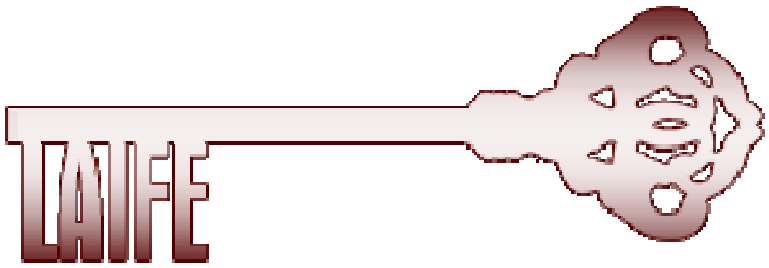

Latvian Academic Identity Federation (LAIFE) policy

Document Management	
Version	1
Date:	19. September 2012
Related documents:	LAIFE Technical Policy
Author(s):	Dana Ludviga (IMCS UL) Mārtiņš Pūriņš (UL IT)
Approved by:	LAIFE Steering Committee

1. Terms & Definitions

In this policy the concepts below are defined as follows:
Authentication: Verification of the end user's identity;
Authorization: Granting to an end user access to a service;
Attributes: User references (e.g.: affiliation, surname, first name, e-mail);
Service Provider: LAIFE Member authorized to provide services to the users of LAIFE;
Identity Provider: LAIFE Member authorized to manage and keep the identity data of its users.
Federation operator: The entity running the federation core services.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119, see http://www.ietf.org/rfc/rfc2119.txt.

2. LAIFE policy

Latvian Academic Identity Federation policy (hereinafter - Policy) defines the *Latvian Academic Identity Federation* (hereinafter - **LAIFE** by specifying procedures and practices which allow its Members to use available federation technologies for electronic identification and for access to authorization information about individuals, resources and other objects in the federation. This Policy does not directly describe practices or procedures specific to any particular choice of federation technology.

The technical minimum requirements for being able to be affiliated to the infrastructure of LAIFE have been described in the technical document (Technical Policy).

LAIFE Steering Committee (see 3.2.2 Steering Committee) reserves the right to alter this Policy and the technical minimum requirements in the Technical Policy at any time. The alterations MUST be published on LAIFE's website and will come into effect two months after their notification via e-mail.

3. The purpose and structure of LAIFE

LAIFE is introduced to facilitate and simplify the offering of shared services across its Members. This is accomplished by using technologies to extend the scope of an (electronic) identity issued by one Member of LAIFE to be valid across the whole federation.

3.1. Objectives and scope

The purpose of LAIFE is to make it possible for (Application / Information) Service Providers (see 3.2.4. Service Provider) to provide services to the end users of LAIFE (see 3.2.5 LAIFE users). This is accomplished by making infrastructure for federated identification and authentication available to the higher education and research community in Latvia, including but not limited to universities, university colleges, scientific institutes, research hospitals, government agencies and private sector organizations involved in higher education and research.

In order to facilitate collaboration across national and organizational borders LAIFE MAY participate in interfederation agreements.

The University of Latvia is responsible for maintaining formal ties with relevant national and international organizations.

3.2. LAIFE structure

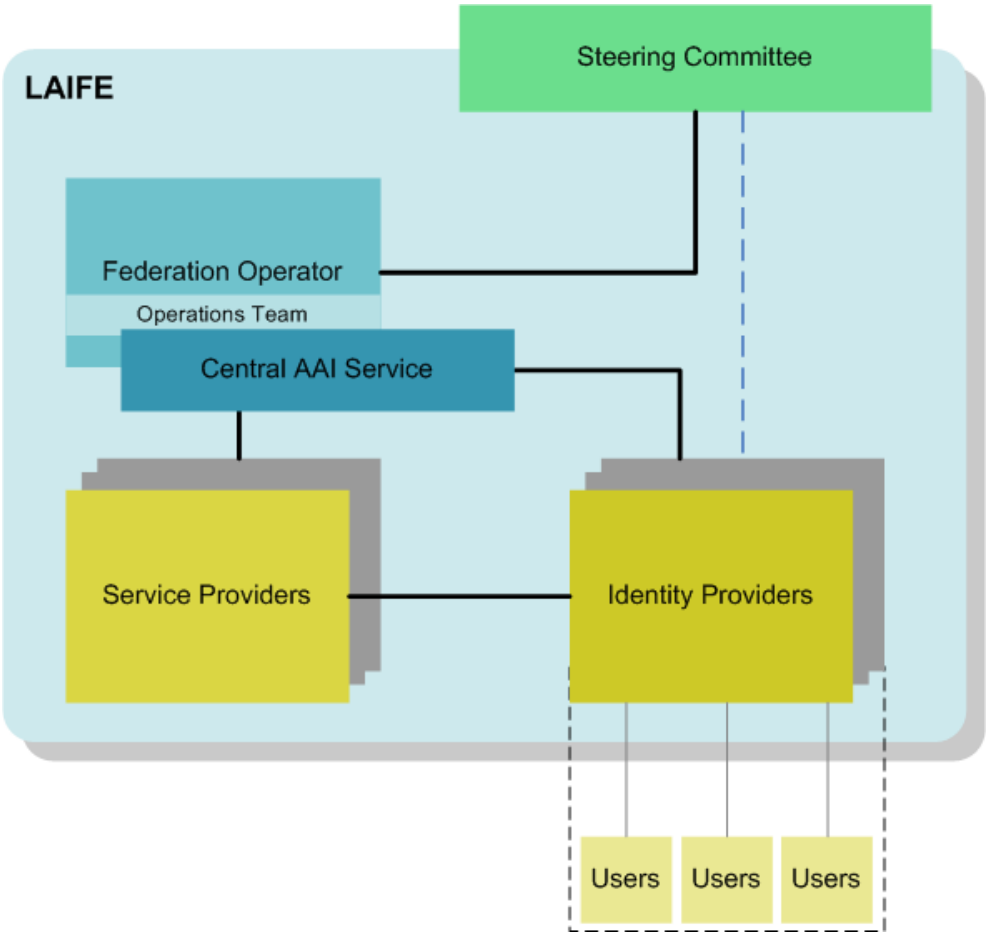

Chart 1: The structure of LAIFE

3.2.1. Federation operator

University of Latvia Information Technology Department (hereinafter – UL IT) provide the service of LAIFE. UL IT is the first and principal Member of LAIFE.

3.2.1.1. Rights and obligations

As the provider of the federative service, the UL IT commits itself to:

1. provide the central infrastructure, as described in the Technical Policy;
2. provide and maintain the federative service;
3. in the case of temporary unavailability or possible malfunctioning of the central infrastructure carry out the repairs as quickly as possible;
4. put the service provision on hold, with regard to Member which does not comply with the contractual obligations;
5. comply with the legislation on the processing of personal data;
6. act as the Identity Provider for the end users of the University of Latvia;
7. terminate the agreement with regard to a party, which does not comply with an essential contractual obligation, if approved by the LAIFE Steering Committee;

3.2.2. Steering Committee

The governance of LAIFE is supervised by the LAIFE Steering Committee, which is appointed by the UL IT and the Institute of Mathematics and Computer Science, University of Latvia (hereinafter – IMCS UL): each institution delegates two representatives for a period of up to 2 years.

3.2.2.1. Rights and obligations

LAIFE Steering Committee commits itself to:

1. alter the technical minimum requirements in the Technical Policy at any time;
2. alter the LAIFE Policy at any time;
3. in the case of policy breach issue a formal notification of impending revocation, including an adequate time limit for rectification.

3.2.3. Operations Team

The operational management of LAIFE is assigned to the LAIFE Operations Team which is appointed by the Federation operator. Information about the team members and other contact information are published on LAIFE's web site.

3.2.3.1. Rights and obligations

LAIFE Operations Team commits itself to:

1. act as a support line for support requests from LAIFE Members. Members of LAIFE MUST NOT redirect end user queries directly to the LAIFE Operations Team but MUST make every effort to ensure that only relevant problems and queries are sent to the LAIFE Operations Team.
2. evaluate each Membership application, the evaluation process involves checking, if the applying organization fulfills the requirements of the LAIFE policy;
3. communicate acceptance or denial of the Membership application to the applying organization in written form, including the reason for denying the application (if applicable);
4. maintain LAIFEs website http://laife.lanet.lv:
    a. maintain a list of LAIFE Members;
    b. publish relevant information on any interfederation agreements;
    c. publish online (http://laife.lanet.lv) all decisions made by the LAIFE Steering Committee.
5. duly inform all Members of LAIFE about downtimes caused by adaptations and upgrades of the federative service;
6. duly notify by e-mail all Members of LAIFE about changes in the Technical or LAIFE Policy;

3.2.3. Identity Provider

Identity Provider is a Member of LAIFE authorized to provide the Identity Management of its users (see 3.2.5 LAIFE users)

Identity Management is the process by which Identity Providers first issue and then manage identities throughout their life-cycles and by which they also make claims of identity for subjects (e.g. individuals, resources and other objects). A claim of identity is an electronic representation, using a specific identity management technology, of a set of attributes identifying a subject.

In order to become an Identity Provider in LAIFE an organization MUST be a legal entity established as a non-profit organization which MAY carry out research or technological development as one of its main objectives (such as: universities, institutes of further education, research institutes, schools (primary and secondary), libraries, museums, archives, cultural institutions, hospitals, government departments).

3.2.3.1. Rights & obligations

The Identity Provider commits itself to:

1. sign the LAIFE membership agreement;
2. inform the LAIFE's Operations Team immediately, and in writing, of every alteration with regard to the information provided in 1;
3. accept the technical minimum requirements in the Technical Policy of LAIFE.
4. obtain the end user's unambiguous permission to process his/her personal data and to exchange these with Service Providers of LAIFE;
5. keep the data of the attributes concerning the end users complete and up to date;
6. guarantee the safe proceeding of the exchange of data;

7. safeguard UL and IMCS UL against claims which are filed by other Members of LAIFE or third parties, or against disputes which are taken up by other Members of LAIFE or third parties with regard to this Policy.
8. be responsible for fulfilling the requirements of applicable laws with respect to its own end users.

3.2.4. Service Provider

Service Provider is a Member of LAIFE authorized to provide services to the users of LAIFE (see 3.2.5 LAIFE users).

Thanks to the federative service, it is not necessary for the Service Providers to store or manage the identity data, which has been forwarded by the Identity providers.

3.2.4.1. Rights and obligations

The Service Provider commits itself to:

1. sign the LAIFE membership agreement;
2. accept the technical minimum requirements in the Technical Policy of LAIFE.
3. respect the intellectual rights (including the copyrights, neighboring rights, databank right, trademark right, drawing and model right, ...) and rights of third parties (amongst others the right of respect and protection of privacy, the publishing rights of the creators of personal likenesses, slander and libel, ...) applicable to the services;
4. provide content that serves academic or research goals;
5. safeguard UL and IMCS UL against claims filed by other Members of LAIFE or third parties, or against disputes which are taken up by other Members of LAIFE or third parties with regard to this Policy.

3.2.5. LAIFE users

LAIFE users are individuals with an employment, student or other form of association with the LAIFE Member institution (Identity Provider).

4. LAIFE Membership procedures

4.1. How to become a Member

In order to become a Member of LAIFE an organization formally applies for membership. If the application is accepted by the Operations Team, the organization becomes a Member by signing the LAIFE membership agreement.

Detailed information and Membership agreements are published on LAIFE website.

4.2. Membership cancelation

LAIFE member MAY cancel an LAIFE membership at any time by sending a written request to the LAIFE Operations Team.

4.3. Membership revocation

LAIFE Member who fails to comply with the Policy MAY have its Membership revoked by UL IT (if approved by the LAIFE Steering Committee).

If LAIFE Operations Team is aware of a breach of policy by a Member, the LAIFE Operations Team MAY issue a formal notification of concern. If the cause for the notification of concern is not rectified within the adequate time specified by LAIFE Operations Team, LAIFE Steering Committee MAY issue a formal notification of impending revocation, including an adequate time limit specified by LAIFE Steering Committee for rectification of the breach by the Member, after which LAIFE Steering Committee MAY approve the revocation of LAIFE Membership.

5. Confidentiality

The parties commit themselves to treat information, which is presented to them within the framework of the federative service, with the necessary discretion. The parties commit themselves, both during and after the execution of the assignment, to keep under cover all confidential information, of whatever nature, which would be provided to them, or with which they would become acquainted within the framework of this federative service. No single data may be used for any other purpose than indicated in this Policy.

6. Liability

Neither the UL nor IMCS SHALL be liable for damage caused to the federation member or its end user. LAIFE Members SHALL not be liable for damage caused to the UL or IMCS UL due to the use of the LAIFE services, service downtime or other issues relating to the use of the LAIFE services.

The LAIFE Member is REQUIRED to ensure compliance with applicable laws. The UL or the IMCS UL SHALL NOT be liable for damages caused by failure to comply with any such laws on behalf of the LAIFE member or its end users relating to the use of the federation services.

The LAIFE Operations Team and the LAIFE Member SHALL refrain from claiming damages from other LAIFE Members for damages caused by the use of the LAIFE services, service downtime or other issues relating to the use of the LAIFE services. Neither party SHALL be liable for any consequential or indirect damage.

None of the parties will be responsible for the delay or shortcoming in the execution of the commitments of this agreement, if such a delay or shortcoming is caused by

force majeure. Force majeure points to all occurrences which are independent of the will of the parties, such as e.g. strike, war, revolt or destruction of the machines.

7. Protection of personal data

The parties commit themselves to execute the processing of the personal data needed for the working of LAIFE, in compliance with the law for the protection of privacy (in relation to the processing of personal data), and as altered by later and future legislation.