F E N I X

Annex Identity Provider Policies (IdP)

Authors	Fernando Aranda
Last Modification	April 18, 2017
Version	1.0
Date	April 18, 2017

Copyright

The research conducted by CUDI and leading to these results has received funding from FONCICYT, under Agreement 4 / II / 2014, which authorized the allocation of resources to support the Second Call for registration of pre-proposals CONACYT Horizon2020 and through Agreement number 15/IVE/2015, of the Technical and Administration Committee of "FONCICYT", authorizing the transfer of resources in favor of CUDI for the development of the project called "**M**iddleware for Collaborative **A**pplications and **G**lobal V**I**rtual Communities". It is based on the results obtained from the financing granted by the Seventh Framework Program (FP7 2007-2013) of the European Community, under Grant Agreement No. 238875 (GÉANT).

Table of Contents

1 Definiciones

Identity Management	Process of issuing and managing the digital identities of the End Users.
Attribute	Piece of information describing the End User their properties and/or their roles within an Organization.
Authentication	Process by which the identity of a previously registered End User is verified.
Authorization	Process to allow or deny the right of access to a service for previously authenticated End User.
Digital Identity	A set of information attributable to an End User. This information is issued and administered by an Identity Provider Organization based on prior End User Authentication.
Discovery Service	Service managed by the Federation Operator for Federation Members acting as Service Providers which provides a list of Federation Identity Provider Organizations.
End User	Any person affiliated to an Identity Provider Organization, e.g. an employee, a researcher, teacher or student, making use of the services of a Service Provider.
Federation	The Identity Federation. An association of organizations that unite to exchange information of their users and their resources, in order to allow collaboration and transactions.
Identity or IdP Provider Organization	Organization with which the End User is affiliated. This is responsible for authenticating the End User and managing the data of the Digital Identity of its End Users.
Interfederation	Voluntary Collaboration of two or more Identity Federations to enable End Users in an Identity Federation to access to Service Providers of another Identity Federation.
Member of the Federation	An organization that has joined the Federation by accepting in writing the Federation Policies. Within the framework of the Federation a Member may act as an Identity Provider and/or a Service Provider.
Metadata	file in SAML / XML format containing information about Federation Members.
NREN	National Research and Educations Network (Also known as NREN)
Operator of the Federation	Organization which provide the infrastructure for the Authentication and Authorization of the Members of the Federation.
Service Provider or SP	Organization responsible to offering the End User the service it intends to use. The Service Providers can rely on the results of the authentication and attributes that the Identity Providers validate from their End Users.

2 Introduction

The Identity Management procedures used by the Identity Providers are very important in terms of the fact that the Digital Identity that is presented is effectively that of the End User.

This document describes the Obligations and Rights that the Identity Providers will have when joining FENIX and is an annex of the Federation's Policies.

3 Obligations and Rights

3.1 Obligations and Rights of the Federation Operator

This Federation is operated by CUDI, the National Education and Research Network in Mexico.

In addition to what is stated in any other section of the Federation's Policies, CUDI is responsible for:

- Safe and reliable operational management of Federation Metadata and Discovery Service (WAYF).
- Publish information about the attributes required for each Service Provider (SP)

3.2 Obligations and Rights of the Identity Provider

In addition to what is indicated in any other section of the Federation's Policies, if a Member is an Identity Provider:

- Will be responsible for delivering and managing the authentication credentials of its End Users, as well as for authenticating them, as specified in its Guarantee Level Profile.
- Must send his Identity Management Statement of Practice to CUDI (afiliaciones@fenix.org.mx), who in turn may provide it to other Federation Members upon request. The Identity Management Practice Statement is a description of the Identity Management lifecycle including a description of how individual digital identities are logged, maintained, and removed from the identity management system. The statement should contain descriptions of the administrative processes, practices, and core technologies used in the identity management lifecycle, and must be able to support a secure and consistent identity management lifecycle. Specific requirements may be imposed on the Warranty Level Profile.
- Ensure that the End User complies with the Acceptable Use Policy of the Identity Provider.
- Operate a Technical Assistance Center for its End Users regarding issues related to the Federation's services. Identity Providers are requested to maintain a Technical Assistance Center to respond to inquiries from End Users at least during normal business hours in the local time zone. Identity Providers should not forward End User queries directly to CUDI and should ensure that only relevant issues and queries are submitted to CUDI through the contacts registered by the Identity Providers.
- Be responsible for assigning Attribute values to End Users and managing the values to ensure they are updated.
- Be responsible for releasing the Attributes to Service Providers.
- Will be responsible for keeping your Metadata updated. In case of any change in their metadata, the technical responsible must notify CUDI of this fact (afiliaciones@fenix.org.mx).
- At the time of canceling your membership with the Federation, must send a list to CUDI (afiliaciones@fenix.org.mx) of the Service Providers with which were related.

4 Eligibility

Member institutions of CUDI may apply as an Identity Provider only by filling out the application for this purpose (afiliaciones@fenix.org.mx) and complying with the necessary technical requirements.

For other institutions or organizations your request must be studied, and the resolution will be informed via email within a maximum period of 15 calendar days from the date of receipt of the request.

5 Modification

CUDI has the right to modify the Federation Policies. Such changes must be communicated in writing (e-mail and/or postal mail) to all Members of the Federation at least 90 calendar days before coming into force.