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.

Table of Contents

1. Definitions and Terminology

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 collaboration and transactions.
Federation Member	An organisation that has joined the Federation by agreeing in writing to be bound by the Federation Policy.
Federation Operator	Organisation providing or commissioning the infrastructure for Authentication and Authorisation to the members of its Federation.
Federation Policy	A document describing the obligations, rights, and expectations of the Federation Members and the Federation Operator.
Entity	A discrete component that a Federation member wishes to register and describe in metadata. This is typically an Identity Provider or Service Provider.
EntityID	A persistent identifier used in SAML software configuration and databases to uniquely identify an Entity. A machine-readable persistent identifier for a specific Entity. An entityID must be unique across all registered entities in an extended ecosystem (such as a Federation). For the purposes of this document, it is assumed that such identifiers must be globally unique.
Registered Representatives	Individuals authorised to act on behalf of the Federation Member. Registered Representatives may take on different roles with different rights attached to each role.

2. Introduction and Applicability

This document and prior versions shall be published on the Federation website at: [CHANGEME - <url>].

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

The procedure and eligibility criteria for becoming a member of the Federation are documented at: [CHANGEME - <url>].

The member's official name is disclosed in the entity's <md:OrganizationName> element [SAML-Metadata]. The official name of a member may change during the membership period, for example as a result of corporate name changes or mergers.

4. Metadata Format

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.

5. Entity Eligibility and Validation

5.1 Entity Registration

The process by which a Federation Member can register an entity is described at [CHANGEME - <url>].

5.2 EntityID Format

Values of the registered entityID attribute 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 software-as-a-service or cloud-hosted solutions that do not support adding entityIDs, all of the following apply:
    1. The format of an entityID is well-known and contains a unique identifier for each specific instance. 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 an instance is both persistent and is not reassigned; and
    3. The instance'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 official 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 instance by means of login to a well-known protected resource that displays both the instance's unique identifier from the entityID, as well as the official 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 on end-user-facing endpoints, 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.
- Ensuring all validation rules specified in 5.2 and 5.3 where applicable.

5.5 Domain Validation

Where domain validation is required by this document, the Federation Operator will establish a Member's right to use a domain name in the following way(s)

[CHANGEME - Describe, removing what you will not use and adding any mechanisms your federation uses not otherwise listed]

- A Member's official 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;
- 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

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 the addition, change, or removal of an Entity by a Federation Member must be communicated from or confirmed by their respective Registered Representative.

Communication of change happens via [CHANGEME - *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 (as defined in the eduGAIN Constitution) agreements;
- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

7. References

[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/.

Guidance per section

Everything that follows is notes and guidance to help you customise the MRPS template. It should not be included in your final document. Instead, you should read through the notes below section by section, updating the example text in the template as you go. You should ensure that the final version accurately describes your own federation's practices.

You should ensure that you find everything that says "[CHANGE ME -]" with instructions and update it.

Once you've customised the template, remove this entire guidance section before publication.

1. Definitions and Terminology

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

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

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 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 these changes.

This section should briefly introduce the Metadata Registration Practice Statement (MRPS) 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 changes are significant, you will publish metadata that has been processed against

different practice statements. It is important that both the MRPS documentation and the metadata reflect the changes (see section 5). Federation Operators should publish previous MRPS versions to support change tracking.

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.

3. Member Eligibility

This section should describe the process by which the Federation determines 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.

The membership procedure ensures that the members are aware of and is appropriately bound to Federation Policy. The Federation Operator makes checks based on the official name provided. The checks are conducted with a number of official sources including (list examples here).

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.

If you have different procedures for SPs and IdPs in joining your federation, and that information is on separate web pages, include both <urls> in the text.

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.

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

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 permit URN-based entityIDs for historical or operational reasons. While generally discouraged, you will need additional wording if your Federation supports this entityID format. 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.

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 roles under the Registered Representative category (e.g., management contacts, technical contacts, administrative contacts), detail the responsibilities of each role here.

7. References

The included references contain all the references from the template; the references you use may be different. Remember to include references to documentation within your own Federation, such as your Federation Policy.