



# GrIDP: Grid IDentity Pool Federation

---

## WebSSO Service Providers Appendix

<b>Authors</b>	Marco Fargetta, Roberto Barbera
<b>Last Modified</b>	12 August 2016
<b>Version</b>	2.6
<b>Based on</b>	<a href="#">COFRE WebSSO Services Providers Appendix v. 2.0</a>



This work is licensed under a [Creative Commons Attribution-ShareAlike3.0 Unported License](#).

## Table of Contents

1. Definitions and Terminology .....	3
2. Introduction.....	3
3. WebSSO Service Provider Obligations.....	3
3.1. Obligations and Rights of Federation Operators.....	3
3.2. Obligations and Rights of Service Providers.....	4
4. Eligibility .....	4
5. Amendment.....	5

# 1. Definitions and Terminology

Definitions and terminology used in this document:

Attribute	A piece of information describing a characteristic of an entity (in this context of 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, e.g. as an employee, researcher or student.
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 and/or a Service Provider.
Identity Provider or IdP	A service managed by an entity with which the 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 or Resource	A service an entity is offering to the End User. Service Providers may rely on the authentication outcome and attributes that Identity Providers assert for its End Users.
Federation Metadata	SAML/XML file which contains information about Federation Members.
Discovery Service	Service used by Services Providers to manage a list of available Identity Providers of the Federation enabled to perform the authentication for the service.

## 2. Introduction

This document describes the points implied in the WebSSO Service Providers' application process.

## 3. WebSSO Service Provider Obligations

### 3.1. Obligations and Rights of Federation Operators

The GridP Federation is jointly managed and operated by the Division of Catania of the Italian National Institute of Nuclear Physics (hereinafter referred to as "INFNCT") and by the Department of Physics and Astronomy of the University of Catania (hereinafter referred to as "UNICT-DPA"). The Federation central services are hosted at GARR, the Italian National Research and Education Network.

In addition to what is stated elsewhere in the Federation Rules, INFNCT and UNICT-DPA are responsible for:

- Secure and trustworthy operational management of the Federation Metadata and Discovery Services.

### 3.2.Obligations and Rights of Service Providers

In addition to what is stated elsewhere in the Federation Rules, 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;
- In addition to access grant, the Service provider can use the information retrieved from Identity Providers only for the following purposes:
  - Customization (Interface);
  - Audit;
  - Usage reports;
  - For any other purpose specifically agreed between the Identity Provider and the Service Provider.
- Is responsible for noticing INFNCT and UNICT-DPA which Attributes are needed for access grant and the other purposes described before;
- Can make use of the GrIDP's Discovery Service;
- Is responsible for keeping its metadata up-to-date;
- Must send a list of Identity Providers which it is related to if there is an intention of cancelling its membership.

## 4. Eligibility

Service Providers can apply for membership at any time by submitting a specific application form available on the [GrIDP website](#). Their applications will be evaluated (either accepted or denied) within 15 days against the following criteria:

- Completeness, consistency of the documentation;
- Installed certificates;
- The accuracy of the Service registration in the Federation;
- The proper working of the Service;
- The consistency with the information provided through the request forms.

Upon acceptance, the Organisation receives exclusively to the provided email addresses the countersigned documents. If rejected, the Organisation is notified with the reason of the refusal.

## **5. Amendment**

INFNCT and UNICT-DPA have the right to amend the Federation Rules from time to time. Any such changes need to be reviewed and shall be communicated to all Federation Members via email at least 90 days before enter into force.