eduIDM Federation for
Education and Research

Metadata Registration Practice Statement (MRPS)

Version: 1.0
Authors: S. El Haddouti, H. Bouhaddou, R. Merrouch
Organization: CNRST
Contact: team@eduidm.ma

Version 1.0
(14-05-2018)

Table of Contents

Acknowledgements:

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

1. Definitions and Terminology

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 [RFC2119].

Federation: eduIDM federation is an association of organizations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transaction.

eduIDM Operator: eduIDM federation is managed and operated by MARWAN, the Moroccan National Research and Education Network.

eduIDM Member: an institution that has joined eduIDM Federation by agreeing to be bound by the eduIDM Federation Policy and by signing the eduIDM Federation Member Request.

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 (IdP) or a Service Provider (SP).

Federation Registry: a system to register metadata of entities. This system is run by the operator of eduIDM Federation – MARWAN.

Registered Representatives: individuals authorized to act on behalf of the member. These may take on different roles with different rights attached to them.

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]

2. Introduction and applicability

This document specifies the metadata registration practices used by the eduIDM Identity Federation for education and research (Moroccan Federation) in its role as a metadata operator. All new entity registrations performed on or after the date of this document SHALL be processed as described here until the document is superseded. This document SHALL be published on the federation website at: http://www.eduidm.ma/mrps-eduidm.pdf-v1.0. Updates to the documentation SHALL be accurately reflected in the federation 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 eduIDM helpdesk via team@eduidm.ma.

3. Common practices

Each registered representative can connect to the federation registry web interface (https://rr.eduidm.ma/rr3) and authenticate first through his local IdP or with a local account. Account requests MAY be made to the federation helpdesk via team@eduidm.ma. Data provided by an IdP or SP administrator, once validated, are stored in the federation registry database and allows to generate both the federation metadata and the inter-federation metadata.

An IdP/SP needs to be attached to a trusted organization which designates two contacts. These contacts can later register an IdP and SPs with the eduIDM federation. A confirmation is needed.

The administrators and technical contacts can manage (modify, add, remove...) the information of their entities. The update request will require validation by the eduIDM federation administrators. The administrators of the SAML entity will be notified when changes have been validated and published in the metadata of the eduidm federation.

4. Member Eligibility and Ownership

Members of the eduIDM 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 an eduIDM federation member is documented here: https://www.eduidm.ma/adhesion/

The membership process verifies that the prospective member has legal capacity, and requires that all members enter into a contractual relationship with the eduIDM federation operator by agreeing to the federation policy.

The eduIDM operator makes checks based on the legal name provided. The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealings with the federation operator. Verification is achieved by 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 **<OrganizationName>** element.

5. Metadata Format

Metadata for all entities registered by the eduIDM 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 that applies to the entity.

The RegistrationInfo Element:

```
<Exentions>
  <mdrpi:RegistrationInfo
    registrationAuthority="https://www.eduidm.ma/"
    registrationInstant="2018-02-25T15:25:07Z">
  <mdrpi:RegistrationPolicy xml:lang="en">
     http://www.eduidm.ma/eduidm-mrps.pdf-v1.0
  </mdrpi:RegistrationPolicy>

   </mdrpi:RegistrationInfo>

 </Exentions>
```

6. Entity Eligibility and Validation

6.1. Entity Registration

The process by which a federation member can register an entity is described at*:* https://rr.eduidm.ma/rr3**.**

The eduIDM federation operator SHALL verify the member's right to use particular domain names in relation to **entityID** attributes and **scoping** 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 DNS.
- 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.

6.2. 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.

6.3. Entity Validation

During the entity registration, the federation operator SHALL carry out entity validations checks. These checks MAY include:

- ensuring that all required information is present in the metadata;
- ensuring that metadata is correctly formatted;
- ensuring that URLs specified in the metadata are technically reachable;
- ensuring that protocol endpoints are properly protected with TLS / SSL certificates.

7. Entity Management

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

7.1. 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 (team@eduidm.ma)

7.2. 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 inter federation agreements;
- improve the interoperability;
- add value to the metadata.

Changes will be communicated to Registered Representatives for the entity via email.

8. References

- **[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-OS]** 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.