eduID.hu Metadata Registration Practice Statement

Version	**2.0**
Authors	**Péter Molnár**
Last Modified	2019-03-29

Acknowledgements

This document is based on the REFEDS Metadata Registration Practice Statement template. This document draws on work carried out by the SWITCHaai Federation with gratitude.

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:

Definition	Description
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.
eduID.hu Participant	An eduID.hu participating organisation (a legal entity, Member or Partner as described in Federation Policy) is called an eduID.hu Participant and is legally bound to the Federation Policy.
Federation Operator	Organisation providing the infrastructure for Authentication and Authorisation to Federation Participants.
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.
eduID.hu Resource Registry	The self-service system provided by the Federation Operator where eduID.hu Participants can register their Entities and which generates the appropriate metadata.
Registered Representatives	Individuals authorised to act on behalf of the member. These may take on different roles with different rights attached to them.
Resource	Each eduID.hu Participant eligible to operate an IdP appoints its Resource

Definition	Description
Registration Authority Administrator (RRA Admin)	Registration Authority Administrators who take the responsibility to administer entities associated to the eduID.hu Participant.

2. Introduction and Applicability

This document describes the metadata registration practices of KIFÜ as 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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: `https://metadata.eduid.hu/eduid.hu-mrps-v2.0.pdf`. 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 made to the Federation helpdesk.

3. Member Eligibility and Ownership

Members of the Federation are eligible to make use of the Federation Operator's registry to register entities.

The procedure for becoming a member of the Federation is documented at: `https://eduid.hu/en/` .

KIFÜ participants may register SAML entities in any role and join the Federation by signing a supplemental agreement.

Organizations which are not regular KIFÜ participants and provide services for Federation users may register SAML entities in the Service Provider role and join Federation as a Partner by signing the eduID Partner Service Agreement.

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 like:

- Collections of national law (for public institutions)
- National Company Index

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 direct contact, or confirmation of prior relationship with the organisation, or consulting the organisation's on-line staff directory.

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 SAML v2.0 `<md:OrganizationName>` element.

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. The following is a non-normative example:

```
<mdrpi:RegistrationInfo
    registrationAuthority="http://eduid.hu"
    registrationInstant="2016-11-29T13:39:41Z">
    <mdrpi:RegistrationPolicy xml:lang="en">
        https://metadata.eduid.hu/eduid.hu-mrps-v2.0.pdf
    </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

5. Entity Eligibility and Validation

The eduID.hu Federation is built on a delegation model to manage the entities. Each eduID.hu Participant eligible to operate an Identity Provider appoints its Resource Registration Authority Administrators (RRA Admin) who take the responsibility to administer entities associated to the eduID.hu Participant.

KIFÜ as Federation Operator takes the responsibility for the registration of all IdPs, its own SPs as well as further SPs, e.g. the ones of Federation Partners that offer services to the whole community and not only to a single eduID.hu Participant.

5.1 Entity Registration

An eduID.hu Member has to register its entities in the eduID.hu Resource Registry: `https://rr.eduid.hu` .

The Federation Operator SHALL verify the member'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 member's canonical name matches registrant information shown in WHOIS.
- 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.

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.

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 '$' anchor (e.g. `(foo|bar)\.example\.com$`).

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 protocol endpoints are properly protected with TLS / SSL certificates.

The federation manager web application, the eduID.hu Resource Registry, generates the metadata for all the entities based on the data registered and approved. Therefore, it is always in a well-defined and consistent representation.

6. Entity Management

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

A Registered Representative with the administration right for a Federation Member Organization can invite a further person to gain the same administration right for this Member Organization. Vice versa, each Registered Representative with the administration right for a Member Organization can revoke another person's administration right for this Organization.

6.1 Entity Change Requests

Any request for entity addition, change or removal from eduID.hu Members needs to be performed within the eduID.hu Resource Registry by their respective Registered Representatives entitled by their administration rights.

Changes on behalf of eduID.hu Federation Partners for their own entities can be requested by e-mail to the eduID.hu Helpdesk. The Federation Operator verifies and

processes such requests.

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.

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.