Federación de Identidad para redes de Educación Latinoamericanas

Identity Federation Policy

Identity Federations for Latin American - FIEL

Table of contents

1. Definitions and Terminology

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization.
Attribute Authority	An organization responsible for managing additional Attributes for an End.
Authentication	Process of proving the identity of a previously registered End User.
Authorization	Process of granting or denying access rights to a service for an authenticated End User.
Digital Identity	A set of information that is attributable to an End User. Digital identity consists of Attributes. It is issued and managed by a Home Organization and zero or more Attribute Authorities on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. as an employee, researcher or student making use of the service of a Service Provider.
Entity	A discrete component that a member wishes to register and describe in metadata. This is typically an Identity Provider or Service Provider.
Federation	Identity federation. An association of organizations that come together to exchange information as appropriate about 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.
Home Organization	The organization with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management	Process of issuing and managing end users' digital identities.
Interfederation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
Registered Representatives	Individuals authorized to act on behalf of the member. These may take on different roles with different rights attached to them.
Registry	System used by the Federation Operator to register entity metadata. This may be via a self-service tool or via other manual processes.
Service Provider	An organization that is responsible for offering the End User the service he or she desires to use. Service Providers may rely on the authentication outcome and attributes that Home Organizations and Attribute Authorities assert for its End Users.

2. Introduction

An Identity Federation (Federation) is an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.

The FIEL Identity Federation (the Federation) is introduced to facilitate and simplify the introduction of shared services across the Federation. This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation. The Federation relies on Home Organizations and Attribute Authorities to correctly and accurately assert information about the identity of End Users to Service Providers, that may use that information to grant (or deny) access to the services and resources they offer to End Users.

The Federation Policy document defines the Federation by defining the Federation Members' obligations and rights to be able to use available Federation Technologies for electronic identification and for access to attribute and authorization information about End Users in the Federation.

This document, together with its appendices constitutes the Federation Policy. The current list of all appendices is available on the website of the Federation.

3. Governance and Roles

3.1 Governance

The governance of the Federation is delegated to RedCLARA: Latin American Cooperation of Advanced Networks.

In addition to what is stated elsewhere in the Federation Policy, RedCLARA is responsible for:

- Setting criteria for membership for the Federation.
- Determine whether to grant or deny an application for membership in the Federation.
- Determine whether a Federation Member is entitled to act as Home Organization.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Plan future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Address financing of the Federation.
- Approves the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

3.2 Obligations and rights of Federation operator

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator is responsible for:

- Secure and trustworthy operational management of the Federation and providing central services following the procedures and technical descriptions specified in this document and its appendices.
- Provides support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Acts as center of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Prepares and presents issues to RedCLARA and acts as a liaison to RedCLARA meetings.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation activities and work with other Identity Federations in the area of harmonization.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator reserves the right to:

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting secure and trustworthy operation of the Federation.
- Publish a list of Federation Members along with information about which profiles each Federation Member fulfills or implements, for the purpose of promoting the Federation.
- Publish some of the data regarding the Federation Member using specific Technology Profile. Definition of which data may be published is provided in appropriate Technology Profiles.

3.3 Obligations and rights of Federation Members:

In addition to what is stated elsewhere in the Federation Policy all Federation Members:

- Shall appoint and name an administrative contact for interactions with the Federation Operator.
- Must cooperate with the Federation Operator and other Members in resolving incidents and should report incidents to the Federation Operator in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Federation or any of its Members.
- Must comply with the obligations of the Technology Profiles which it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely. Must pay the fees.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and must follow the practice presented in Data Protection Profile.

If a Federation Member is acting as a Home Organization, it:

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them, as may be further specified in Level of Assurance Profiles.
- Should submit its Identity Management Practice Statement to the Federation Operator, who in turn makes it available to other Federation Members upon their request. The Identity Management Practice Statement is a description of the Identity Management lifecycle including a description of how individual digital identities are enrolled, maintained and removed from the identity management system. The statement must contain descriptions of administrative processes, practices and significant technologies used in the identity management life cycle, which must be able to support a secure and consistent identity management life cycle. Specific requirements may be imposed by Level of Assurance Profiles.
- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy.
- Operates a helpdesk for its End Users regarding Federation services related issues. Home Organizations are encouraged to maintain a helpdesk for user queries at least during normal office hours in the local time zone. Home Organizations must not redirect End User queries directly to the Federation Operator but must make every effort to ensure that only

relevant problems and queries are sent to the Federation Operator by appropriate Home Organization contacts.

If a Federation Member is acting as a Home Organization or Attribute Authority, it:

- Is responsible for assigning Attribute values to the End Users and managing the values in a way which ensures they are up-to-date.
- Is responsible to releasing the Attributes to Service Providers.

If a Federation Member is acting as a Service Provider, it:

- Is responsible for making decision on which End Users can access the services they operate, and which access rights are granted to an End User, it is Service Providers responsibility to implement those decisions.

4. Eligibility

The Federation sets out eligibility criteria that determines who is able to become a Federation Member and who is able to act as Home Organization.

In order to become an Identity Provider in the FIEL Identity Federation the Home Organization MUST be part of RedCLARA. The FIEL Identity Federation will only allow Home Organizations that do not have a National Research and Educational Network (NREN) in their country. If there is already a National Research and Educational Network representing the country of origin, the Home Organization MUST join the local federation.

Federation members operating Identity Providers will have end users associated with them: these are individuals with an employment, student, business, or other form of association with the federation member. Each federation member is responsible for its own users and responsible for fulfilling all the rules of the federation.

To become a member of the FIEL Identity Federation as a Service Provider only, and to receive identity information from FIEL Identity Federation Identity Providers, a Service Provider is NOT REQUIRED to become a participant of RedCLARA. These requests will be evaluated by the FIEL Identity Federation and MUST comply with RedCLARA policies (https://www.redclara.net/index.php/en/somos/redclara-la-organizacion/mision-vision-y-estatutos)

5. Procedures

5.1 How to join

In order to become a Federation Member, an organization applies for membership in the Federation by agreeing to be bound by the Federation Policy in writing by an official representative of the organization.

Each application for membership should include an Identity Management Practice Statement for evaluation by the Federation Operator. The Federation Operator presents a recommendation for membership with an evaluation report to RedCLARA who in turn decides on whether to grant or deny the application.

If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.

5.2 How to withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to the Federation Operator. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization in reasonable time interval.

The Federation Operator may cancel its participation in the Federation by announcing the termination date to the Federation Members. Until termination date, Federation Operator shall run the Federation on best effort basis. After the termination date, Federation Operator shall cancel the use of all Federations Technology Profiles for all Federation Members.

6. Legal conditions of use

6.1 Termination

A Federation Member who fails to comply with the Federation Policy may have its membership in the Federation revoked.

If the Federation Operator is aware of a breach of the Federation Policy by a Federation Member, the Federation Operator may issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, RedCLARA may issue a formal notification of impending revocation after which RedCLARA can make a decision to revoke the membership.

Revocation of a membership implies as soon as possible the revocation of the use of all Technology Profiles for the Federation Member.

6.2 Liability and indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and RedCLARA for any faults and defects meaning amongst other that the Federation Member cannot demand that Federation Operator amend defects, refund payments or pay damages. Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.

The Federation Operator and RedCLARA may not be held liable for any loss, damage or cost that arises as a result of the Federation Member connection to or use of Federation services, or other systems to which the Federation Member obtains access in accordance with the agreement. This limitation of liability does not however apply in the case of gross negligence or intent shown by Federation Operator personnel.

Neither the Federation Operator nor RedCLARA shall be liable for damage caused to the Federation Member or its End Users. The Federation Member shall not be liable for damage caused to the Federation Operator or RedCLARA due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services.

Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member's

membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members. Federation Operator and the Federation Member shall refrain from claiming damages from other Federation Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.

The Federation Member is required to ensure compliance with applicable laws. Neither the Federation Operator nor RedCLARA shall be liable for damages caused by failure to comply with any such laws on behalf of the Federation Member or its End Users relating to the use of the Federation services.

Neither party shall be liable for any consequential or indirect damage.

Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Federation Operator and Federation Members remain bound only by their own respective laws and jurisdictions.

The Federation Member and Federation Operator shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

6.3 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy shall be settled primarily through negotiation. If the issue cannot be resolved through negotiation, any disputes shall be submitted to RedCLARA board of directors.

If such negotiations do not succeed within four weeks of the date on which the claim for negotiations was made in writing by one party, each of the parties may bring the dispute before RedCLARA board of directors.

The FIEL Identity Federation Member Agreement and this policy is governed by the Laws of Uruguay and all disputes SHALL be settled before the Commercial Court of Montevideo.

6.4 Interfederation

In order to facilitate collaboration across national and organizational borders the Federation may participate in interfederation agreements. How the potential interfederation agreement is administratively and technologically reflected for certain technology is described in appropriate Technology Profiles.

The Member understands and acknowledges that via those interfederation arrangements the Member may interact with organizations which are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in this Federation.

6.5 Amendment

The Federation Operator has the right to amend the Federation Policy from time to time. Any such changes need to be approved by the governance and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.

7. Metadata Registration Practice Statement

7.1 Introduction and Applicability

This section below 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.redclara.net/index.php/en/servicios-rc/federaciones-de-identidad 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.

7.2 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 procedure for becoming a member of the Federation is documented in section 5.1.

The membership procedure verifies that the prospective member has legal capacity and requires that all members enter a contractual relationship with the Federation Operator by agreeing to the Federation policy. The Operator makes checks based on the legal name provided.

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 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.

7.3 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.

```
<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>
```

7.4 Entity Eligibility and Validation

7.4.1 Entity Registration

The process by which a Federation member can register an entity is described at https://www.redclara.net/index.php/en/somos/integrarse-a-redclara/tipos-de-asociacion

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.

7.4.2 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.

7.4.3 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 '$' anchor (e.g. (foo|bar)\.example\.com$).

7.4.4 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.

7.5 Entity Management

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

7.5.1 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 (fiel@redclara.net).

7.5.2 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 interFederation agreements;

- Improve interoperability;
- Add value to the metadata.

Changes will be communicated to Registered Representatives for the entity.

7.6 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. 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.