LOGO

*** enter Federation Name ***

Federation Operator Practice: Metadata Registration Practice Statement

Publication Date	
Version History	

Acknowledgements
This document is based on the REFEDS Metadata Registration Practice Statement template version 2.0.

License

Table of Contents

1. Definitions and Terminology

Review and remove this box of text before publishing your MRPS.

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	Also known as 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.
EntityID	A machine-readable persistent identifier for a specific Entity. For the purposes of this document, it is assumed that such identifiers must be globally unique.
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

Review and remove this box of text before publishing your MRPS.

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 it 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 what version is normative.

Readers will be looking to understand where you publish documents, 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 a 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

Review and remove this box of text before publishing your MRPS.

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 <md:OrganizationName> element [SAML-Metadata].

4. Metadata Format

<u>Review and remove this box of text before publishing your MRPS.</u>

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.

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.example.org"
      registrationInstant="2023-10-20T13:39:41Z">
      <mdrpi:RegistrationPolicy xml:lang="en">
      http://federation.example.org/doc/mrps-20121110
      </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Entity Eligibility and Validation

Review and remove this box of text before publishing your MRPS.

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. While they tend to be discouraged, some Federations still permit URN-based entityIDs and may need to include additional wording to cover these cases. You should describe what you do and do not permit under each scheme. 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>.

5.2 EntityID Format

Values of the entityID attribute registered MUST be an absolute URI using the HTTP or HTTPS 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.

The right to use a URI in an entityID SHOULD be established in one of the following ways:

- A Member demonstrates the right to use the host part of a URL by means of domain validation (see 5.5 Domain Validation).
- In the case of multi-tenanted providers, such as software-as-a-service or cloud-hosted solutions, ALL of the following apply:
    1. The format of an entityID is well-known and contains a unique identifier for each specific tenant. Such an identifier could be contained within the path or query subcomponents of a URL, or as a unique subdomain of the domain name identified in the host subcomponent;
    2. There is reasonable certainty that the unique identifier for a tenant is both persistent and is not reassigned; and
    3. The tenant's unique identifier can be directly associated with the Federation Member in one of the following ways:
        - The solution provider has a lookup or API service that returns either the canonical name of the Member or a domain name the Member has the right to use; or
        - A Registered Representative of the Member attests to the Member's right to use the entityID; and can demonstrate operational control of the tenant by means of login to a well-known protected resource that displays both the tenant's unique identifier from the entityID, as well as the canonical name of the Member or a domain name the Member has the right to use.

5.3 Scope Format

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

The right to use a particular scope SHALL be established by means of domain validation (see 5.5 Domain Validation).

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 regular expression consisting of a literal '.', followed by at least two DNS labels separated by literal '.'s (representing a domain to be validated per 5.5), and ending with a '$' anchor (e.g., `(foo|bar)\.example\.com$` for two subdomains under example.com).

5.4 Entity Validation

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

- Ensuring all required information is present in the metadata;
- Ensuring metadata is correctly formatted;
- Ensuring protocol endpoints are protected with TLS / SSL certificates. Where a private certificate authority is used, the Federation Operator MAY ask the Registered Representative to confirm that the trust anchor is reasonably likely to be embedded into the browsers of all users of the Entity.

5.5 Domain Validation

Where domain validation is required by this document, the Federation Operator SHALL establish a Member’s right to use a domain name in one of the following ways:

- A Member’s canonical name matches the registrant information shown in public WHOIS records held by the corresponding DNS registrar;
- A DNS registrar confirms the Member’s eligibility from privately-held information; or
- A Registered Representative of the Member attests to the Member’s right to use the domain name; and can demonstrate operational control of the domain name by completing Domain Control Validation [DCV] using any of the mechanisms commonly accepted by public certification authorities.
- 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.

6. Entity Management

Review and remove this box of text before publishing your MRPS.

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 any 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

Review and remove this box of text before submitting your MRPS.

The example below includes all the references from the template. 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, RFC 2119, 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. http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html.
[SAML-Metadata]	OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
[DCV]	"Validation of Domain Authorization or Control" in "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", CA/Browser Forum. https://cabforum.org/baseline-requirements-documents/.