UK Access Management Federation for Education and Research

Metadata Registration Practice Statement

Ian A. Young

2 September 2013

Version 20130902

Table of Contents

1 Introduction

This document specifies the metadata registration practices used by the UK Access Management Federation for Education and Research (the UK federation) in its role as a metadata registrar. The terms “UK federation registrar” and “the registrar” in this document are to be understood to refer to the UK federation operator or its agents acting in this role.

This document includes documentation of some of the UK federation's conventions with respect to the elements of metadata included in its published metadata aggregates. Fuller coverage of this topic can be found in [UKFTS].

1.1 Document Status

This edition describes the metadata registration practices of the UK federation with effect from its date of publication as shown on the cover page.

1.2 Notation

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

Conventional XML namespace prefixes are used throughout this document to stand for their respective namespaces as follows:

Prefix	XML Namespace	Defined in
`md:`	`urn:oasis:names:tc:SAML:2.0:metadata`	[SAML2Meta]
`mdrpi:`	`urn:oasis:names:tc:SAML:metadata:rpi`	[SAML-Metadata-RPI-V1.0]
`mdui:`	`urn:oasis:names:tc:SAML:metadata:ui`	[SAML-Metadata-UI-V1.0]
`shibmd:`	`urn:mace:shibboleth:metadata:1.0`	[ShibMetaExt]

This document uses the following typographical conventions in text:

- `<prefix:XMLElement>` to signify an XML element. If the prefix is omitted, “`md:`” can be assumed.
- `XMLAttribute` to signify an XML attribute. Attributes accompanied by values are written as `XMLAttribute="value"`.

1.3 Changes in this Edition

This is a new document.

1.4 Future Directions

Where appropriate, major sections of this document contain a sub-section called “Future Directions” describing likely future developments in the area under consideration. These notes are provided to allow readers to incorporate this information into planning activities.

2 Versioning and Applicability

This document describes the metadata registration practices of the UK federation with effect from its date of publication as shown on the cover page. All new entity registrations performed on or after that date SHALL be processed as described here until this document is superseded by a later edition.

Registration practices change over time; editions of this document are distinguished by their dates of publication and by a compact URL derived from that date. The compact URL for an MDRPS published on a particular date SHALL be:

`http://ukfederation.org.uk/doc/mdrps-`*YYYYMMDD*

Where:

- YYYY represents the document's year of publication,
- MM represents the document's month of publication, from “`01`” to “`12`”,
- DD represents the document's day of publication, from “`01`” to “`31`”.

The MDRPS currently in effect for new registrations, as well as archived copies of earlier MDRPS documents still relevant for older entities, SHALL be published on the UK federation web site at the following URL:

http://ukfederation.org.uk/mdrps

Metadata for all entities registered by the UK federation registrar SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate:

- The fact that the UK federation registrar was the registrar for the entity, and
- The particular MDRPS which applies to the entity, if any.

For example, the following metadata fragment represents an entity registered by the UK federation registrar under the practices documented in the (fictional) MDRPS of 1st January 2006:

```
<EntityDescriptor entityID="https://example.org/entity">
  <Extensions>
    <mdrpi:RegistrationInfo
      registrationAuthority="http://ukfederation.org.uk"
      registrationInstant="2006-03-09T10:06:35Z"/>
      <mdrpi:RegistrationPolicy
        xml:lang="en">http://ukfederation.org.uk/doc/mdrps-20060101</mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
    <Extensions>
    ...
```

An entity whose `<mdrpi:RegistrationInfo>` does not include reference to a specific MDRPS by including an `<mdrpi:RegistrationPolicy>` element MUST be assumed to have been registered under a historic, undeclared registration practice regime. This can be assumed to have been broadly similar to a more recent documented MDRPS, and such an assumption may be adequate for many relying parties.

If a metadata relying party requires assurance of an entity's compliance with a documented MDRPS, a request MAY be made via the UK federation helpdesk for the registrar to perform an MDRPS re-evaluation for the entity. Such a re-evaluation MAY be performed for a registered entity at the registrar's discretion under the following circumstances:

- At the request of a relying party,
- When an entity's metadata is changed by the entity's registrant,
- When a new MDRPS edition is published.

The expected result of an MDRPS re-evaluation is to verify the entity's registration against the then-current MDRPS, with the metadata published for the entity being updated to reflect this.

Requests to re-evaluate an entity in terms of a previous MDRPS SHALL NOT be accepted.

3 Eligibility and Ownership

Members of the UK federation are eligible to make use of the UK federation registrar to register entities. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a UK federation member is documented here:

http://www.ukfederation.org.uk/content/Documents/JoinFederation

The membership process verifies that the prospective member has legal capacity, and requires that all members enter into a contractual relationship with the UK federation operator by agreeing to the *Rules of Membership.* [UKROM]

The process also establishes a canonical name for the federation member. The canonical name of a member MAY change during the membership period, for example as a result of corporate name changes or mergers.

A federation member is regarded as the *owner* of all entities registered by the member, and is held responsible for the actions of the entity.

Entities registered by a federation member are distinguished in metadata by the inclusion of a `<ukfedlabel:UKFederationMember/>` label in the `<Extensions>` element of the entity's `<EntityDescriptor>`. The member's canonical name is disclosed in the entity's `<OrganizationName>` element. See [UKFTS] for additional details on conventions used in published metadata.

3.1 Future Directions

The UK federation has in the past registered certain entities based on specific partner agreements rather than the standard membership agreement. Such entities are represented in metadata:

- Without a `<ukfedlabel:UKFederationMember/>` label,
- With a `<mdrpi:RegistrationInfo>` element, but
- Without a `<mdrpi:RegistrationPolicy>` element.

We anticipate that registration of all such entities will ultimately pass back to their natural “home” registrar, and the metadata for them will be provided to UK federation members through inter-federation metadata exchange.

Until this transition has been completed, requests for MDRPS re-evaluations for these entities SHALL be rejected.

4 Use of Domain Names

In order to provide a basis for technical trust in an entity, the UK federation registrar verifies the registrant's right to use particular domain names in the following contexts:

- An `<EntityDescriptor>`'s `entityID` attribute,
- For identity provider entities, any `<shibmd:Scope>` elements.

Registrations for which this right to use can not be established by the registrar SHALL be rejected.

In both contexts, this right to use a domain name MAY be established in one of the following ways:

- A registrant is regarded as owning, and therefore having a right to use, any domain registered by the member. This determination extends to any sub-domain of the registered domain.
- A registrant MAY be granted the right to make use of a specific domain name through a permission letter from the domain's owner, either:
  - For a specific domain name, for use in a specified entity only. Such permission SHALL NOT be regarded as including permission for the use of sub-domains, or use in other than the specified entity.
  - Exceptionally, for a given domain name and its sub-domains, for use in any entity. Such a generic grant SHALL only be accepted in the case of closely-related legal entities.

Domain permission grant letters MAY be accepted both from federation members and from non-members. The acceptability of a permission grant is dependent on context, as described in the sections below.

4.1 Domain Names in `entityID` Atttributes

Values of the `entityID` attribute for entities registered with the UK federation MUST be an absolute URI using either the `http`, `https` or `urn` schemes. `https`-scheme URIs are RECOMMENDED.

`http`-scheme and `https`-scheme URIs used for `entityID` values MUST contain a host part whose value is a DNS domain. The registrant MUST demonstrate that the domain used is either owned by them, or that specific permission has been given to them to use the domain for the purpose of registering the entity (see above).

The use of `urn`-scheme URIs for `entityID` values is NOT RECOMMENDED but MAY be permitted in exceptional circumstances. When permitted, such values MUST be part of a properly delegated registry under the `urn:mace` namespace, as described in [RFC3613]. The registrant MUST also demonstrate that the `urn:mace` URI value in question has been issued for their use.

When establishing the right of a registrant to use a domain name in an `entityID` attribute, the registrar may rely on either:

- A permission letter from an existing UK federation member, or

- A permission grant letter from a non-member after suitable validation of the non-member's identity.

4.2 Domain Names in `<shibmd:Scope>` Elements

The UK federation's convention is that scopes are named by DNS domain names, expressed in lower case. Entity owners registering metadata containing `<shibmd:Scope>` elements MUST demonstrate that each domain used is either owned by them, or that specific permission has been given to them to use the domain for the purpose of registering the entity.

When establishing the right of a registrant to use a domain name in a `<shibmd:Scope>` element, the registrar MAY rely on a permission letter from an existing UK federation member. Permission letters from non-members SHALL NOT be accepted for this purpose.

As well as the ownership and permission grant mechanisms described above, two additional mechanisms are available in support of the UK Schools sector.

UK local authorities which are members of the UK federation SHALL be presumed by the registrar to have permission to use any domain under the third-level `.sch.uk` domain for their area.[1] For example, Aberdeen City Council SHALL be presumed to have permission to use any domain under `aberdeen.sch.uk`. This presumption SHALL be set aside if challenged by the individual registrant of such a domain.

English local authorities which are members of the UK federation, or any Regional Broadband Consortium which is a member of the UK federation and of which the local authority is part, SHALL be implicitly allocated permission by the federation registrar to have permission to use a *synthetic domain* of the following form, along with all corresponding sub-domains:

> *code*`.eng.ukfederation.org.uk`

In this construction, *code* shall be the three-digit numeric LA code assigned to the local education authority.[2] For example, Dorset's code is 835.

[1] See **http://www.nominet.org.uk/uk-domain-names/registering-uk-domain/choosing-domain-name/schools**

[2] See **http://www.education.gov.uk/edubase/search.xhtml**

5 References

[RFC 2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels,* March 1997. See **http://www.ietf.org/rfc/rfc2119.txt**

[RFC3613] R. Morgan et al, *Definition of a Uniform Resource Name (URN) Namespace for the Middleware Architecture Committee for Education (MACE),* October 2003. Available as **http://tools.ietf.org/html/rfc3613**

[SAML-Metadata-RPI-V1.0] *SAML V2.0 Metadata Extensions for Registration and Publication Information Version 1.0.* 03 April 2012. OASIS Committee Specification 01. **http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html**

[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/**

[ShibMetaExt] *SAML 2.0 Metadata Extensions for Shibboleth, V1.0* See **https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0**

[SP800-57part1] NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revision 3),* July 2012. See **http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf**

[SP800-131A] NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths,* January 2011. See **http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf**

[UKFTS] *UK Access Management Federation for Education and Research: Federation Technical Specifications.* This document. See **http://ukfederation.org.uk/doc/federation-technical-specifications**

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

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

[UKTRP] *UK Access Management Federation for Education and Research: Technical Recommendations for Participants* See **http://ukfederation.org.uk/doc/technical-recommendations-for-participants**