eduID Luxembourg

Federation Operator Practice: Metadata Registration Practice Statement

Authors	S. Winter
Publication Date	2015-07-02
Version	0.2

License

This document draws heavily on work carried by the UK Access Management Federation and ACOnet in the development of their Metadata Registration Practice Statements.

Table of Contents

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 authorised 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 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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://www.eduid.lu *(section "eduID.lu Policy").*

3. Member Eligibility and Ownership

The procedure for becoming a member of the Federation is documented at: http://www.eduid.lu *(Section "Joining eduID.lu")*.

The membership process 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 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 or phone.

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.

4. Entity Management

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

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.

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.

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.

5. 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:

```
<mdrpi:RegistrationInfo
registrationAuthority="http://eduid.lu"
registrationInstant="2016-11-29T13:39:41Z">
<mdrpi:RegistrationPolicy xml:lang="en"> http://eduid.lu/
/media/eduid-mrps-02.pdf</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

Canonical Name and <OrganizationName>

The member's canonical name is disclosed in the entity's <OrganizationName> element.

SAML 2.0 Entity Validation

The following elements of entity metadata are validated:

Permitted content and formats of <EntityID>

The Federation Operator SHALL verify the member's right to use particular domain names in relation to <entityID> attributes.

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.

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).

SAML 2.0 Metadata 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.

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.