



LEAF

(Moldovan Research And Education Identity Federation)

Identity Federation Policy

Authors	P. Bogatencov, V. Pocotilenco, C. Scifos, A. Cacean, A. Rusu
Last Modified	11.02.2015
Version	0.2



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
	4.1 How to Join	6
	4.2 How to Withdraw	6
5	Legal conditions of use	7
	5.1 Termination	7
	5.2 Liability	7
	5.3 Jurisdiction and dispute resolution	7
	5.4 Interfederation	8
	5.5 Amendment	8

1 Definiții și Terminologie

<i>MD-IF</i>	Federația de Identitate pentru instituțiile de cercetare și educație din Republica Moldova
<i>LEAF</i>	Operator MoLdovan ResEarch and EducAtion Identity Federation
<i>Pagina web</i>	federations.renam.md
<i>Atribut</i>	Componentă informațională care descrie Utilizatorul final, proprietățile și rolurile în Organizație membru.
<i>Manager Atribute</i>	Organizație responsabilă pentru managementul Atributelor adiționale pentru Utilizatorul final al Organizației membru.
<i>Autentificare</i>	Procesul de validare a identității Utilizatorului existent.
<i>Autorizare</i>	Procesul de acordare sau refuzare a drepturilor de acces la un serviciu pentru Utilizator autentificat.
<i>Identitate digitală</i>	Set de informație atribuită unui Utilizator final. Identitatea digitală constă din Atribute. Este emisă și gestionată de o Organizație membru și zero sau mai mulți Manageri de Atribute în baza identificării Utilizatorului final.
<i>Utilizator final</i>	Orice persoană fizică afiliată la o Organizație membru, de exemplu, angajat, cercetător sau student, fiind utilizator de serviciu unui furnizor de servicii.
<i>Federație</i>	Federație de identitate. O asociație de Organizații membre în colaborare, cu schimb de informație despre utilizator în scopul partajării resurselor informaționale.
<i>Operator Federație</i>	Organizație responsabilă pentru funcționarea și dezvoltarea infrastructurii pentru autentificare și autorizare și furnizarea serviciilor AAI membrilor Federației.
<i>Membru Federație</i>	Organizație care a aderat la Federație acceptând politica de activitate a Federației, prin semnarea unui acord de colaborare. În cadrul Federației, un membru Federației poate activa ca Furnizor de Identitate și/sau un Furnizor de Servicii și/sau Manager Atribute.
<i>Furnizor de Identitate</i>	Organizația cu care este afiliat Utilizatorul final. Acesta este responsabil pentru autentificarea Utilizatorului final și gestionarea datelor de Identitate digitală a Utilizatorilor finali.
<i>Furnizor de Servicii</i>	Organizația responsabilă pentru oferirea Utilizatorului final serviciul spre utilizare. Furnizorii de servicii se bazează pe rezultatele autentificării și atributele care Furnizorul de Identitate și Managerul Atribute prestează pentru utilizatorii finali.
<i>Interfederație</i>	Colaborare voluntară a două sau mai multe Federații de identitate, pentru a permite Utilizatorilor finali dintr-o Federație de identitate accesul către Furnizorii de servicii într-o altă Federație de identitate.
<i>Management de Identitate</i>	Procesul de emitere și gestionare a identităților digitale al Utilizatorilor finali.

2 Introducere

Federație de identitate (Federație) este Asociație la nivel național pentru organizațiile de cercetare și educație care vin împreună pentru a face schimb de informații despre utilizator în scopul partajării resurselor informaționale.

LEAF (Federația) este destinată pentru a facilita și simplifica introducerea serviciilor partajate în instituțiile de cercetare și învățământ din Republica Moldova. Acest lucru se realizează prin utilizarea tehnologiilor Federative de extindere a domeniului de aplicare al unei Identități Digitale emise de un Membru Federație să fie valabilă în întreaga Federație. Federația se bazează pe informații corecte despre identitatea Utilizatorilor finali prestate de Furnizori de Identitate și Manageri Atribute către Furnizorii de servicii, care TREBUIE să utilizeze această informație pentru a acorda (sau refuza) accesul la serviciile și resursele oferite Utilizatorilor finali.

Politica Federației definește Federația prin definirea obligațiilor și drepturilor membrilor Federației de a putea folosi Tehnologiile Federative, disponibile pentru identificarea electronică și accesul la atribute și informații de autorizare despre Utilizatorii finali din Federație.

LEAF activează în conformitate cu legislația națională a Republicii Moldova și respectă prescripțiile sale.

Acest document, împreună cu anexele sale constituie politica Federației. Lista curentă a tuturor anexelor este disponibilă pe pagina web a Federației.

3 Guvernare și Roluri

3.1 Guvernare

CORPUL DE GUVERNARE (CG) al Federației de Identitate pentru instituțiile de cercetare și educație din Republica Moldova este MD-IF Consorțiul, în continuare Consorțiu.

În plus față de ceea ce este declarat în altă parte în cadrul politicii Federației Consorțiul este responsabil pentru:

- Stabilirea criteriilor de aderare la Federație.
- Evaluarea și determinarea cazului de acord sau refuz al cererii de aderare la Federație.
- Determinarea dreptului unui Membru a Federației de a activa în calitate de Furnizor de Identitate.
- Revocarea acordului de colaborare în cazul în care un Membru Federației încalcă prescripțiile din Politica Federației.
- Planificarea direcțiilor de dezvoltare pentru majorarea calității serviciilor pentru Federație împreună cu Operatorul Federației.
- Menținerea legăturilor formale cu organizațiile naționale și internaționale relevante.
- Aprobarea modificărilor în Politica Federației înaintate de Operatorul Federației.
- Managementul financiar în procesul de operare a Federației.
- Crearea unui comitet de audit și validare a rapoartelor publice.
- Aprobarea schemei de finanțare pentru acoperirea costurilor operaționale ale Federației.
- Luarea deciziilor cu privire la alte probleme referitoare la Federație.

3.2 Obligations and Rights of Federation Operator

Federation Operator is responsible for operation and development of Infrastructure for Authentication and Authorization and providing AAI services to Federation Members. In addition to what is stated elsewhere in the Federation Policy, *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: recommends and documents solutions, provides 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 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.

Also it 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.
- Define the procedure and terms of revising the criteria that determines who is able to become a Federation Member and who is able to act as Home Organization

3.3 Obligations and Rights of Federation Members

Basically 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.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws of Moldova, Republic of.
- MUST ensure agreed by the Consortium contributions to support MOLDOVAN R&E IDENTITY FEDERATION operation;
- MUST follow the National law of the Republic of Moldova

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.
- 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 lifecycle.

- 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.

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 are fully described in LEAF Federation Operation document. Responsibility for setting membership criteria rests with the *MD-IF* of the Federation and MAY be revised from time to time by the MD-IF Consortium.

4.1 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 written by an official representative of the organization letter.

Each application for membership first is evaluated by the Federation Operator. Operator presents a recommendation for membership with an evaluation summary to the *Consortium* 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.

4.2 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.

The Federation Operator MAY cancel its participation in the Federation by announcing the termination date to the Federation Members. Until termination date, Federation Operator SHALL run the Federation on best effort basis. After the termination date, Federation Operator SHALL cancel the usage of all related Federations Technology Profiles for all Federation Members.

5 Legal conditions of use

5.1 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, notification of revocation will be issued and membership will be revoked.

Revocation of a membership implies as soon as possible the revocation of the use of all related Technology Profiles for the Federation Member.

5.2 Liability

The Federation Operator offers this service on an “as is” basis, without any warranties or liabilities to the Federation Member or its End Users. Neither the Federation Operator operations team nor the Federation Members SHALL be liable for damage caused to the Federation Member or its end user. LEAF members SHALL not be liable for damage caused to the LEAF due to the use of the Federation services, service downtime or other issues relating to the use of the LEAF services. Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.

Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member’s membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members. Federation Operator and the Federation Member shall refrain from claiming damages from other Federation Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.

Federation Member neither party SHALL be liable for any consequential or indirect damage.

Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Federation Operator and Federation Members remain bound only by their own respective laws and jurisdictions.

The Federation Member and Federation Operator SHALL refrain from claiming damages from entities in other federations involved in an interfederation agreement.

5.3 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy SHALL be settled primarily through negotiation. If the issue cannot be resolved through negotiation within MD-IF Consortium, any disputes SHALL be submitted to an authorized court in Chisinau that will decide according to the National law of the Republic of Moldova.

5.4 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 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.

5.5 Amendment

The Federation Operator or any Federation Member have the rights to propose amendment to the Federation Policy. Any such changes need to be approved by the Governing Body - MD-IF *Consortium* and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.