GrIDP: Grid IDentity Pool Federation

Identity Federation Rules

Authors	Marco Fargetta, Roberto Barbera
Last Modified	12 August 2016
Version	2.6
Based on	COFRE Identity Federation Rules v. 2.1

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.
Digital Identity	A set of attributes belonging to an End User. It is issued and managed by an Identity Provider on the basis of the identification of the 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.
Interfederation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
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.
Technology Profile	A defined type of federated technology (e.g., WebSSO, eduroam)
WebSSO Identity Provider appendix	Appendix with specific rules for Federation Members who wants to apply to the federation as a WebSSO Identity Provider.
WebSSO Service Providers appendix	Appendix with specific rules for Federation Members who wants to apply to the federation as a WebSSO Service Provider.

2. Introduction

An Identity Federation (Federation) is an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions. The Grid IDentity Pool, GrIDP (the Federation), is a cross-border/cross-domain federation spanning multiple continents introduced to facilitate, simplify and promote the use and the adoption of shared e-Research services across the world. The main goal of GrIDP is to provide: (i) a home to Identity

Providers and Service Providers not (yet) member of any national federations, and (ii) authentication services for users not enrolled in any Identity Providers. Additionally, the GrIDP federation is meant to be an open test-bed for its members to experiment on large scale new technologies and policies related to federated authentication and authorisation.

This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation. The Federation relies on Identity Provider Organizations to correctly and accurately assert information about the identity of End Users to Service Providers, that may use that information to grant (or deny) access to the services and resources they offer to End Users. The Federation Rules document defines the Federation by defining the Federation Members' obligations and rights to be able to use available Federation Technologies for electronic identification and for access to attribute and authorization information about End Users in the Federation. This document, together with its appendices constitutes the Federation Rules. The current list of all appendices is available on the GrIDP website.

3. Governance and Roles

3.1. Governance

The Federation is jointly managed 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:

- Setting criteria for membership of the Federation;
- Evaluating and determining whether to grant or deny an application for membership in the Federation;
- Revoking the membership if a Federation Member is in a breach of the Federation Rules;
- Evaluating and determining future directions and enhancements for the Federation;
- Evaluating and determining the entering into inter-federation agreements according to the interest of Federation Members;
- Maintaining formal ties with relevant national and international organizations;
- Approving changes to the Federation.
- Deciding on any other matter referred to the Federation.

3.2. Obligations and Rights of Federation Operators

The Federation is jointly operated by INFNCT and UNICT-DPA .

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 and providing central services following the procedures and technical descriptions specified in this document and its appendices;
- Providing support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services;
- Acting as centres of competence for Identity Federation: test software, recommend and document solutions, provide software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding inter-federation activities and work with other Identity Federations in the area of harmonization;
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.

In addition to what is stated elsewhere in the Federation Rules, INFNCT and UNICT-DPA reserve the right to:

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

3.4.Obligations and Rights of Federation Members

In addition to what is stated elsewhere, in the Federation Rules all Federation Members:

- Must appoint a technical and/or an administrative contact for interactions with INFNCT and UNICT-DPA;
- Must cooperate with INFNCT, UNICT-DPA and other Members in resolving incidents and should report incidents to INFNCT and UNICT-DPA in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Federation or any of its Members;
- Must comply with the obligations defined in the Technology Profiles, when specified;
- Must agree in facilitate the use of their names in the communicational channels disposed by INFNCT and UNICT-DPA, for the purpose of promoting the Federation;
- In the same way, the member must commit to mention INFNCT and UNICT-DPA as the service operators in their communicational media as appropriate.

4. Eligibility

The Federation welcomes all kind of legal entities, both public and private, to become Federation Members and register services. Depending on the profile of the service(s) that the institution wants to apply (WebSSO Service Provider, WebSSO Identity Provider or other) additional technical eligibility criteria are described in

the respective appendices. Responsibility for defining membership criteria rests with INFNCT and UNICT-DPA and may be revised from time to time.

5. Procedures

5.1. How to Join

In order to become a Federation Member, an organization applies for membership in the Federation by agreeing to be bound by the Federation Rules in written by an official representative of the organization.

Each application for membership has to be sent to INFNCT and UNICT-DPA who in turn decides on whether to grant or deny the application.

If the application is denied, the decision and the reason for denying the application are communicated to the applying organization by INFNCT or UNICT-DPA.

5.2. How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to either INFNCT or UNICT-DPA. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization in reasonable time interval.

6. Legal conditions of use

6.1. Termination

A Federation Member who fails to comply with the Federation Rules may have its membership revoked.

If INFNCT or UNICT-DPA are aware of a breach of the Federation Rules by a Federation Member, they may issue a formal notification of concern within 5 working days. If the cause for the notification of concern is not rectified within 60 days by the Federation Member, INFNCT and UNICT-DPA 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 Federation Member.

6.2.Inter-federation

In order to facilitate collaboration across national and organizational borders the Federation may participate in inter-federation agreements. How the potential inter-federation agreement is administratively and technologically reflected for certain technology is described in appropriate Technology Profiles.

The Members understand and acknowledge that via those inter-federation arrangements they may interact with organizations which are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in this Federation.

6.3.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.