Federation Operator Practice: Metadata Registration Practice Statement(MPRS)

1 Document Control

ROLE	NAME	TITLE	DATE	SIGNATURE
Prepared by	Zanga Chimombo	Systems Manager	27 Dec 2023	
Approved by	Solomon Dindi	CEO		

2 Revision Control

VERSION	DATE	AUTHOR	DESCRIPTION OF CHANGES
1.0	27 Dec 2023	Zanga Chimombo	First draft.
2.0	12 Dec 2024	Jones Kumwenda Joyce Mtawali Grace Gausi	

3 Definitions and Terminology

The keywords "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: An association of organizations that come together to exchange information as appropriate by their users and resources to enable collaborations and transactions.

Federation Operator: Organization providing Infrastructure for Authentication and Authorization to Federation Members.

Federation Member: An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the federation framework, a Federation Member can act as a Home Organization and/or a Service Provider and/or an Attribute Authority

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 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.

Table of Contents

4 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All new entity registrations performed on or after that date SHALL be processed as described here until the document is superseded.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://mif.maren.ac.mw. 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 a historic, undocumented registration practice regime. Requests to re-evaluate a given entity against a current MRPS MAY be made to the Federation helpdesk.

5 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 is documented at: https://mif.maren.ac.mw

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 Operator makes checks based on the legal name provided. The checks are conducted with a number of official databases.

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

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 [SAML-Metadata-OS].

6 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="https://mif.maren.ac.mw"
        registrationInstant="2023-12-29T11:34:27Z">
  <mdrpi:RegistrationPolicy xml:lang="en">
    https://mif.maren.ac.mw/MAREN_Id_Fed_Policy-v1.0
  </mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

7 Entity Eligibility and Validation

7.1 Entity Registration

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 the registrant information shown in DNS. This information will be retrieved using the WHOIS query tool.
- 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.

7.2 DNS-based Scope Registration

The Federation Operator SHALL ensure that each Identity Provider (IdP) registers a DNS-based scope in its metadata.

The DNS-based scope registration SHALL adhere to the following requirements:

- The scope MUST be a domain name under the administrative control of the member organization.
- The scope SHALL be included in the IdP metadata using the shibmd:Scope element.
- The domain used for the scope MUST match the domain used in the entityID.

7.3 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.

7.4 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 metadata is correctly formatted;
- Ensuring URLs specified in the metadata are technically reachable;
- Ensuring protocol endpoints are properly protected with TLS / SSL certificates.

8 Entity Management

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

8.1 Entity Change Requests

Any request to add, modify, or remove an entity from Federation members must be communicated by, or confirmed through, their respective Registered Representatives. Change-related communication should be sent via email to systems@maren.ac.mw.

8.2 Unsolicited Entity Changes

The Federation Operator may amend or modify the Federation metadata at any time to:

- Ensure the security and integrity of the metadata;
- Comply with inter-federation agreements;
- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to the entity's registered representatives.

9 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.oasisopen.org/security/saml/Post2.0/saml-metadatarpi/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.

MIF Identity Federation Policy https://mif.maren.ac.mw.