

**LOGO**

**\* enter Federation Name \***

Federation Operator Practice: Metadata Registration Practice Statement

|                  |  |
|------------------|--|
| Authors          |  |
| Publication Date |  |
| Version          |  |

#### License



This template document is licensed under Creative Commons CC BY 3.0. You are free to share, re-use and adapt this template as long as attribution is given. This document draws on work carried out by the UK Access Management Federation and the AConet Identity Federation with gratitude.

## Table of Contents

|   |    |
|---|----|
| 1. Definitions and Terminology .....      | 3  |
| 2. Introduction and Applicability.....    | 4  |
| 3. Member Eligibility and Ownership ..... | 5  |
| 4. Metadata Format.....                   | 6  |
| 5. Entity Eligibility and Validation..... | 7  |
| 6. Entity Management .....                | 9  |
| 7. References .....                       | 10 |

## 1. Definitions and Terminology

*In this section, basic terms that are used in the document are defined. If a specific notation system is used (such as RFC2119), this should also be referenced.*

*Readers will be looking to ensure that they have an accurate understanding of any terminology used in the document.*

### Example Wording:

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 [RFC2119].

The following definitions are used in this document:

|                            |  |
|----------------------------|--|
| Federation                 | Identity Federation. An association of organisations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions. |
| Federation Member          | An organisation that has joined the Federation by agreeing to be bound by the Federation Policy in writing.  |
| Federation Operator        | Organisation providing the infrastructure for Authentication and Authorisation to Federation Members.  |
| Federation Policy          | A document describing the obligations, rights and expectations of the federation members and the federation Operator.  |
| Entity                     | A discrete component that a member wishes to register and describe in metadata. This is typically an Identity Provider or Service Provider.  |
| Registry                   | System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual processes.   |
| Registered Representatives | Individuals authorised to act on behalf of the member. These may take on different roles with different rights attached to them.   |

## 2. Introduction and Applicability

*The introduction should briefly introduce the Metadata Registration Practice Statement and describe the document publication process. It is important to remember that you may wish to change and update your Metadata Registration Practice Statement over time. If these changes are significant, it will mean that you will be publishing metadata that has been processed against different practice statements and as such it is important that is represented both in the documentation and in the metadata (see section 5). Previous editions of the MRPS should continue to be published to support referencing of these changes.*

*If you provide the document in multiple languages this should be referenced here, indicating which version is normative.*

*Readers will be looking to understand where you publish documentation, how you reflect changes and how this relates to published metadata.*

### **Example Wording:**

This document describes the metadata registration practices of the Federation Operator with effect from the publication date shown on the cover sheet. All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.

This document SHALL be published on the Federation website at: *<url>*. Updates to the documentation SHALL be accurately reflected in entity metadata.

An entity that does not include a reference to a registration policy MUST be assumed to have been registered under an historic, undocumented registration practice regime. Requests to re-evaluate a given entity against a current MRPS MAY be made to the Federation helpdesk.

### 3. Member Eligibility and Ownership

*This section should describe the process by which the Federation establishes member eligibility. HOW members join is probably already documented in the Federation Policy, and this can be referenced here. The MRPS should provide more detail about WHAT the Federation does to manage and restrict membership.*

*Readers will be looking to understand how organisations become members of your Federation, how you carry out any specific checks on these organisations and whether you permit any exceptions to these processes, such as outsourcing arrangements.*

#### **Example Wording:**

Members of the Federation are eligible to make use of the Federation Operator's registry to register entities. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a member of the Federation is documented at: <url>.

The membership procedure verifies that the prospective member has legal capacity, and requires that all members enter into a contractual relationship with the Federation Operator by agreeing to the Federation policy. The Operator makes checks based on the legal name provided. The checks are conducted with a number of official databases (provide examples).

The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organisation in dealings with the Federation Operator. Verification is achieved by (describe process).

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. The member's canonical name is disclosed in the entity's SAML v2.0 <md:OrganizationName> element [SAML-Metadata-OS].

#### 4. Metadata Format

*This section should refer to the way in which registration information is referenced in the entity metadata. For the purposes of this document, use of the SAML V2.0 Metadata Extensions for Registration and Publication Information is assumed [SAML-Metadata-RPI-v1.0]*

##### **Example Wording:**

Metadata for all entities registered by the Federation Operator SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate that the Federation Operator is the registrar for the entity and to detail the version of the MRPS statement that applies to the entity. The following is a non-normative example:

```
<mdrpi:RegistrationInfo
registrationAuthority="http://Federation.org"
registrationInstant="2016-11-29T13:39:41Z">
<mdrpi:RegistrationPolicy xml:lang="en">
http://Federation.org/doc/MRPS20121110</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

## 5. Entity Eligibility and Validation

*This section describes the processes and checks put in place before an entity is registered. Readers will be looking to understand how you determine a member's right to publish information about a given entity and any checks you make to ensure the entity metadata is well constructed.*

*Text regarding entityIDs using URIs is included below. Some Federations will also permit URN-based entityIDs. You should describe what you do and do not permit under each schema. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.*

### Example Wording:

#### 5.1 Entity Registration

The process by which a Federation member can register an entity is described at <url>.

The Federation Operator SHALL verify the member's right to use particular domain names in relation to entityID attributes and, for Identity Provider entities, any scope elements.

The right to use a domain name SHALL be established in one of the following ways:

- A member's canonical name matches registrant information shown in WHOIS.
- A member MAY be granted the right to make use of a specific domain name through a permission letter from the domain owner on a per-entity basis. Permission SHALL NOT be regarded as including permission for the use of sub-domains.

#### 5.2 EntityID Format

Values of the entityID attribute registered MUST be an absolute URI using the http, https or urn schemes.

https-scheme URIs are RECOMMENDED to all members.

http-scheme and https-scheme URIs used for entityID values MUST contain a host part whose value is a DNS domain.

#### 5.3 Scope Format

For Identity Provider entities, scopes MUST be rooted in the DNS domain namespace, expressed in lowercase. Multiple scopes are allowed.

Regular expressions representing multiple scopes MAY be used, but all DNS domains covered by the expression SHALL be included in checks by the Federation Operator for the member's right to use those domains. For these checks to be achievable by the Federation Operator, the set of DNS domains covered by the regular expression MUST end with a domain under a public suffix – that is, a literal '.', followed by at least two DNS labels separated by literal '.' (representing a domain to be validated as "owned" by the entity owner), and ending with a '\$' anchor (e.g. (foo | bar)\.example\.com\$).

#### 5.4 Entity Validation

On entity registration, the Federation Operator SHALL carry out entity validations checks. These checks include:

- Ensuring all required information is present in the metadata;

- Ensuring metadata is correctly formatted;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates.



## 6. Entity Management

*This section describes the processes undertaken once an entity has been registered – including processes for change requests, removal and any intervention the Federation Operator may take. If you have a Monitoring Practice Statement, this is likely to be referenced here. The reader will want to understand that any changes made to an entity are completed with the correct permission and for good reasons. Please ensure that any processes described here reflect your current practice and any published documentation currently available for your Federation.*

*If you have multiple different roles under the Registered Representative category (e.g. management contacts, technical contacts, administrative contacts) the different rights of these roles can be detailed here.*

### Example Wording:

Once a member has joined the Federation any number of entities MAY be added, modified or removed by the organisation.

#### 6.1 Entity Change Requests

Any request for entity addition, change or removal from Federation members needs to be communicated from or confirmed by their respective Registered Representatives.

Communication of change happens via (*e-mail, Federation registry tool etc.*)

#### 6.2 Unsolicited Entity Changes

The Federation Operator may amend or modify the Federation metadata at any time in order to:

- Ensure the security and integrity of the metadata;
- Comply with interFederation agreements;
- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

## 7. References

*Remember to include references to documentation within your own Federation, such as your Identity Federation Policy.*

|                          |  |
|--------------------------|--|
| [RFC2119]                | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, <a href="#">RFC 2119</a> , March 1997.  |
| [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. <a href="http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html">http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html</a> . |
| [SAML-Metadata-OS]       | OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a> .   |