

LIFE (Lebanese Identity Federation Ecosystem)

Identity Federation Policy

Last Modified	January 2017
Version	0.1



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	Membership and Eligibility	5
4	Governance and Roles	5
	4.1 Obligations and Rights of Federation Operator	5
	4.2 Obligations and Rights of Federation Members	6
	4.3 Obligations and Rights of a Home Organization	6
	4.4 Obligations and Rights of an Attribute Authority	7
	4.5 Obligations and Rights of a Service Provider	7
5	Conditions of use	7
	5.1 Interfederation	7
	5.2 Amendment	7

1 Definitions and Terminology

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization.
Attribute Authority	An organization responsible for managing additional Attributes for an End User of a Home 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 based on the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. such 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. In this case the American University of Beirut (AUB)
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.
Federation Executive Board	It is the decision making authority in the Federation Operator

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 *Lebanese Identity Federation Ecosystem (LIFE)* (the Federation) is formed to facilitate and simplify the deployment 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.

LIFE is hosted and operated by the American University of Beirut AUB, hereby referred to as “Federation Operator”.

The Federation Policy document defines the Federation Members’ obligations and rights while they 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 life.aub.edu.lb.

3 Membership and 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 are described below. Responsibility for setting membership criteria rests with the governing body of the Federation and may be revised from time to time.

Federation membership is open to organizations that support research and education such as:

- Higher education
- Lower, primary or secondary education
- Further education
- University libraries
- Public research institutions

All Federation Members are required to have a point of contact for technical coordination

The “Federation Executive Board” will periodically revise and amended the list of eligibility criteria as needed

4 Governance and Roles

4.1 Obligations and Rights of Federation Operator

The Federation Operator is responsible for establishing, communicating, implementing, and executing policies and processes based to::

- Grant or deny an application for membership in the Federation
- Decide whether a Federation Member is entitled to act as Home Organization.
- Enter into inter-federation agreement.
- Maintain formal ties with relevant national and international organizations.
- Decide on the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Provide secure and trustworthy operational management of the Federation and central services following the procedures and technical descriptions specified in this document and its appendices.
- Provide support services for Federation Members’ appropriate contact persons to work out operational problems regarding the Federation services.
- Act 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.
- Prepare and present issues to the *Advisory Committee* and acts as the secretary of the **governing body** meetings.
- Maintain 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.
- Promote 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 in the following sections of the Federation Policy, the Federation Operator, based on its published policies, reserves the right to:

- Revoke the membership if a Federation Member is in a breach of the Policy.
- 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 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.

4.2 Obligations and Rights of Federation Members

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

- Agree to abide by the Federation Operator policies
- Are eligible for all services provided by the Federation Operator, unless the Federation Member specifies excluded services
- 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 that it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- 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.

4.3 Obligations and Rights of a Home Organization

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

- 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 (sample template is provided in the Membership Agreement).
- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy.
- 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.

4.4 Obligations and Rights of an Attribute Authority

If a Federation Member is acting as an Attribute Authority, it:

- Is responsible for assigning Attribute values to the End Users and managing the values in a way that ensures they are up-to-date.
- Is responsible to releasing the Attributes to Service Providers.

4.5 Obligations and Rights of a Service Provider

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 define the policies and implement those decisions.

5 Conditions of use

5.1 Interfederation

In order to facilitate collaboration across national and organizational borders the Federation may participate in interfederation agreements.

The 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.

5.2 Amendment

The Federation Operator has the right to amend the Federation Policy from time to time.