



MATE Federation

Model for Access to Technology and Education

Identity Federation Policy

Authors	Angel Martinez
Last Modified	07-15-2014
Version	0.0



This work is licensed under a [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

Table of Contents

1	Definitions and Terminology	3
2	Introduction	4
3	Governance and Roles	4
	3.1 Governance	4
	3.2 Obligations and Rights of Federation Operator	5
	3.3 Obligations and Rights of Federation Members	5
4	Eligibility	6
5	Procedures	7
	5.1 How to Join	7
	5.2 How to Withdraw	7
6	Legal conditions of use	7
	6.1 Termination	7
	6.2 Interfederation	8
	6.3 Amendment	8

1 Definitions and Terminology

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.
Digital Identity	A set of information that is attributable to an End User. Digital identity consists of Attributes. It is issued and managed by a Home Organization and zero or more Attribute Authorities on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home 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 a Home Organization and/or a Service Provider and/or an Attribute Authority.
Home Organization	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.
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	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 Home Organizations and Attribute Authorities assert for its End Users.

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 MATE Identity Federation (the Federation) is introduced to facilitate and simplify the introduction of shared services across the Federation. 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 Home Organizations and Attribute Authorities 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 Policy 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 Policy. The current list of all appendices is available on the website of the Federation.

3 Governance and Roles

3.1 Governance

The governance of the Federation is delegated to the Federation Governing Committee. Structure and election process of the Federation Governing Committee is defined in appendix Federation Governing Committee Constitution.

In addition to what is stated elsewhere in the Federation Policy the Federation Governing Committee is responsible for:

- Setting criteria for membership for the Federation.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Maintaining formal ties with relevant national and international organisations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

3.2 Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator is 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.
- Provides support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Acts as centre of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Prepares and presents issues to the Federation Governing Committee and acts as the secretary of the Federation Governing Committee meetings.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation 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 Policy, the Federation Operator reserves 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 fulfills 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.

3.3 Obligations and Rights of Federation Members

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

- Shall appoint and name an administrative contact for interactions with the Federation Operator.
- Must cooperate with the Federation Operator and other Members in resolving incidents and should report incidents to the Federation Operator 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 of the Technology Profiles which it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- Must comply with the obligations of the appendix Fees.

- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and must follow the practice presented in Data Protection Profile.

If a Federation Member is acting as a Home Organization, it:

- 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 delivering and 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 the Federation Operator, 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 Level of Assurance Profiles.
- Operates a helpdesk for its End Users regarding Federation services related issues. Home Organizations are encouraged to maintain a helpdesk for user queries at least during normal office-hours in the local time zone. Home Organizations must not redirect End User queries directly to the Federation Operator, but must make every effort to ensure that only relevant problems and queries are sent to the Federation Operator by appropriate Home Organization contacts.

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.

4 Eligibility

The Federation sets out eligibility criteria that determines who is able to become a Federation Member and who is able to act as Home Organization. The criteria is fully described in appendix Eligibility Criteria.

Responsibility for setting membership criteria rests with the Federation Governing Committee of the Federation any 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 Policy in writing by an official representative of the organization.

Each application for membership is evaluated by the Federation Operator. The Federation Operator presents a recommendation for membership with an evaluation report to the Federation Governing Committee who in turn decides on whether to grant or deny the application.

If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.

5.2 How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to the Federation Operator. 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 Policy may have its membership in the Federation revoked.

If the Federation Operator is aware of a breach of the Federation Policy by a Federation Member, the Federation Operator may issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, the Federation Governing Committee may issue a formal notification of impending revocation after which the Federation Governing Committee 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 Interfederation

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

The Federation Member understands and acknowledges that via those interfederation arrangements the Member 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

The Federation Operator has the right to amend the Federation Policy from time to time. Any such changes need to be approved by the Federation Governing Committee and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.