YAMI

Identity Community Policy

December 2024

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 User of a Home Organization.

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: consists of Attributes of an End User. It is issued and managed by a Home Organization and zero or more Attribute Authorities based on 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.

Community of Identity Communities: An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.

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

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

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.

Inter-community: Voluntary collaboration of two or more Identity Community to enable End Users in one Identity Community to access Service Providers in another Identity Community.

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.

Yami: The Costa Rican Community for Identity Management. Yami means "family" in the indigenous language Bribri.

2. Introduction

The Costa Rican Community for Identity Management (YAMI) is the union of entities or organizations with the purpose of exchanging information and resources to facilitate and simplify the introduction of mutually shared services, through the adoption of technologies that allow the establishment of a common Digital Identity, valid for all members of the Community.

YAMI relies on Identity Management Organizations/Providers to recognize and confirm the identity of end users to Service Providers, who may use that identity to grant (or deny) access to the services and resources they offer to end users correctly and accurately.

The Community Policy defines the obligations and rights of YAMI Members to use the best available technologies for electronic identification and access to attribute information and authorization regarding End Users.

This document, along with its appendices, constitutes the Community Policy. The current list of all appendices is available on the YAMI Community website.

3. Governance and Roles

3.1 Governance

The governance of the YAMI Community is delegated to the National Research and Education Network of the National Council of Rectors called RedCONARE; who will be responsible for:

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

3.2. Obligations and Rights of Community Operator

The Community Operator shall be a member of the Community providing infrastructure for proper and secure end-user authentication and authorization for Community members, who will be responsible for:

- Secure and trustworthy operational management of the Community and providing central services following the procedures and technical descriptions specified in this document and its appendices.
- Provides support services for Community Members' appropriate contact persons to work out operational problems regarding the Community services.

- Acts as center of competence for Identity Community: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within the Community.
- Prepares and presents issues to RedCONARE and acts as a liaison to RedCONARE meetings.
- Maintaining relationships with national and international stakeholders in the area of Identity Community. This especially includes contacts regarding inter-community activities and work with other Identity Community in the area of harmonization.
- Promoting the idea and concepts implemented in the Community so prospective Community Members learn about the possibilities of YAMI.

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

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

3.3. Obligations and Rights of Community Members

An entity or organization joining the Community agrees in writing to be bound by the Community Policy. A member of the Community may act as a Home Organization and/or a Service Provider and/or an Attribute Authority.

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

- Shall appoint and name an administrative contact for interactions with the Community Operator.
- Must cooperate with the Community Operator and other Members in resolving incidents and should report incidents to the Community Operator in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Community 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.
- To keep up to date with the affiliation agreements established in the collaboration agreement between RedCONARE and the entity or organization.
- If a Community Member processes personal data, Community Member will be subject to applicable data protection laws and must follow the practice presented in Data Protection Profile.

3.4. Home Organization

Any member may act as a Home Organization to which an End User is affiliated. It shall be responsible for authenticating the End User and managing the End Users' digital identity data.

In addition to what is stated elsewhere herein, the Home Organization shall have the following powers and duties:

- 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 Community Operator, who in turn makes it available to other Community 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 Community 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 Community Operator but must make every effort to ensure that only relevant problems and queries are sent to the Community Operator by appropriate Home Organization contacts.

3.5. Attribute Authority

Any member may act as an Attribute Authority by assuming responsibility for administering additional attributes for an End User of a Home Organization.

In addition to what is stated elsewhere in this document, the Attribute Authority shall have the following powers and duties:

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

3.6. Service Provider

Any member acting as a Service Provider shall:

- Be responsible for deciding which End Users can access the services they operate, and determining the access rights granted to an End User. It is Service Providers responsibility to implement those decisions.

4. Eligibility of YAMI Community

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

The Identity Provider will be a Home Organization responsible for offering the End User the service they wish to use. They will be able to rely on the authentication result and the attributes that the Home Organizations and Attribute Authorities assert for their End Users.

Community 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 community member. Each community member is responsible for its own users and responsible for fulfilling all the rules of the community.

To become a member of Yami Identity Community as a Service Provider only, and to receive identity information from Yami Identity Community Identity Providers, a Service Provider is NOT REQUIRED to become a participant of RedCONARE. These requests will be evaluated by the Yami Identity Community and MUST comply with RedCONARE policies.

5. Procedures

5.1. Admission and denials

In order to become a YAMI Community Member, an organization applies for membership in the Community by agreeing to be bound by the Community 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 Community Operator. The Community Operator presents a recommendation for membership with an evaluation report to RedCONARE who in turn decides on whether to grant or deny the application.

The membership procedure ensures that prospective members possess full legal capacity and mandates that all members engage in a contractual agreement with the Community Operator, adhering to the Community Policy. The Operator may conduct a verification process using the provided legal name. Additionally, Registered Representatives of the applicant organization or entity, authorized to represent them before the Community Operator, must be identified and verified.

If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Community Operator. Within one month of receiving notification, the organization denied membership may submit a written request to RedCONARE for reconsideration of the decision. This request should include reasons and evidence supporting the organization's claim. Each organization is allowed only one reconsideration request.

5.2. Voluntary withdrawals

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

If a Community Operator presents voluntary withdrawal from its participation in the Community, it shall give prior notice of its decision to RedCONARE, indicating an exact date of termination to the other Community Members, which may not be less than one calendar month. During the notice period and until the termination date, the Community Operator will be obliged to manage the Community on a best effort basis. After the date of its withdrawal, the Community Operator will terminate the use of the Community Members' Technology Profiles.

6. Legal conditions of use

6.1. Termination

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

If the Community Operator is aware of a breach of the Community Policy by a Community Member, the Community 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 Community Operator, RedCONARE may issue a formal notification of impending revocation after which RedCONARE 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 Community Member.

6.2. Liability and indemnification

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

The Community Operator and RedCONARE may not be held liable for any loss, damage or cost that arises as a result of the Community Member connection to or use of Community services, or other systems to which the Community 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 Community Operator personnel.

Neither the Community Operator nor RedCONARE shall be liable for damage caused to the Community Member or its End Users. The Community Member shall not be liable for damage caused to the Community Operator or RedCONARE due to the use of the Community services, service downtime or other issues relating to the use of the Community services.
Unless agreed otherwise in writing between Community Members, the Community Member will have no liability to any other Community Member solely by virtue of the Community Member's membership of the Community. In particular, membership of the Community alone does not create any enforceable rights or obligations directly between Community Members. Community Operator

and the Community Member shall refrain from claiming damages from other Community Members for damages caused by the use of the Community services, service downtime or other issues relating to the use of Community services. The Community Member may, in its absolute discretion, agree variations with any other Community Member to the exclusions of liability. Such variations will only apply between those Community Members.

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

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

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

The Community Member and Community Operator shall refrain from claiming damages from entities in other communities involved in an inter-community agreement.

6.3. Jurisdiction and dispute resolution

Complaints and disputes related to the interpretation, scope, content or execution of the Community Policy in force shall be resolved by direct negotiation and the signing of agreements. If such negotiations are unsuccessful within 30 business days of the submission of the written complaint, each member may separately submit its disagreement to the knowledge and resolution of CONARE, which shall resolve the dispute in accordance with the current policies of the YAMI Community.

This policy will always be governed by the Costa Rican legal system, regardless of the nationality or origin of the member organization of the Community. Admission as a member of the YAMI Community shall imply for all legal purposes the voluntary and unconditional submission to the laws and Ordinary Courts of Justice of the Republic of Costa Rica.

6.4. Inter-Community Agreements

To foster international collaboration, Community members may establish Inter-Community agreements with other entities or organizations, adhering to the YAMI Community Policy. The process for establishing such agreements will be communicated through administrative and technological channels, as outlined in the technological profiles.

6.5. Updates and Amendments

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

7. Metadata Registration Practice Statement

7.1. Introduction and Applicability

The present Community 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 Community 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 Community helpdesk.

7.2. Member Eligibility and Ownership

Members of the Community are eligible to make use of the Community 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 Community 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

```
<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 Community Operator SHALL make use of the [SAML-Metadata-RPI-V1.0] metadata extension to indicate that the Community Operator is the registrar for the entity and to detail the version of the MRPS statement that applies to the entity.

7.4. Entity Eligibility and Validation

7.4.1. Entity Registration

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

The Community 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.

7.4.2. 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.

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 Community Operator for the member's right to use those domains. For these checks to be achievable by the Community 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 Community 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 Community 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 Community members needs to be communicated from or confirmed by their respective Registered Representatives.
Communication of change happens via e-mail (redes@conare.ac.cr).

7.5.2. Unsolicited Entity Changes

The Community Operator may amend or modify the Community metadata at any time in order to:

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

Changes will be communicated to Registered Representatives for the entity.

8. Effectiveness

The present Community Policies of YAMI Information shall be effective from the date of their publication on the official website.

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.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.