The UK
Access
Management
Federation
FOR EDUCATION AND RESEARCH
SUPPORTED BY JISC AND BECTA

UK Access Management Federation for
Education and Research

Federation Technical Specifications

Ian A. Young

1 June 2007

Version 1.1
ST/AAI/UKF/DOC/004

Table of Contents

1 Introduction

This document specifies the detailed technical architecture of the UK Access Management Federation for Education and Research (the UK federation).

> *Where appropriate, this document also describes the rationale behind the particular choices made. Paragraphs describing rationale are formatted in this way.*

A companion document, the *Technical Recommendations for Participants* ([UKTRP]), provides specific technical recommendations for members of the federation based on these specifications.

1.1 Keeping Up To Date

Due to the rapidly changing nature of the software and standards associated with identity technologies, it will be necessary to update this document frequently to reflect new developments. The latest version of this document can always be found on the federation web site (see [UKFTS]); federation members should review the latest version of this document periodically, and in any case whenever a new deployment is contemplated.

New editions of this and other federation technical documents, as well as other announcements thought to be relevant to federation members, are reported on the federation mailing list. The technical and administrative contacts listed for all entities registered with the UK federation are made members of the mailing list automatically; other addresses can be added to the list by request.

1.2 Document Status

This edition describes the UK federation with effect from 1 June 2007.

1.3 Recent Document Changes

1.3.1 Changes for Edition 1.1

- Added the `UKFederationMember` label. Entities owned by federation members are now explicitly labelled, rather than being indicated implicitly by the absence of the `SDSSPolicy` label.

- Changed the definition of the `SDSSPolicy` label to allow its retention even when an organisation has become a UK federation member.

- Added the `DeletedEntity` label for internal use by the federation operator.

- Removed potentially misleading comments from metadata examples.

- Described the various conventions used for the `Organization` element in UK federation metadata.

- When abbreviating the federation's name, use "UK federation".

1.3.2 Changes for Edition 1.0

- Added "Future Directions" sections; reworked some of the rationale in "Trust Fabric" to take advantage of this.

- Added a major section on "Metadata Usage and Extensions".

- New document numbering.

1.4 Future Directions

Each major section of this document contains a sub-section called "Future Directions" describing likely future developments in the area under consideration. These notes are provided to allow members to incorporate this information into planning activities.

2 Trust Fabric

The underlying trust fabric for the federation is based on X.509 Public Key Infrastructure (PKI) technology, which enables mutual authentication between IdP and SP servers and user browsers. This is based on use of the SSL/TLS protocol and XML digital signatures using keys contained in X.509 certificates, conventionally obtained from independent Certification Authorities (CAs).

An alternative approach, supported in Shibboleth 1.3 onwards, is to dispense with CAs altogether and simply to bind keys asserted by members directly to Shibboleth entities by including these public keys in the federation metadata. In effect, the federation operator assumes the role of CA.

This approach may in time become accepted as a method conferring a degree of assurance similar to that given by conventional certification. For the foreseeable future, however, the federation requires members to obtain X.509 certificates from one of a specified group of conventional CAs. The current list of acceptable certificate products is described in [UKTRP]; the process by which new CAs and CA products are validated and accepted into the UK federation's trust fabric is described in [UKPROC].

> *At a technical level, switching from a PKI trust fabric to a "direct key" mode would require all federation members to be capable of operating on the basis of keys embedded directly in the metadata. This mode of operation is supported by Shibboleth 1.3 and later, and by Guanxi, but not by earlier versions of Shibboleth or by current versions of AthensIM. At present, with around 10% of the federation's entities unable to utilise a direct key trust fabric, it is not possible to move to a purely direct key model.*
>
> *The second issue with a pure direct key trust fabric is that the federation operator can no longer rely on the verified procedures of the CA to take some of the load of identity proofing for entities. This increases the federation operator's costs. Against this must be balanced the costs of verifying the CA's own procedures and tracking technical changes in the CA's certificate product offerings over time. This trade-off changes as the size of the federation increases: at larger scales, it is more cost-effective to "outsource" institutional identity proofing by qualifying commercial CAs than it is for the federation operator to perform the same work.*

The use of commercial CAs is not a perfect solution. Their registration procedures are not fully transparent and are subject to change without notice. Further, each new certificate product proposed for use in the federation has to be tested for the rigour of its enrolment procedure and for its technical compatibility with Shibboleth, both of which are time-consuming tasks.

In the Server Certificate Service (SCS) managed by TERENA, the national academic operator in each country acts as Registration Authority (RA), and communicates certification requests to a single commercial CA. (In the UK, the RA is UKERNA.) This offers several advantages over the use of commercial CAs:

- the CA is acting according to service requirements set by the academic community;
- the cost to institutions is lower, and billing is simpler;
- the RAs already have a trust relationship with the client institutions.

2.1 Future Directions

As an alternative to requiring that either the CA-based or the direct key scheme is used exclusively, it may be possible to reach a compromise between the two pure schemes by implementing one of a range of hybrid models, in which both direct keys and CAs play their part. Such a hybrid trust fabric can combine the performance and other benefits of the direct key approach with the external identity proofing advantages of PKI using commercial CAs, and could be operated without interruption during a transition phase from one scheme to the other. Additional work is still required, however, to determine whether a hybrid approach would be appropriate for the federation.

A move towards a hybrid trust fabric is likely to be required in any case in order to support some features of SAML 2.0, such as signing and encryption of SAML messages.

3 Metadata Usage and Extensions

The federation publishes metadata describing participating entities. This metadata provides the information required for entities to know how to communicate with each other, and establishes a trust fabric permitting entities to verify each other's identities.

The federation's standard metadata format is based on the metadata profile defined by the Shibboleth software. The Shibboleth profile is itself based on [SAML2Meta], [SAML1Meta-xsd] and [SAML1Meta], with additions defined in [ShibProt] section 3.4. These standards leave the meaning of some constructs undefined to allow flexibility, and allow extensions to the metadata to be defined to meet unforeseen requirements. This document therefore specifies the UK federation's particular uses of the standardised constructs, and documents the extensions to the standards which are used in the federation's published metadata.

3.1 UK Federation Label Namespace

The following XML namespace is defined for use in UK federation metadata:

http://ukfederation.org.uk/2006/11/label

All elements defined in this namespace will take the form of simple labels which are either present or absent in a particular context. Labels may be either XML elements (with or without attributes) or simple attributes.

Note that although the identifier for the label namespace contains its date of definition, additional elements may be added to this namespace at any time.

3.1.1 SDSS Policy Label

During the transition from the SDSS federation to the UK federation, entities registered by members of the SDSS federation are temporarily "grandfathered" into the UK federation metadata even though the member's participation will initially be under the looser policies devised for the SDSS federation.

Such legacy entities are indicated by the presence of the following label element within the `Extensions` element of their `EntityDescriptor` element:

```
<SDSSPolicy xmlns="http://ukfederation.org.uk/2006/11/label"/>
```

After a federation member agrees to the Rules of Membership (see [UKROM]), it confirms to the federation operator those entities which it wishes to retain within the UK federation. The federation operator will then add the `UKFederationMember` label to the metadata for those entities to signal that they now operate under the Rules of Membership.

At the end of the transition period, all entities still labelled as only operating under the SDSS Federation Policy will be removed from the UK federation.

Federation members are strongly recommended to verify through inspection of the published metadata that each of their entities has been appropriately recognised as operating under the UK federation rules prior to the end of the transition period.

3.1.2 UK Federation Member Label

If an entity is owned by a member in good standing of the UK federation, the following element will be added to the `Extensions` element of the entity's `EntityDescriptor` element:

```
<UKFederationMember
   xmlns="http://ukfederation.org.uk/2006/11/label"/>
```

The presence of this element indicates that the owner of the entity has agreed to be bound by the UK federation's Rules of Membership [UKROM].

3.1.3 Accountable Users Label

The federation's Rules of Membership allow for a member to assert to the federation operator that a given identity provider entity provides for user accountability (see [UKROM] section 6.1). A member making such an assertion must comply with all the requirements of section 6 of the Rules.

If such an assertion has been made to the federation operator in respect of an entity, the following element will be added to the `Extensions` element of that entity's `EntityDescriptor` element:

```
<AccountableUsers xmlns="http://ukfederation.org.uk/2006/11/label"/>
```

Note that the assertion of user accountability is made by the federation member alone; it is not verified by the federation operator.

3.1.4 Deleted Entity Label

As part of the maintenance of federation metadata, the federation operator may mark an entity as "deleted" by adding the following element to the `Extensions` element of the entity's `EntityDescriptor` element:

```
<DeletedEntity xmlns="http://ukfederation.org.uk/2006/11/label"
    date="deletion date"/>
```

The `date` attribute should contain the date on which the entity was marked for deletion, in `xs:date` format (CCYY-MM-DD, for example `date="2006-11-30"`).

The effect of this label is to prevent the metadata for the individual entity from being included in the published metadata for the federation. Consumers of UK federation metadata should never encounter this label, and have no need to check for its presence.

3.2 SDSS Federation WAYF Namespace

UK federation metadata currently makes use of an XML namespace originally defined by the SDSS federation:

http://sdss.ac.uk/2006/06/WAYF

This namespace is used solely to label identity provider entities in order to hide them from the normal (filtered) federation "Where Are You From" (WAYF) service. This is done by adding the following element to the `EntityDescriptor`'s `Extensions` element:

```
<wayf:HideFromWAYF xmlns:wayf="http://sdss.ac.uk/2006/06/WAYF"/>
```

The different central federation WAYF services are described in section 6.3 of [UKTRP].

3.3 `EntityDescriptor` Element

3.3.1 `ID` Attribute

Each `EntityDescriptor` element is given a unique `ID` attribute, formed by concatenating the two letters "`uk`" and six decimal digits, such as "`uk000123`". This attribute value is used as a name for the individual `EntityDescriptor` by the federation operator as part of the operational procedures of the federation.

During the transition from the SDSS federation to the UK federation, it will always be the case that:

- Entities which appear in both the SDSS federation metadata and the UK federation metadata will have `ID` attribute values of `uk000199` or lower.
- Entities which only appear in the UK federation metadata will have `ID` attribute values of `uk000200` or higher.

This convention will not necessarily be observed after the end of the transition period, at which time the SDSS federation will cease to exist.

3.4 `Organization` Element

The SAML 2.0 Metadata specification defines the `Organization` element as specifying "basic information about an organization responsible for a SAML entity or role" ([SAML2Meta], section 2.3.2.1). Its mandatory child elements are:

- `OrganizationName`, containing a name that "may or may not be suitable for human consumption"
- `OrganizationDisplayName`, containing a name "suitable for human consumption"

- `OrganizationURL`, containing a URL specifying "a location to which to direct a user for additional information".

Many Shibboleth federations make use of `OrganizationDisplayName` as a convenient location from which to draw a string identifying a particular identity provider. This string is used when selection from a list of identity providers is required: for example this might be done at a central discovery service, often known as a WAYF ("Where Are You From") service.

This convention is unremarkable in an environment where a one-to-one mapping exists between organisations and identity providers, so that the organisation "responsible for" the SAML entity is the same (singular) organisation for which the identity provider speaks. Because the UK federation allows both outsourcing and aggregated identity provision, different conventions are adopted.

The UK federation currently makes use of two different conventions for the information included in `Organization` elements:

- *`Organization` convention A* was used in the precursor SDSS federation.
- *`Organization` convention B* makes explicit the distinction between the responsible organisation and the function of the particular SAML entity.

It is anticipated that the metadata published by the UK federation will largely move from convention A to convention B as a result of the transition from the SDSS federation.

3.4.1 `Organization` Convention A

In convention A, all entities are provided with an `Organization` element in which the `OrganizationName` and `OrganizationDisplayName` are identical.

For an identity provider entity:

- The `OrganizationName` and `OrganizationDisplayName` both contain a string describing the identity community on behalf of which the identity provider makes assertions. In many cases, this will be the same as the organisation responsible for the SAML entity, but this will not always be the case when identity provision has been outsourced or aggregated.
- The `OrganizationURL` contains a URL leading to either more information about the organisation responsible for the entity, or more information about the identity community served by the entity.

For a service provider entity:

- The `OrganizationName` and `OrganizationDisplayName` both contain a string describing either the organisation responsible for the entity, or alternatively the service provided by the entity.
- The `OrganizationURL` contains a URL leading to either more information about the organisation responsible for the entity, or more information about the service provided by the entity.

Note that some very old entities possess an `OrganizationURL` value of "`http://www.example.com/`"; this is left over from an even older convention based on Shibboleth 1.2 metadata. Such metadata is being updated as time permits.

3.4.2 `Organization` Convention B

In convention B, all entities are provided with an `Organization` element in which the `OrganizationName` contains a string representing the UK federation's canonical name for the member organisation responsible for the entity. This will normally be the organisation's legal name, as taken for example from the organisation's constitution or from Companies House records.

In this convention, the `OrganizationDisplayName` contains a string describing the function of the particular entity, and the `OrganizationURL` contains a URL leading to more information as appropriate to the entity's function.

For an identity provider entity:

- The `OrganizationDisplayName` should contain the string by which the identity provider is to be known by discovery services.
  - In the case of identity providers representing a single member organisation, this will normally be a simplified form of the canonical name of that member organisation, selected by the federation operator to provide users of discovery services with a coherent selection.
  - In the case of an aggregated identity provider representing multiple member organisations, the `OrganizationDisplayName` will be chosen by the federation operator to represent the combined identity community.
- The `OrganizationURL` contains a URL leading to either more information about the organisation responsible for the entity, or more information about the identity community served by the entity.

For a service provider entity:

- The OrganizationDisplayName will be descriptive of the particular service provided. This may include a component representing the organisation offering the particular service.
- The OrganizationURL contains a URL leading to either more information about the organisation responsible for the entity, or more information about the service provided by the entity.

In the case where member organisation A entrusts the operation of one of its entities to a second member organisation B (or, alternatively, where A purchases services from B):

- The OrganizationName will refer to member B.
- The OrganizationDisplayName will refer to member A.
- The OrganizationURL may refer to either A or B, as appropriate in the particular case.

3.5 Future Directions

3.5.1 SDSS Federation WAYF Namespace

The use of the SDSS federation WAYF namespace will be discontinued at some point during the transition from the SDSS federation. The SDSS-defined HideFromWAYF marker element will be replaced by a new element in the UK federation label namespace.

3.5.2 Organization Conventions

The move to the scheme described here as *Organization convention B* is intended to bring the UK federation metadata into closer conformance with the original SAML 2.0 metadata specification ([SAML2Meta]). In particular, once the change has been completed metadata consumers will have a reliable indication (in the form of the OrganizationName element) of the organisation responsible for any given entity.

This conformance could be improved still further by making use of the SAML 2.0 AttributeConsumingService element to describe services. This element specifically includes both ServiceName and ServiceDescription child elements, which could be used in place of the OrganizationDisplayName element for service provider entities.

Such an alternative is unfortunately not available within [SAML2Meta] for identity provider entities. In addition, any move to a UK federation-defined alternative convention for the “WAYF display string” would need to be promulgated well in advance to avoid disruption to any existing WAYF deployments, not all of which can be assumed to be known to the federation operator.

4 References

[SAML1Meta] G. Whitehead and S. Cantor, *SAML 1.x Metadata Profile.* OASIS SSTC, March 2005. Document ID sstc-saml1x-metadata-cd-01.
See **http://www.oasis-open.org/committees/security/**

[SAML1Meta-xsd]
S. Cantor et al., *SAML 1.x Metadata Profile Schema.* OASIS SSTC, March 2005. Document ID sstc-saml1x-metadata.
See **http://www.oasis-open.org/committees/security/**

[SAML2Meta] S. Cantor et al., *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS SSTC, March 2005. Document ID sstc-saml-metadata-2.0.
See **http://www.oasis-open.org/committees/security/**

[ShibProt] S. Cantor et al. *Shibboleth Architecture: Protocols and Profiles.* Internet2-MACE, September 2005. Document ID internet2-mace-shibboleth-arch-protocols.
See **http://shibboleth.internet2.edu/shibboleth-documents.html**

[UKFTS] *UK Access Management Federation for Education and Research: Federation Technical Specifications.* Document ID ST/AAI/UKF/DOC/004; this document.
See **http://www.ukfederation.org.uk/**

[UKPROC] *UK Access Management Federation for Education and Research: Federation Operator Procedures.* Document ID ST/AAI/UKF/DOC/005.
See **http://www.ukfederation.org.uk/**

[UKROM] *UK Access Management Federation for Education and Research: Rules of Membership.* Document ID ST/AAI/UKF/DOC/001.
See **http://www.ukfederation.org.uk/**

[UKTRP] *UK Access Management Federation for Education and Research: Technical Recommendations for Participants.* Document ID ST/AAI/UKF/DOC/003. See **http://www.ukfederation.org.uk/**

Copyright:

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.