eduID.tg

eduID.tg

Federation Operator Practice: Metadata Registration Practice Statement

Authors	Arnaud AMELINA, Laté-Ognadon LAWSON, Olalekan ALLADE
Publication Date	October 2nd, 2023
Version	1.1

License

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.
Registry	System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual processes.
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 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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://www.eduid.tg. 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. Registration requests from other sources SHALL NOT be accepted.

The procedure for becoming a member of the Federation as an Identity Provider is documented in the procedures section of the Togo Federation Identity Policy document at: https://www.eduid.tg/docs/Togo-Federation-Policy-Document-v1.1.pdf

The summary of the procedure for becoming a member of the Federation as an Identity Provider is documented at: https://www.eduid.tg/page/idp/how-to-join.html.

The summary of the procedure for becoming a member of the Federation as a Service Provider is documented at: https://www.eduid.tg/page/sp/how-to-join.html.
Non IdP members are eligible to become Service Providers subject to review of their application by the Federation Operator and Steering Committee. Service Providers handling of data must meet the "data protection profile" derived from theTogo Data Protection Regulation of 2019 by the ***Instance de Protection des Données à Caractère Personnel (IPDCP)*** see: < **https://assemblee-nationale.tg/wp-content/uploads/2021/10/donnees-perso-LOI-AN.pdf**

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 https://www.eduid.tg/docs/Togo-Federation-Policy-Document-v1.1.pdf. The Operator makes checks based on the legal name provided. The checks are conducted with a number of official databases e.g (*Ministère de l'Enseignement Supérieur et de la Recherche*).

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 reviewing the application form submission and confirming that e-mail address and telephone numbers of representatives are of the said representative by checking with the institution's central administration..

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 [SAML-Metadata-OS].

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:

5. Entity Eligibility and Validation

5.1 Entity Registration

```
<mdrpi:RegistrationInfo
registrationAuthority="https://www.eduID.tg"
registrationInstant="2023-09-28T10:05:41Z">
<mdrpi:RegistrationPolicy xml:lang="en">
https://www.eduid.tg/docs/MRPS-eduid-tg-v1.1.pdf
</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

The process by which a Federation member can register an entity is described at https://www.eduid.tg/page/idp/how-to-join.html.

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, 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.

5.3 Scope Format

For Identity Provider entities, scopes MUST be rooted in the DNS domain namespace, 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 '.' (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 vaildations checks. These checks include:

- Ensuring all required information is present in the metadata;
- Ensuring metadata is correctly formatted;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates.

6. Entity Management

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

6.1 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, Federation registry tool etc.)*

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.

7. References

Remember to include references to documentation within your own Federation, such as your Identity Federation Policy.

[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.
eduID.tg Identity Federation Policy	**https://www.eduid.tg/docs/Togo-Federation-Policy-Document-v1.1.pdf**