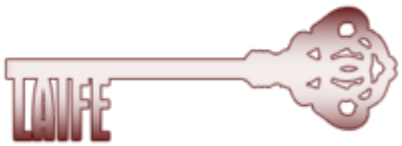

Document	LAIFE Federation Policy
Identifier	https://www.laife.lv/policy
Version	V2.0
Last modified	20.04.2023
Pages	5
Status	FINAL
License	Creative Commons BY-SA 3.0

LAIFE Federation Policy

1 Terminology

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 (http://www.ietf.org/rfc/rfc2119)

1.1 Definition of terminology

Subject: Any natural person affiliated with a LAIFE Member, e.g., as a teacher, researcher, staff, or student.

Identity Provider (IdP): The system component that issues Attribute assertions on behalf of Subjects who use them to access the services of Relying Party.

Relying Party (RP): A Service that relies upon a Subject's credentials, typically to process a transaction or grant access to information or a system. Also known as a Service Provider (SP).

2 Introduction

The Latvian Academic Identity Federation (LAIFE) facilitates and simplifies shared services across the Identity Federation. This is accomplished by using Federation Technologies to extend the scope of a Digital Identity issued by one Member of the Federation to be trusted across the whole Federation.

This Policy defines the Federation by defining the procedures and practices which allows participating organisations to use available Federation Technologies for digital identification. This Policy does not directly describe practices or procedures specific to any choice of Federation Technology.

Identity Management are the processes by which Identity Providers issue and manage digital identities throughout their lifecycles and by which they also make Claims of identity. A Claim of identity is a digital representation, using a specific identity management technology, of a set of attributes identifying a Subject. The LAIFE Policy has three main parts:

- this document which describes governance, membership, and scope.
- a set of Identity Assurance Profiles.
- a set of Federation Technology Profiles.

The Identity Assurance Profiles and the Federation Technology Profiles are based on current and evolving standards and are described in separate documents.

An Identity Assurance Profile describes levels of trust in claims and organisations. An Identity Assurance Profile allows a Relying Party to determine the degree of certainty of the identity of a Subject and its personal data. Identity assurance is to a large extent independent of the technology used to convey Claims of identity.

The Federation Technology Profiles describe concrete realisations of the Policy and Assurance Profiles in terms of specific technologies (e.g., SAML2, OpenID Connect or eduroam).

3 Purpose and Scope

The purpose of LAIFE is to make it possible for Relying Parties to provide services to Subjects in the Federation. 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, research hospitals, government agencies and private sector organisations involved in higher education and research.

The scope of the LAIFE Policy is limited to those technologies which can support federated secure authentication and authorisation of Subjects as described by the Federation Technology Profiles. The set of procedures and practices described in this document applies equally to all Federation Technology Profiles of LAIFE.

To facilitate collaboration across national and organisational borders LAIFE SHOULD actively participate in interfederation agreements (e.g., eduGAIN or cross sector interfederations).

4 Governance and Roles

4.1 LAIFE Board

LAIFE is operated by the Society "Higher Education and Science IT Shared Service Centre" (VPC). VPC Board governs LAIFE federation and serves as LAIFE federation board (LAIFE board). Information about the LAIFE board members is published on the LAIFE web site (https://www.laife.lv).

Any changes to the LAIFE Policy MUST be approved by the LAIFE Board, published on the LAIFE website, and communicated to the LAIFE Members.

All decisions made by the LAIFE Board are public.

VPC is responsible for maintaining formal ties with relevant national and international organisations.

4.2 LAIFE Operations Team

The LAIFE Operations Team is appointed by LAIFE board. The chair of the LAIFE Operations Team is the federation operation manager and is appointed by LAIFE board.

Information about the team members and other contact information is published on the LAIFE website.

The LAIFE Operations Team is responsible for:

- the daily operations of the LAIFE federation;
- the development of the LAIFE federation including the LAIFE Policy Framework and operational tools;
- maintaining and publishing a list of LAIFE Members including approved Identity Assurance Profiles and implemented Federation Technology Profiles of each Member.

The LAIFE Operations Team acts as a third line support for support requests from the second line support of LAIFE Members. Members MUST NOT redirect Subjects to the LAIFE Operations Team.

4.3 LAIFE Member

To be an Identity Provider in LAIFE an organisation MUST be a Member of LAIFE. Federation Technology Profiles MAY impose additional requirements on LAIFE Members.

A Relying Party is not required to become a Member of LAIFE to consume identity information from LAIFE Identity Providers. Federation Technology Profiles MAY impose additional requirements on Relying Parties.

All education and scientific institutions which are registered in Latvia and meets LAIFE policies are allowed to become a LAIFE Member. An organisation not connected to education and research field under special circumstances MAY become a LAIFE Member by decision of LAIFE board. An organisation becomes a Member of LAIFE by applying for membership according to the process of Membership Application described in this document.

Members operating Identity Providers will in most cases have Subjects associated with them: these are individuals with an employment, student, business, or other form of association with the Member. Each Member is responsible for its own Subjects. Each Member is responsible for fulfilling the requirements of the Latvian personal data protection legislation with respect to its own Subjects.

Members are responsible for first line (e.g., call centre or equivalent) and second line (technical support and problem classification) support for its Subjects. Membership in LAIFE does not mandate any specific service level for this support.

All LAIFE Members and their Subjects MUST fulfil one or more of the LAIFE Identity Assurance Profiles.

5 Identity Management Practice Statement

Each LAIFE Member with an Identity Provider MUST create and maintain an Identity Management Practice Statement.

The Identity Management Practice Statement is a description of the Identity Management lifecycle including how Subjects are enrolled, maintained, and removed from the identity management system based on the Identity Assurance Profiles.

The Identity Management Practice Statement is audited against claims of compliance with Identity Assurance Profiles.

6 Procedures

6.1 Membership application

To become a Member of LAIFE an organisation MUST formally apply for membership. Detailed information and application forms are published on the LAIFE website.

For organisations with an Identity Provider the Membership Application MUST include an Identity Management Practice Statement.

Each Membership Application is evaluated by the LAIFE Operations Team against the LAIFE Policy Framework. The LAIFE Operations Team presents a recommendation for membership with an evaluation report to the LAIFE Board. LAIFE board approve or deny the membership request.

The LAIFE Operations Team communicates the decision of the LAIFE Board to the applying organisation.

6.2 Membership cancellation

A LAIFE membership MAY be cancelled by the LAIFE Member at any time by sending a request to the LAIFE Operations Team. A cancellation of the LAIFE membership implies the automatic and immediate cancellation of the use of all Federation Technology Profiles for the organisation.

6.3 Membership revocation

A LAIFE Member who fails to comply with the LAIFE Policy Framework SHOULD have its membership in LAIFE revoked by the LAIFE Board. Under special circumstances LAIFE Board MAY revoke membership with LAIFE Board decision.

If the LAIFE Operations Team is made aware of a breach of LAIFE Policy Framework by a LAIFE Member, the LAIFE Operations Team SHALL issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the LAIFE Operations Team, the LAIFE Board SHALL issue a formal notification of impending revocation after which the LAIFE Board SHOULD revoke the membership. If the LAIFE Policy breach is severe, LAIFE Operations Team MAY temporarily revoke the membership under the revocation dispute process.

A revocation of the LAIFE membership implies the automatic and immediate revocation of the use of all Federation Technology Profiles for the organisation.

7 Audit

Identity Assurance Profiles and Federation Technology Profiles MAY impose audit of compliance on LAIFE Members.

8 Fees

VPC board will decide on yearly fees for LAIFE Members which will cover the operational costs of LAIFE. This decision MUST be made no later than November 1 each year or the fees will default to the fees from the previous year.

9 Liability

Neither the LAIFE Operations Team nor the LAIFE Board SHALL be liable for damage caused to the LAIFE Member or its Subjects. LAIFE Members SHALL NOT be liable for damage caused

to the LAIFE Operations Team or the LAIFE Board due to the use of the LAIFE federation services, service downtime or other issues relating to the use of the LAIFE federation services.

LAIFE Members and Relaying parties are REQUIRED to ensure compliance with the Latvian Personal Data Protection and Latvian Cyber security Regulation. The LAIFE Operations Team or the LAIFE Board SHALL NOT be liable for damages caused by failure to comply with this law on behalf of the LAIFE Member or its Subjects relating to the use of the federation services.

For any other damage, the liability for damages in case of a breach is limited to one thousand (1000) euros. The LAIFE Operations Team and LAIFE Members SHALL refrain from claiming damages from each other for damages caused using the LAIFE federation services, downtime or other issues relating to the use of the LAIFE federation services.

Neither party SHALL be liable for any consequential or indirect damage.