



LEAF

(Moldovan Research and Education Identity Federation)

Federation Operator Practice: Metadata Registration Practice Statement

Authors	V. Pocotilenco, P. Bogatencov, C. Scifos, A. Cacean, A. Rusu
Last Modified	21.04.2015
Version	1.1



This template document is license under Creative Commons CC BY 3.0.

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

2. Introduction and Applicability

This document describes the metadata registration practices of the LEAF 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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: <http://federations.renam.md>. 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 addressed to the Federation Operator.

3. Member Eligibility

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

The procedure for becoming a member of the Federation is documented at: <http://federations.renam.md/index.php?menu=join>

The membership process verifies that the prospective member has legal capacity, is eligible to become Federation Member in accordance with the Federation policy (<http://federations.renam.md/index.php?menu=docs>), and requires that all the members enter into a contractual relationship with the Federation Operator by agreeing with the Federation policy.

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.

4. Entity Validation

The process by which a Federation member can register an entity is described at <http://federations.renam.md/index.php?menu=docs>

4.1 Entity ID Format

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

4.2 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 URLs specified in the metadata are technically reachable;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates.

5. Entity Management

Once a member has joined the Federation any number of entities MAY be added by the organization.

5.1 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 message signed by personal certificate.

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.

6. 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 .
Federation Policy	Version 1.0 http://federations.renam.md/index.php?menu=docs
Metadata Registry	http://federations.renam.md/index.php?menu=info