GrIDP: Grid IDentity Pool Federation

WebSSO Identity Providers Appendix

Authors	Marco Fargetta, Roberto Barbera
Last Modified	12 August 2016
Version	2.6
Based on	COFRE WebSSO Identity Providers Organizations Appendix v. 2.0

Table of Contents

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 Identity Providers' application process.

3. WebSSO Identity 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.
- Publish the information about the Attributes needed by Services Providers.

3.2. Obligations and Rights of Identity Providers

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

- Is responsible for 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 INFNCT and UNICT-DPA, who in turn make 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 Level of Assurance Profiles;
- Operates a helpdesk for its End Users regarding Federation services related issues. Identity Providers 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 INFNCT and/or UNICT-DPA, but must make every effort to ensure that only relevant problems and queries are sent to INFNCT and/or UNICT-DPA by appropriate Identity Provider 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 keeping its metadata up-to-date;
- Must send a list of Services Providers which it is related to if there is an intention of cancelling its membership.

Additionally, if the users enrolled in the Identity Provider are not strictly related to the organisation providing the service but the Identity Provider accepts “homeless” users, the organisation:

- Is responsible for the correct association between organisations and users;
- Should verify the validity of the Attribute Values of the End User, at least once a year. The organisation should apply a policy forcing the End User to validate their Attribute or they will expire with the subsequent lock of the End User account.

4. Eligibility

Identity 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 they enter into force.