Agenţia de Administrare a Reţelei Naţionale de Informatică
pentru Educaţie şi Cercetare - RoEduNet
Str. Mendeleev 21-25, Sector 1, 010362
Bucureşti – România
www.nren.ro
Tel./Fax: +40-21-3171174

RoEduNetID

Federation Operator Practice:
Metadata Registration Practice Statement (MRPS)

Authors	RoEduNet
Last Modified	13mar2019
Version	0.7

Table of Contents

1 Definitions and Terminology

This section defines several basic terms used further in this document.
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].

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 RoEduNetID Federation by agreeing to be bound by the RoEduNetID Federation Policy in writing.
Federation Operator	Organisation providing the infrastructure for Authentication and Authorisation to Federation Members. . Agency ARNIEC – RoEduNet (AARNIEC) is the RoEduNetID federation operator.
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 authorised to act on behalf of the member. These may take on different roles with different rights attached to them.
RoEduNetID	The name of Romanian Education Network Identity Federation

2 Introduction and Applicability

This document describes the metadata registration practices of the RoEduNetID 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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 RoEduNetID Federation website at https://eduid.roedu.net/. 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 undocumented registration practice during a previous period. Requests to re-evaluate a given entity against a current MRPS MAY be made to the RoEduNetID Federation contact.

3 Member Eligibility and Ownership

Subscribers of the RoEduNetID 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 RoEduNetID Federation is documented at https://eduid.roedu.net/.
The membership subscription process verifies that the applicant has legal capacity, and requires that all members enter into a contractual relationship with the Federation Operator by agreeing to the RoEduNetID Federation Policy. The Federation Operator makes checks based on the legal name provided by the applicant. The checks are conducted with a number of official databases. Examples include:

- ABN Lookup
- Tertiary Education Quality and Standards Agency

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 personal contact between the Federation Operator and the organization, exceptionally via email (PGP signed) or phone.

The process also establishes a canonical name for the RoEduNetID 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.

4 Metadata for Technology Profile SAML 2.0

SAML 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:

```
<mrdpi:RegistrationInfo
    registrationAuthority="https://eduid.roedu.net"
    registrationInstant="2019-03-09T18:39:41Z">
    <mdrpi:RegistrationPolicy xml:lang="en">
        https://eduid.roedu.net/wp-content/uploads/2019/03/RoEduNet-
Metadata_Registration-v0.5.pdf
    </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5 Entity Eligibility and Validation

5.1 Entity Registration

The Federation Operator SHALL verify the subscriber'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 subscriber's canonical name matches registrant information shown in DNS;
- A subscriber 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, which the entity has a right to use (as defined above).

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.

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 '.'s (representing a domain to be validated as "owned" by the entity owner), and ending with a '$' anchor [e.g. (admin|stud)\.institution\.ro$].

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 URLs specified in the metadata are technically reachable;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates, according to existing deployment best practices (including certificate key lengths and strong signature algorithms).

6 Entity Management

Once a member has joined the Federation, the member MAY add any number of entities.

6.1 Entity Change Request

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, preferable PGP or similar signed/encrypted. When a suitable Federation registry tool will be available, it also will be used.

6.2 Unsolicited Entity Changes

The Federation Operator may amend or modify the RoEduNetID 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.

Registered Representatives of the affected entity can observe changes by inspection of the published federation metadata. For technology profiles, which do not lead to public disclosure of metadata, the Federation Operator will inform the affected entity of the change.

7 References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[AAF-Federation-Rules]	AAF Federation Rules 28 November 2017. https://aaf.edu.au/media/2017/fedrules/AAF_Federation_Rules_Nov_28_2017.pdf
[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.