COFRe: Comunidad Federada REUNA

WebSSO Identity Provider Organizations Appendix

Version 2.1 - 01/21/2021

RedUNA
Ciencia y Educación en Red

Table of Content

RedUNA
Ciencia y Educación en Red

1. Definitions and Terminology

In this document

Attribute	A piece of information describing the End User, his/her properties or roles in an 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.
End User	Any natural person affiliated to an Identity Provider Organization, e.g. as an employee, researcher or student making use of the service of a 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 an Identity Provider Organization and/or a Service Provider.
Identity Provider Organization or IdP	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.
Service Provider or SP	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 Identity Provider Organizations assert for its End Users.
Federation Metadata	SAML/XML file which contains information about Federation Members.
Discovery Service	Service managed by the Federation Operator offered to the Federation Members acting as a Services Providers with a list of available Identity Provider Organizations of the Federation.
Level of Assurance Profile	Model or best practices which are used by the Identity Provider Organization as guideline in the validation and assurance of the End User identity (e.g. NIST 800-63-3)

2. Introduction

This document describes the points implied in the WebSSO Identity Provider Organization application process.

3. WebSSO Identity Provider Organization Obligations

3.1 Obligations and Rights of Federation Operator

This federation is operated by REUNA, the Chilean National Research and Education Network.

In addition to what is stated elsewhere in the Federation Rules, REUNA is responsible for:

- Secure and trustworthy operational management of the Federation Metadata and Discovery Services.
- Publish the information about the Attributes needed by Services Providers

3.2 Obligations and Rights of Identity Provider Organizations

In addition to what is stated elsewhere in the Federation Rules, if a Federation Member is acting as an Identity Provider Organization, it:

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them, as may be further specified in their Level of Assurance Profiles.
- Should submit its Identity Management Practice Statement to REUNA, 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 life-cycle 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 the Level of Assurance Profiles.
- Ensures an End User is committed to the Identity Provider Organization's Acceptable Usage Policy.
- Operates a helpdesk for its End Users regarding Federation services related issues. Identity Provider Organizations are encouraged to maintain a helpdesk for user queries at least during normal office-hours in the local time zone. Identity Provider Organizations must not redirect End User queries directly to REUNA, but must make every effort to ensure that only relevant problems and queries are sent to REUNA by appropriate Identity Provider Organization contacts.
- 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.
- Is responsible for keep its metadata up-to-date. If there is a change in its metadata, the technical responsible must notice this fact to REUNA.
- Must send a list of Services Providers which it is related if there is an intention of cancel its membership.

4. Eligibility

For Identity Provider Organizations, REUNA member institutions can apply to this membership directly. For other institutions its application shall be studied and take a resolution and informed via email within 15 days.

5. Amendment

REUNA has the right to amend the Federation Rules from time to time. Any such changes need to be reviewed by REUNA and shall be communicated to all Federation Members via email at least 90 days before they are to take effect.