



**UK Access Management Federation
for Education and Research**

Federation Operator Procedures

22 November 2006

Version 1.0
ST/AA/UKF/DOC/005

Contents

1	Introduction	3
2	Membership application processing	3
3	Registration of entities	4
4	CA qualification	5
5	Support	6
6	Monitoring	7

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 describes the procedures undertaken by the federation operator:

- membership application processing;
- registration of entities;
- CA qualification;
- support;
- monitoring.

2 Membership application processing

All organisations that wish to join the UK Federation must first send a formal application for membership and agree to be bound by the federation's Rules of Membership, as published on the federation website (<http://www.ukfederation.org.uk/content/Documents/FedDocs>). This applies to both identity providers and service providers. Where an applicant intends to use an outsourced provider, such as Eduserv's Athens gateway service, both the applicant and the external organisation providing the outsourcing service must become members of the federation

The main steps of the procedure followed by the federation operator are summarised below. Details of the information the applicant is required to supply is shown at <http://www.ukfederation.org.uk/content/Documents/JoinFederation>.

- a) *Application.* An application to join the federation is received in writing, and is checked for accuracy and completeness. Additional checks on the identity of the applicant may be made.
- b) *Eligibility.* The eligibility of the organisation is evaluated. All educational and research institutions, and groups within those institutions, are eligible to join the federation; this may be extended to include other publicly funded organisations such as museums and library services, subject to suitable funding support from the appropriate bodies. In addition, other organisations, including commercial organisations, that provide services relevant to the work of other members, may be sponsored by those members to join the federation. The federation operator is given some latitude to evaluate eligibility in the light of its understanding of the overall goals of the federation.

The key individuals identified in this process are the Executive Liaison, who is responsible for making the application and is authorised to legally bind the organisation, and the Management Liaison who has the authority to request the registration of identity provider and service provider entities on behalf of the organisation. The Management Liaison is also responsible for registering use of an outsourced provider supplied by an external organisation.

3 Registration of entities

An organisation which has been accepted for membership of the UK Federation may register any number of identity provider and service provider entities. The organisation may devolve the operation of a provider to any group within the organisation (including department, faculty, or project), or to an external agency.

The information supplied by the applicant is checked as described below. The information required varies according to the type of registration being made (identity provider, service provider, or outsourced provider). See <http://www.ukfederation.org.uk/content/Documents/RegisterEntities> for further details.

- a) *Authority.* The request to register an entity must be made by the Management Liaison. Where the entity being registered is an identity provider, the Management Liaison must also specify the security domains that the identity provider is authorised to assert. The Management Liaison may delegate authority to an administrative contact for providing registration data to the federation operator and for the operation of the entity.
- b) *Security domains.* Any security domains (scopes) claimed by an identity provider must correspond to a DNS name registered to the applicant. This name may already be known to belong to the applicant organisation (in the case of a large institution, for example). For less familiar names, a registry check or other independent verification may be required. If the scope is the same as the domain name of the applicant's Shibboleth server then no check is necessary, since the CA that issued the server certificate is trusted to verify the certificate holder's right to use the domain.

Exceptionally, an organisation may delegate full managerial responsibility to an external organisation and authorise it to register security domains on its behalf.

- c) *Completeness.* The information supplied by the applicant is checked for typographical errors, inaccuracies and omissions. Common configuration errors can usually be identified at this stage. Further communication with the administrative contact may be necessary to ensure that all required information is available.

- d) *Certification.* The applicant must possess X.509 certificates for its Shibboleth server(s), drawn from a list of CA products approved for use in the federation.
- e) *Technical standards.* Where possible, the applicant's adherence to the Technical Recommendations for Participants and the Federation Technical Specification is confirmed. The federation requires that the URLs of Shibboleth server components conform to the HTTPS (SSL) scheme rather than unsecured HTTP, and requires scopes registered to the applicant to be valid DNS names.
- f) *Consistency.* The consistency of server URLs, certificate subject name, letter of authority, and claimed scope(s) is checked. In practice, anomalies discovered in cross-checking occur as the result of registration errors and can usually be resolved by email exchange.
- g) *Policy disclosure.* Disclosure of policy on identity management by identity providers and on attribute usage by service providers is recommended as a means of building mutual confidence among members of the federation. The information is made publicly available to other federation members, where possible by placing it in the federation metadata.
- h) *Outsourced provider.* Where an organisation intends to employ an identity provider or service provider supplied by an external organisation, details of that organisation and of the authority delegated to it are specified. The federation operator verifies that the external organisation is also a member of the federation.

4 CA qualification

The federation relies on CAs to undertake real-world identity verification. Possession of a certificate from an approved supplier will often be the only independent verification of the identity claimed in a membership application submitted via insecure e-mail. It is crucial therefore for the federation operator to have faith in the identity verification procedures of the CA products it endorses. Since CAs generally offer multiple certificate product types, with different levels of identity assurance, the federation operator must evaluate each CA product individually rather than declare blanket acceptance of all products provided by that CA.

Before approving a certificate product, the federation operator evaluates products as follows:

- a) The federation operator inspects the vendor's published information about the different certificate products it offers.

- b) The federation operator makes judgements about which of these products are likely to be suitable for use with the UK Federation. A product whose acceptance entails extending trust to a range of additional products from that CA would not be a strong candidate for qualification; where the additional products offer lower assurance the product would not be accepted. Products that allow self-registration are not accepted. There is also a presumption against approving any certificate product that does not include at least some element of offline identity verification.
- c) For each product judged likely to be suitable, the federation operator applies for and obtains a one-year (or nearest available duration) certificate of that type. If the standard of identity verification exercised in practice by the CA is considered inadequate, or falls short of the standard claimed in the vendor's published information, that certificate product is not accepted.
- d) The federation operator verifies that an identity provider and a service provider, both using the standard software, can be configured to use the certificate obtained and interoperate successfully with each other. It will also verify interoperability with entities that use already qualified certificate products. (Some certificate products have in the past failed to operate with the Shibboleth software at a technical level.)

After qualification has been successfully completed, the federation operator will add the root CA certificate and any intermediate CA certificates required by the tested certificate product to the federation metadata. Each federation member's technical contact will be informed that a new certificate product is supported, to allow those running older (1.2) Shibboleth IdP implementations to update their CA certificate bundles by hand.

5 Support

The purpose of the federation operator's support activities is to assist new members in configuring their installations and to assist all members in resolving interworking problems.

The federation operator operates test identity provider and test service provider services which are available to members to exercise their deployments and to help diagnose configuration errors. Experience to date is that members require advice mainly for the initial configuration task and subsequently become self-sufficient. The federation operator's support activity is not intended to be open-ended.

The federation operator has, at most, only an indirect role in the resolution of interworking problems between members, and becomes involved only at the request of those members. The key information is held on log files owned by the identity provider and service provider and can only be examined if both parties disclose this information to the federation operator.

The UK Federation's recommended software base is the standard Shibboleth release as maintained by Internet2/MACE. The federation operator implements all new Shibboleth releases as they become available and maintains a current set of software versions for which technical support is provided. Members are strongly encouraged to upgrade their software before support for the version they are currently using has ended.

Members may use other third party software which is compatible with the supported versions of Shibboleth, but should then expect to obtain support from the relevant supplier.

6 Monitoring

The federation operator may undertake monitoring exercises from time to time in two areas:

- a) *Metadata refresh.* Members who do not refresh the published federation metadata at daily intervals will eventually be using inaccurate metadata. This may cause loss of service, or continuing exchange of information with an identity provider or service provider whose federation membership has ended. The federation operator may encourage members which continue to rely on stale metadata to implement a regime of daily refreshment.
- b) *Certificate use.* The handling and installation of certificates can be error-prone, and may result in a failure to secure service equipment as intended. A limited level of checking of this is possible by attempting to connect to service equipment and observing its response.

Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from the JANET Service Desk.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

© The JNT Association 2006