UK Access Management Federation for Education and Research

Federation Operator Procedures

6 October 2006

Version 0.4

ND/ATG/AAI/DOC/019

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:

- enrolment;
- CA qualification;
- support;
- monitoring.

2 Enrolment

All organisations applying for membership go through the enrolment process in order to join the federation. The main steps of the procedure followed by the federation operator are summarised below. Additional technical information is given in the Federation Technical Specifications and the Technical Recommendations for Participants.

a) Application. An application to join the federation is received, usually by unauthenticated (insecure) e-mail. In general, each organisation must apply for membership in its own right, even where it contracts the operation of its identity provider or service provider to a third party. In some cases, a registration authority for a group of organisations under common management may authorise an outsourced identity provider to supply operational management for those organisations on its behalf.

No identity checks are normally performed at this stage unless specific concerns arise over the identity of the applicant.

b) Eligibility. The eligibility of the applicant is evaluated. All educational and research institutions, and groups within those institutions, are eligible to join the federation as identity providers; 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 join as service providers at the discretion of the federation operator, which is given some latitude to evaluate eligibility in the light of its understanding of the overall goals of the federation.

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 applicant 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 servers conform to the HTTPS (SSL) scheme rather than unsecured HTTP, and requires scopes registered to the applicant to be valid DNS names.

f) Scopes. Any scope 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.

g) *Authority.* If the application is for an identity provider and the claimed scope corresponds to an entire organisation, or in the opinion of the federation operator to an organisation with a lifetime longer than a short-term project group, then a letter on headed notepaper is required from a suitably senior member of the organisation. This commits the organisation to observe federation policy, and asserts the scopes which may be claimed in attribute assertions (in effect, this states whether the identity provider is authoritative for the whole organisation, or just for a department or unit within it). The letter must also state the domain names of the servers which will issue assertions.

   For short-term projects with no formal claim of authority, all that is required is a commitment in the e-mailed application itself to observe federation policy.

h) *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.

i) *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.

It can be seen that offline verification of the applicant's claimed identity is normally performed by the federation operator only for long-lifetime identity providers, such as institutions. For other entities, the use of X.509 certificates in Shibboleth, and the restriction to HTTPS URLs in (e) above, enables this function to be performed by a trusted third party, the CA. The CA is trusted to issue server certificates only to the legitimate owner of the DNS name which is the subject of the certificate.

Service providers can therefore be confident that an informal project-group identity provider is operated within the organisation implied by its scope, but should not rely on the Organization details (e.g., project name) claimed for it in the federation metadata, since these are not subject to independent verification. A service provider relying on such an identity provider should confirm out of band the scope associated with the project it is dealing with.

3 CA qualification

The federation relies on CAs to undertake real-world identity verification. For entities other than institutional or departmental identity providers, possession of a certificate from an approved supplier will usually 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 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.

4 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 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.

5 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 been suspended. 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 using probing mechanisms to test the externally visible behaviour of service equipment.

The findings of all monitoring exercises are treated as confidential.