Botswana Identity Federation Metadata Registration Practice Statement (MRPS)

Document Control

Role	Name	Title	Date	Signature
Prepared by	Bofelo McFadden	Network Systems Engineer	18 March 2025	
Approved by	Tshepo Tsheko	Managing Director	01 April 2025	

Revision Control

Version	Date	Author	Description of Changes
1.0	18 March 2025	Bofelo McFadden	Initial draft
2.0			

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].

Federation: A group of organizations that agree to interoperate using a common framework for identity and access management..

Federation Participant: An organization that participates in the federation and operates one or more entities such as Identity Providers or Service Providers.

Federation Operator: The organization responsible for managing the federation infrastructure, metadata registry, and operational processes.

Federation Policy: A document outlining the rights, responsibilities, and rules for Federation members and the operator.

Entity: A discrete component within the federation, typically an Identity Provider (IdP) or Service Provider (SP), described in federation metadata.

EntityID: A unique identifier for an entity within the federation metadata.

Registry: The system used by the Federation Operator to manage entity metadata.

Registered Representatives: An individual authorized by a Federation Participant to manage entities and interact with the Federation Operator.

Metadata A structured XML document describing federation entities, their endpoints, certificates, and other operational information.

Table of Contents

1. Introduction and Applicability

This document describes the metadata registration practices of the Botswana Identity Federation (BIF), effective from the publication date shown on the cover sheet. All new entity registrations performed on or after that date SHALL be processed according to these practices until the document is superseded.

This document SHALL be published on the BIF website: https://botsren.org.bw/index.php/botswana-identity-federation/ . Updates to the documentation SHALL be accurately reflected in the 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 the current MRPS MAY be made to the Federation helpdesk.

2. Member Eligibility and Ownership

Members of BIF are eligible to use 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 at: https://botsren.org.bw/index.php/how-to-join-as-an-idp/.

The procedure for becoming a member of the Federation as a Service Provider is documented at: https://botsren.org.bw/index.php/how-join-as-an-sp/ .

The membership procedure verifies the prospective member's legal capacity and requires all members to enter into a contractual relationship with the Federation Operator by agreeing to the Federation policy. The Operator verifies the legal name provided using official databases.

The process also identifies and verifies Registered Representatives, who are permitted to act on behalf of the organization in dealings with the Federation Operator.

The canonical name of a member MAY change during the membership period, for example, due to corporate name changes or mergers. The member's canonical name is disclosed in the entity's $< md{:}OrganizationName >$ element.

3. Metadata Format

Metadata for all entities registered by the Federation Operator SHALL use 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:

$$< md: EntityDescriptor\ xmlns: md = "urn: oasis: names: tc: SAML: 2.0: metadata" >$$

$$< md: Extensions >$$

$$< rpi: RegistrationInformation\ xmlns: rpi$$
$$= "urn: oasis: names: tc: SAML: 2.0: metadata: rpi" >$$

$$< rpi: MRPSVersion > 1.0 </rpi: MRPSVersion >$$

$$</rpi: RegistrationInformation >$$

$$</md: Extensions >$$

$$\ldots$$

$$</md: EntityDescriptor >$$

4. Entity Eligibility and Validation

4.1 Entity Registration

The process by which a Federation member can register an entity is described at: https://botsren.org.bw/index.php/botswana-identity-federation/ .

The Federation Operator SHALL verify the member's right to use 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. This information will be retrieved using the WHOIS query tool.
- A member MAY be granted the right to use a specific domain name through a permission letter from the domain owner on a per-entity basis. Permission SHALL NOT include the right to use sub-domains.

4.2 EntityID Format

The values of the entityID attribute MUST be an absolute URL using the http, https, or urn schemes. The https-scheme URLs are RECOMMENDED.

4.3 Entity Validation

Upon entity registration, the Federation Operator SHALL perform validation checks which include:

- Verifying that all required metadata elements are present.
- Ensuring metadata complies with SAML metadata schema requirements.
- Verifying that entity endpoints are accessible and properly configured.
- Ensuring that TLS/SSL certificates are valid and trusted.
- Confirming that domain ownership associated with entityID or scope is verified.

4.4 Scope Format

Identity Providers registered in the Botswana Identity Federation may assert scoped attributes.

The scope value MUST correspond to a domain name that is owned or controlled by the participating organization.

The Federation Operator SHALL verify that the organization has the right to use the domain associated with the scope.

Scopes MUST be expressed as fully qualified domain names (FQDN).

Example:
university.ac.bw
botswana.edu.bw

5. Entity Management

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

5.1. Entity Change Requests

Requests for entity addition, modification, or removal MUST be communicated by a Registered Representative of the Federation Participant.

Requests SHALL be submitted via email to the Federation Operator.

Federation Operator Contact:
Botswana Research and Education Network (BotsREN)
Email: support@botsren.org.bw
Website: https://botsren.org.bw

5.2. Unsolicited Entity Changes

The Federation Operator MAY amend federation metadata without prior request in order to:

- Protect the security or integrity of the federation
- Maintain compliance with interfederation agreements (such as eduGAIN)
- Correct technical errors in metadata
- Improve interoperability with federation participants

Where possible, affected Federation Participants SHALL be notified of such changes through their Registered Representatives.

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. 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 .

- Botswana Identity Federation Policy https://botsren.org.bw/wp-content/uploads/2025/04/Botswana-Identity-Federation-Policy.pdf