# YAMI

# Metadata Registration Practice Statement

January 2025

## Table of Contents

# 1. Metadata Registration Practice Statement

## 1.1. Introduction and Applicability

The present Federation Operator Metadata Registration Practices shall affect all registrations of new entities or organizations made on or after the date of signature of this document.

This document SHALL be published on the Federation website at: https://www.redconare.ac.cr/yami/ . 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.

## 1.2. 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 identity is verified via live, real-time conversation.

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-Metadata-OS] <md:OrganizationName> element.

## 1.3. Metadata Format

```
<mdrpi:RegistrationInfo registrationAuthority="urn:mace:mds.redclara.net"
registrationInstant="2021-07-01T11:28:03Z"> <mdrpi:RegistrationPolicy xml:lang="en">
https://www.redclara.net/index.php/en/servicios-rc/federaciones-de-identidad
</mdrpi:RegistrationPolicy>
<mdrpi:RegistrationPolicy xml:lang="es">
https://www.redclara.net/index.php/es/servicios-rc/federaciones-de-identidad
</mdrpi:RegistrationPolicy>
</mdrpi:RegistrationInfo>
```

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.

## 1.4. Entity Eligibility and Validation

### 1.4.1. Entity Registration

The process by which a Federation member can register an entity is described at https://www.redconare.ac.cr/miembros/

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 WHOIS tool to consult the DNS registry.
- 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.

The values of the registered entityID attribute must be an absolute URL using the http, https or urn schemes. The https-scheme URIs are recommended for all members. The http-scheme and https-scheme URLs used for entityID values must contain a host part whose value is a DNS domain.

### 1.4.2. EntityID Format

The values of the registered entityID attribute must be an absolute URL using the http, https or urn schemes.
The https-scheme URIs are RECOMMENDED for all members.
The http-scheme and https-scheme URLs used for entityID values MUST contain a host part whose value is a DNS domain.

### 1.4.3. Scope Format

For Identity Provider entities, scopes MUST be rooted in the DNS domain name space, 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 '.'s (representing a domain to be validated as "owned" by the entity owner), and ending with a '$' anchor (e.g. (foo|bar)\.example\.com$).

### 1.4.4. Entity Validation

On entity registration, the Federation Operator SHALL carry out entity validations checks. These checks include:

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

### 1.5. Entity Management

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

#### 1.5.1. 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 (yami@conare.ac.cr).

#### 1.5.2. 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 inter-Federation agreements.
- Improve interoperability.
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

## 2. 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.
- [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.