



## Kenyan Identity Federation for Research and Education (RAFIKI)

### Federation Operator Practice: Metadata Registration Practice Statement

Authors	Kenya Education Network (KENET)
Publication Date	24/08/2022
Version	24082022

#### License



This template document is licensed under Creative Commons CC BY 3.0. You are free to share, re-use and adapt this template as long as attribution is given.

## Table of Contents

1. Definitions and Terminology	3
2. Introduction and Applicability	4
3. Member Eligibility and Ownership	4
4. Metadata Format	5
5. Entity Eligibility and Validation	5
6. Entity Management	6
7. References	7

## 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.
Kenyan Identity Federation for Research and Education (RAFIKI)	A federation established to serve the Kenyan research and education community and operated by the Kenyan NREN - Kenya Education Network.

## 2. Introduction and Applicability

This document describes the metadata registration practices of the Kenyan Identity Federation for Research and Education (RAFIKI) with effect from the publication date indicated 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://rafiki.ke>. 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 (IdP) is documented at: [https://rafiki.ke/how\\_to\\_join\\_as\\_an\\_idp](https://rafiki.ke/how_to_join_as_an_idp)

The procedure for becoming a member of the Federation as a Service Provider (SP) is documented at: [https://rafiki.ke/how\\_to\\_join\\_as\\_a\\_sp](https://rafiki.ke/how_to_join_as_a_sp)

The member registration process verifies the legal capacity of the prospective member and requires that all members enter into a contractual relationship with the Federation Operator by agreeing to the Federation policy. The Federation Operator makes checks based on the legal name provided to confirm that the prospective member is a member of the Kenyan Research and Education community.

The membership process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the prospective member organization in dealings with the Federation Operator. Verification is achieved by writing a letter to the organization's management seeking to confirm if the nominated representative is an employee of the organization.

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 `<md:OrganizationName>` element.

## 4. Metadata Format

Metadata for all entities registered by RAFIKI SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate that RAFIKI 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="https://rafiki.ke"
registrationInstant="2022-01-01T10:00:00Z">
<mdrpi:RegistrationPolicy xml:lang="en">
https://rafiki.ke/sites/default/files/2022-01/RAFIKI_Identity_Federation_Policy.pdf
</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

## 5. Entity Eligibility and Validation

### 5.1 Entity Registration

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

The Federation Operator SHALL use the following criteria to determine a member's right to use a domain name:

- A member's canonical name matches registrant information shown in public WHOIS records held by the DNS domain registrar.
- 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 party whose value is a DNS domain.

### 5.3 Entity Validation

The Federation Operator SHALL carry out entity validations checks upon entity registration. 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 through email.

### **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

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, <a href="#">RFC 2119</a> , 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. <a href="http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html">http://docs.oasis-open.org/security/saml/Post2.0/saml-metadata-rpi/v1.0/cs01/saml-metadata-rpi-v1.0-cs01.html</a> .
[SAML-Metadata-OS]	OASIS Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf</a> .