use. Standard service

[2] http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf

provider software discards scoped attributes asserted by an identity provider unless the scope is assigned to the identity provider in the federation metadata.

Service providers vary in the attributes they require; see the federation's Technical Recommendations for Participants[3] for further details:

- *None.* Although this approach is deprecated, some service providers will offer service to any user of a particular identity provider on the assumption that each identity provider will always operate exclusively on behalf of a single organisation.
- *eduPersonScopedAffiliation.* It is common to offer services on the basis of the user's relationship (affiliation) with a particular organisation. The organisation, or organisational unit, is identified by its scope; the relationship may be *student, staff, employee* or covering all of those *member*. So a particular service provider might offer access to any *member@arbsd.sch.uk* or *member@ox.ac.uk*; another only to *staff@ncl.ac.uk.* Many services within the JISC Information Environment use this attribute as the main basis for authorisation. Resources are made available to any user whose eduPersonScopedAffiliation has a security domain corresponding to an institution which holds a licence for the resource and an affiliation value of *student, staff, employee* or *member*.
- *eduPersonTargetedID.* Often used in combination with eduPersonScopedAffiliation, this attribute provides a consistent, opaque pseudonym for the user that is different for each service provider This enables service personalisation while preserving privacy and preventing correlation of a user's activity between services.
- *eduPersonPrincipalName.* This scoped attribute provides a name for the user consistent across different services. Since the name is usually based on the same "net ID" used to log in to local services, it will usually be well known to the user, making it possible to create services with authorisation by access control lists that enumerate the names of approved users (*alice@abdn.ac.uk, erpl99@ed.ac.uk*, …).
- *eduPersonEntitlement.* This attribute enables an identity provider to assert that the user satisfies some set of criteria of interest to the service provider and relevant to its authorisation decisions; for example "Authorised to access restricted medical content" or "Member of the parking committee". Multiple values are allowed for the same user.

All organisations should develop an attribute release policy which specifies rules for the release of attributes by its identity provider. Different constraints on releasing information may apply for each service provider, including individual attribute values as well as any values for a given attribute type.

5 Security domain usage

The security domain present in a scoped attribute assertion is often the key information used by the service provider to make its authorisation decision. The following requirements apply to verify an organisation's authority to make such assertions:

- the security domain must correspond to an existing DNS name and so be readily distinguishable from other security domain names;
- normally, it must be owned by the organisation represented, either through formal registration or as part of a systematic name allocation scheme, such as *.sch.uk* assignment in the Schools sector;
- where it is not owned by the organisation, the actual owner of the DNS domain must approve the proposed use; the owner may delegate authority to an outsourced identity

[3] http://www.ukfederation.org.uk/library/uploads/Documents/technical-recommendations-for-participants.pdf

provider to assign the security domains corresponding to a group of organisations under the owner's common management.

This last case is common in the Schools sector, where a Local Authority (LA) which owns a set of security domains delegates to a third party, such as a Regional Broadband Consortium (RBC), the management of identity provision for a collection of schools under the LA's responsibility.

6 Choice of identity provider

An organisation may choose whether to operate its own identity provision or to contract identity provision to a third party based on several factors:

- the identity provision requirements of services important to its users;
- the practicality of implementing a solution compatible with the organisation's existing technical resources and administrative procedures;
- the technical and legal constraints in providing information about individual users;
- the balance of cost and benefit for insourced and outsourced identity provision solutions.

Regardless of the type of identity provider used, the organisation must become a member of the UK federation and agree to observe its Rules of Membership.

A variety of case studies, reports and advice on the possible deployment choices are available from the JISC[4].

6.1 Insourced identity providers

An organisation may choose to operate its institutional identity provider in-house using any federation-compliant software, and employing its own technical capacity to deploy and configure the service. Further technical advice on the deployment of the standard Shibboleth open source software is available from the federation website[5], from the Internet2 Shibboleth site[6], and the Shibboleth wiki[7].

Organisations may also use a third party service to provide assistance in deploying and configuring their in-house solution. Further information on third party services offering support for in-house solutions is available from the JISC[8].

6.2 Outsourced identity providers

Support for participation in the UK federation has been added to Athens, the proprietary access management system provided by Eduserv which has been in use in the H&FE community for many years. This enables existing Athens end-users to access federation services. The OpenAthens IdP (sometimes referred to as the Athens to Shibboleth gateway) supports managed registration for institutions which have implemented Athens Devolved Authentication and for institutions that supply Athens with uploaded user authentication data for use with classic Athens. Other institutions use classic Athens for on-site registration. OpenAthens is still under development, and its current status and technical properties may be confirmed by contacting Eduserv[9] directly.

Information on other third party providers of outsourced federated access management solutions may be obtained from the JISC[8].

Further considerations applying to outsourced identity provision are discussed in clause 7.

[4] http://www.jisc.ac.uk/whatwedo/themes/access_management/federation.aspx
[5] http://www.ukfederation.org.uk/
[6] http://shibboleth.internet2.edu/
[7] https://spaces.internet2.edu/display/SHIB/WebHome
[8] http://www.jisc.ac.uk/publications/publications/identityprovidersbpv1.aspx
[9] http://www.eduserv.org.uk/

6.3 Open access identity providers

The simplest possible deployment for a client organisation with limited resources is for its users to obtain individual accounts from an open access identity provider organisation (e.g., http://protectnetwork.org/) by open access registration. This should be sufficient for access to small, closed-group service providers prepared to manage individual access control lists (for example, a distributed research group whose members require access to a central data store). The level of assurance in the identities themselves is not a major concern if the service provider is willing to add entries to its access control list on the basis of out-of-band communications, for example a telephone call from a well-known colleague asking to add his eduPersonPrincipalName of *jimjones@protectnetwork.org* to the service provider's access control list. (Jim may work at a research institution that has not yet deployed its own identity provider.)

This approach, however, does not scale well: national data services will not be willing to manage access control lists for thousands of individuals; nor can they accept everyone with a protectnetwork.org scope, because anyone at all can obtain such an identity. Client organisations that need access to the kind of services which have previously used Athens for access management cannot use this approach which will be mainly of interest to smaller organisational sub-units such as research groups, for access to private resources, or for initial testing.

7 Issues for outsourced identity provision

An outsourced identity provider may operate in a variety of ways in terms of its method of user registration, its representation in federation metadata, its security domain usage, its attribute usage, its attribute release policy, and the risk of customer lock-in.

The choice of these methods of operation should form part of the agreement between the client organisation and the outsourced identity provider.

7.1 Available registration methods

An outsourced identity provider may support any of the methods of user registration described above (managed, on-site, or open access registration) on behalf of a client organisation.

a) It can support managed registration, and hence user accountability, if it is linked to the organisation's staff and student databases. This may be arranged by periodic upload of user information to the identity provider, or by some other form of integration. Note that any disclosure of personal information must be covered by a data processor contract in order to comply with the Data Protection Act 1998.

b) Where no such integration is available, the outsourced identity provider can support on-site registration by enabling the organisation's users to self-register using equipment known to be present on the organisation's secure network; the identity provider performs an IP address check on each registration request. Re-registration should be required at least once a year.

c) Otherwise, the organisation can simply recommend one of several available open access identity providers to its users where such identities are acceptable to the target services of interest.

7.2 Representation in federation metadata

An outsourced identity provider will typically act on behalf of a number of client organisations. This may be represented in federation metadata in either of two ways.

a) *Single entity.* A single entity representing all of the client organisations is present in the federation metadata (i.e., the identity provider systems are represented by a single metadata entity). The identity provider is permitted to assert any of the security domains (scopes) belonging to its client organisations and is trusted to assert the appropriate security domain in each case.

b) *Multiple entities.* A distinct entity for each client organisation is present in the federation metadata. Each entity has a security domain corresponding to the security domain of a single client organisation, but otherwise, most of the configuration information is identical for each entity and refers to the identity provider's systems, not the client organisation's.

Where the only distinction between client organisations is in their security domains, then the simplification of handling a single entity in the federation metadata rather than a large number of separate entities makes this approach preferable. This is often the case where identity provision for a group of related organisations under common management is collectively outsourced. Where client organisations vary in other ways, such as support for user accountability, which must be reflected in federation metadata, then the use of multiple entries becomes necessary.

7.3 Attribute usage

Where identity provision has been outsourced, the four core attributes described in the Technical Recommendations for Participants[3] may be handled as follows:

— *eduPersonScopedAffiliation*. Unless the identity provider has access to information supplied by the organisation which indicates the user's status, it will be able to assert only the value *member*. Otherwise, it may assert the value appropriate to the user's status where permitted by the governing attribute release policy.

— *eduPersonTargetedID*. The identity provider should be able to supply this attribute in the normal way. Note that the attribute is interpreted relative to the entity name provided for the organisation by the outsourced identity provider. A change of entity name could entail the loss of any personalisation data linked to the attribute.

— *eduPersonPrincipalName*. This may be generated from information supplied by the organisation or created by the outsourced identity provider. The value actually used should always be visible to the user, as some services, such as wikis, require the user to register this explicitly.

— *eduPersonEntitlement*. This attribute may be supported where suitable procedures exist for its administration by the organisation.

7.4 Attribute release policy

As indicated in clause 4, every organisation requires an attribute release policy which specifies the rules under which information about users is disclosed to service providers. These rules may be represented as a table which indicates for each service provider the attributes to be released in that case; this may include rules for the release of specific attribute values as well as all values of a given attribute type.

A client organisation must be able to convey its attribute release policy to its outsourced identity provider to ensure that the provider releases attributes only when authorised. The identity provider should, where necessary, be able to apply a different attribute release policy for each organisation it represents (though a widely acceptable default rule will be to release *eduPersonScopedAffiliation* to all service providers and *eduPersonTargetedID* to any which request it).

Where an authority is responsible for the common management of a group of organisations, it may specify a common attribute release policy which the outsourced identity provider is instructed to observe for all client organisations for which no individual policy is specified.

In no case should attributes be released which disclose personal information without the explicit instruction of the organisation or the organisation's managing authority.

Where the identity provider holds information about individual users (for example e-mail address, personal name) then there should be a written legal agreement setting out how this information will be handled and protected, and directing which attribute release policies shall be configured for each service provider. This is necessary to ensure that both the client organisation and the identity provider remain within the terms of the Data Protection Act 1998. Guidance on sharing personal data is available from JISC Legal[10] and on outsourcing from the Information Commissioner[11]. The federation's Recommendations for Use of Personal Data[12] contains more information on attribute release policies and the protection of individual privacy.

7.5 Vendor lock-in

An organisation which employs an outsourced identity provider should obtain a guarantee that the information presented to service providers on its behalf will contain as little information as possible that is specific to the outsourced identity provider. A failure to ensure this may lead to effective lock-in to a particular identity provider where provider-specific information is recorded in licence registration information and other configuration data used by service providers. If identity provider-specific information is used then stored user information, accounting data and other licence permissions are likely to be lost when the organisation chooses either to change identity provider or to operate its own identity provider system. If the same information is provided by an outsourced identity provider for a number of organisations then service providers may find it difficult or impossible to provide services tailored to individual client organisations.

In particular, all security domains present in attribute assertions should belong to the organisation, or be registered to an agent acting under the instruction of the responsible authority (e.g. the LA). They should not be values relative to the outsourced identity provider.

8 Institution types

It is likely that different solutions will be prevalent in different communities. Some of the factors relevant to different types of institution are described below.

8.1 HE institutions

Many large HE institutions already operate a single-signon scheme for their users and are likely to opt for an in-house identity provider solution. The ongoing costs, following initial deployment, will include the facilities management for service equipment and the management of attribute assignments for individual users (in particular for attributes such as eduPersonEntitlement).

Other HE institutions will have well-developed registrar functions for assigning computer identities to students, but still may not wish to spend time acquiring the skills required to deploy their own in-house identity provider. Outsourcing to an identity provider organisation that asserts attributes based on an institution's own user database should be possible, but is likely to incur significant up-front costs, both in the inevitable customisation required for the identity provider organisation's systems to access this database and in creating a suitable contract in the absence of existing models. Bear in mind that both the identity provider organisation and the client organisation have to commit to observing the UK federation's terms and conditions, and therefore they must clearly divide between them the obligations which this entails.

8.2 FE institutions

Many FE institutions do not give their students individual computer identities and therefore do not maintain a large-scale registrar function. In those cases, an outsourced identity provider organisation may be attractive if it is willing to undertake either on-site registration or managed registration on behalf of the client organisation. The identity provider must be able to assert a scope associated with the client organisation rather than the identity provider organisation, e.g., for scoped affiliation *member@jevc.ac.uk* for Jewel and Esk Valley College, rather than *member@outsourcer.com*. (The alternative of *member@jevc.outsourcer.com* is also feasible for identifying the organisation to service providers but deprecated since the client organisation is

[10] http://www.jisclegal.ac.uk/publications/datasharing.htm
[11] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/outsourcing_-_a_guide_for_small_and_medium_businesses.pdf
[12] http://www.ukfederation.org.uk/library/uploads/Documents/recommendations-for-use-of-personal-data.pdf

obviously tied to the identity provider organisation.) Note that the identity provider organisation should offer some convenient mechanism to give the client organisation control over which user attributes may be released to which service providers. Minimising the attributes released to each service provider to only those genuinely necessary helps preserve user privacy.

One issue arises when the outsourcer also owns the user registration data. In this case, there is substantial risk of vendor lock-in. For example, switching vendors or setting up an in-house identity provider may require changing the eduPersonTargetedID values associated with users, resulting in personalisation information being lost, including saved searches and stored user preferences. At worst, depending on the contract negotiated with the old vendor, users might need to be issued with completely new identities (if the user database is not available to the client organisation). Since drawing up effective contracts will require some of the technical knowledge that the client institution is trying to outsource, it would be wise to assume, at least until model contracts emerge over time, that the client organisation's relationship with an outsourcer is likely to be a long one, and hard to change.

At least one service within the UK Federation currently bases its authorisation decisions on whether the identity provider is in its list of customer identity providers, rather than on attributes asserted by the identity provider about a user. Institutions wishing to make use of such a service cannot use an identity provider organisation that presents itself to service providers as a single identity provider with different scopes distinguishing users from its several client organisations. Only identity provider organisations offering a distinct identity provider entity for each client organisation can support such service providers. However, service providers are being strongly recommended to base their authorisation decisions on user attributes rather than maintaining lists of approved identity providers, so this should not be seen as constraining the choice of identity provider organisation in the longer term.

8.3 The Schools sector

The Schools sector is in many ways the most complicated case, both in its scale and in the variety of its administrative arrangements. The parties involved are:

— *Client organisation.* The school. Note that service providers rely on scopes to distinguish organisations, so in order for a service provider to be able to render its services to some schools in an LA area but not others, users from a particular school should have a scope associated with the school, not with the LA.

— *Identity provider organisation.* May be a commercial organisation operating under contract to an LA or RBC. Alternatively, it may be the RBC itself.

— *Registrar.* May be an LA, an RBC, in some cases the school itself, or a commercial organisation or consultant operating under contract to any of them.

When an identity provider organisation is not performing the registrar function, there is less risk of vendor lock-in, provided that scopes are associated with the client organisation rather than with the identity provider organisation, as described previously (though retaining personalisation data when changing identity provider is still a problem).

Both identity provider organisations and client organisations must agree to observe the UK federation's terms and conditions. For schools, an LA or RBC is allowed to agree on behalf of the schools for which it is responsible, but even with this simplification, ensuring that suitable contracts are in place between all the parties, particularly commercial organisations, to assure service providers and the federation that an identity provider asserting attributes about a school pupil will make only accurate assertions, which everyone involved will stand behind, is one of the less obvious costs of outsourcing. Creating good contracts is likely to require considerable effort in the early days before model contracts become available.