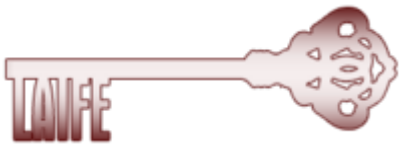

Document	LAIFE Identity Assurance Profile Level 1
Identifier	https://www.laife.lv/policy/assurance/al2
Version	V2.0
Last modified	20.04.2023
Pages	10
Status	FINAL
License	Creative Commons BY-SA 3.0

LAIFE Identity Assurance Profile Level 2

1 Terminology and Typographical Conventions

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)

Text in *Italics* is non-normative. All other text is normative unless otherwise stated.

All normative parts of the profile are governed by the LAIFE Board.

The non-normative (guidance) is maintained by the LAIFE Operations team.

Text in green shows where there is a difference between LAIFE Identity Assurance Level 2 Profile and LAIFE Identity Assurance Level 1 Profile.

LAIFE has multiple assurance level profiles. All Identity Assurance Profiles share the same numbering scheme.

1.1 Definition of terminology

Member Organisation: The LAIFE Member with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

Service Owner: An organisation that is responsible and liable for operating a service registered in LAIFE. The Service Owner may delegate the technical operation of the Relying Party to another organisation.

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).

Shared secret: A piece of information that is shared exclusively between the parties involved in a secure communication.

Credential: A combination of information, cryptographic software and/or cryptographic hardware which a Subject proves possession of to authenticate itself in the Member Organisation's Identity Provider. For example, this can be the combination of a username and password or a username and cryptographic device.

Credential issuing: The process of issuing a Subject a set of credentials which the Subject use to authenticate itself in the Member Organisation's Identity Provider. This also includes the process when a Member Organisation issues an additional set of credentials to the same Subject.

Credential re-issuing: The process where a Member Organisation re-issues credentials to a Subject who has previously been issued credentials, i.e., by replacing a malfunctioning cryptographic device or by giving a Subject the possibility to reset a forgotten password.

Credential renewal: The process where a Subject voluntary change his or her credentials by proving possession of the current credentials, i.e., changing a password by proving knowledge of the current password.

Credential revocation: The process where a Member Organisation invalidates a set of credentials currently issued to a Subject, i.e., because the credentials are suspected to be compromised or if he or she is no longer a current Subject of the Member Organisation.

CAPTCHA: A challenge-response test used as an attempt to ensure that the response is generated by a human being, e.g., a picture with characters that a Subject must retype in a text field.

2 Purpose, Scope and Summary

This document defines the LAIFE Identity Assurance Level 2 Profile. This profile is an extension of the LAIFE Identity Assurance Level 1 Profile.

Metadata registration requirements, SAML Keys and Certificates, Endpoint security, Identity Provider software requirements, Operational Requirements for Relying Parties, Federation Operator, Operational Requirements for Federation Operator, SAML Federation Metadata signing and Metadata publishing is described in Assurance profile 1 and is not doubled in this document.

A claim at this Identity Assurance Profile implies the following:

- the subject is affiliated with the Member Organisation;
- the subject is an identified natural person;
- the subject is identified by a unique permanent user identifier; and
- the Member Organisation is responsible for the attributes/information released.
- the authentication of the subject optionally is a multi-factor authentication.

Relying parties in LAIFE may require elevated levels of assurance.

This Identity Assurance Profile is conditionally mappable to but not interchangeable with REFEDS Assurance Framework ver 1.0.

This Identity Assurance Profile is similar to but not interchangeable with the following assurance level profiles:

- Requirements for enhanced security systems (Regulations number 442 issued on 28.07.2015 of Cabinet of Ministers of Republic of Latvia https://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam)
- Level of Assurance 1 in the sense of ISO/IEC Entity authentication assurance framework (ISO/IEC 29115:2013 https://webstore.iec.ch/preview/info_isoiec29115%7Bed1.0%7Den.pdf);
- Assurance Level 2 in the sense of Kantara Initiative Identity Assurance
- Framework: Service Assessment Criteria (Kantara IAF-1400-SAC https://kantarainitiative.org/download/6182/); and

- Level of Assurance 2 in the sense of NIST Electronic Authentication Guideline (NIST SP 800-63-3 https://pages.nist.gov/800-63-3/).

3 Compliance and Audit

The purpose of this section is to define how to ensure compliance with this technology profile.

3.1 Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement, maintained as a part of the LAIFE membership process. The Identity Management Practice Statement MUST describe how the organisation fulfils the normative parts of this document.

3.2 LAIFE Operations, or another party approved by LAIFE Board, conducts an audit of the submitted Identity Management Practice Statement.

The Member Organisation MUST annually confirm that their Identity Management Practice Statement is still accurate.

The Member Organisation MUST submit an updated Identity Management Practice Statement for renewed audit prior to making changes in the identity management process or technology that makes the Identity Management Practice Statement inaccurate.

Guidance: LAIFE Operations supplies a template for the Identity Management Practice Statement.

3.3 For Relying Parties, Service Owners MUST annually confirm that the Relying Party is operational and fulfils this Technology Profile.

3.4 LAIFE Board MAY impose an additional audit of the Member Organisation or Service Owner performed by LAIFE Operations team, or another party approved by LAIFE Board.

4 Organisational Requirements

The purpose of this section is to define conditions and guidance regarding participating organisations and their registered entities.

4.1 Identity Providers

Registration criteria

4.1.1 Organisation to be eligible to register as an Identity Provider in LAIFE federation the organisation MUST be a member of the LAIFE Identity Federation.

4.1.2 All Member Organisations MUST fulfil one or more of the LAIFE Identity Assurance Profiles to be eligible to have an Identity Provider registered in LAIFE metadata.

4.1.3 Each Member Organisation MUST publish the Acceptable Use Policy to all Subjects including all additional terms and conditions.

4.1.4 All Subjects MUST indicate acceptance of the Acceptable Use Policy before use of the Identity Provider.

4.1.5 The Member Organisation MUST have documented procedures for data retention and protection to ensure the safe management of Subject information.

Deregistration

4.1.3 An Identity Provider no longer fulfilling the registration criteria in 4.1.1 and 4.1.2, MUST be deregistered from LAIFE.

Incident Management

4.1.4 All Member Organisations MUST follow the LAIFE Incident Management Procedure in case of a suspected security incident if

- the Identity Provider is at risk; or
- at least one user with federated logins is at risk or involved.

4.2 Relaying Parties (Service Providers)

Registration criteria

4.2.1 A Relying Party is eligible for registration in LAIFE if they are:

- a service owned by a Member Organisation;
- a service under contract with at least one Member Organisation;
- a government agency service used by at least one Member Organisation;
- a service that is operated at least in part for the purpose of supporting research and scholarship interaction, collaboration, or management; or
- a service granted special approval by VPC Board after recommendation by LAIFE LAIFE Operations Team.

4.2.2 For a Relying Party to be registered in LAIFE the Service Owner MUST accept the LAIFE Metadata Terms of Access and Use.

Deregistration

4.2.3 If a Relying Party no longer fulfils the registration criteria in 4.2.1 and 4.2.2, it MUST be deregistered from LAIFE.

Incident Management

4.2.4 All Service Owners MUST follow the LAIFE Incident Management Procedure in case of a suspected federated security incident if:

- the Relying Party is at risk; or
- at least one user with federated login is at risk or involved.

4.3 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

4.3.1 The Member Organisation MUST maintain a log of all relevant security events concerning the operation of the Identity Provider and the underlying systems, together with an accurate record of the time at which the event occurred (timestamp). These records MUST be retained with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organisational policy.

Guidance: *Audit trails are sensitive personal data and must be protected from unauthorised access. A separate log-server is recommended as best practice but not mandatory. All changes to credentials and attributes used in LAIFE must be logged.*

5 Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.

Language attributes (lang)

All metadata elements where language is relevant, i.e., MDUI/UIInfo and organisational elements, should include languages useful for the Identity Provider's users.

5.1.1 The Identity Provider MUST authenticate Subjects at the request of the Relying Party. The authentication MUST be performed using either Single-Factor Authentication or Multi-Factor Authentication.

Single-Factor Authentication of Subjects MUST be performed using either:

- a memorised secret as defined in NIST 800-63B, i.e. a password or a passphrase with at least 24 bits of entropy as defined in (the old) NIST SP 800-63-2;
- a Single-Factor Cryptographic Software as defined in NIST 800-63B;
- a Single-Factor Cryptographic Device as defined in NIST 800-63B;
- a full Multi-Factor OTP Device as defined in NIST 800-63B;
- a full Multi-Factor Cryptographic Software as defined in NIST 800-63B; or
- a full Multi-Factor Cryptographic Device as defined in NIST 800-63B

Optional Multi-Factor Authentication of Subjects MUST be performed using a full Multi-Factor (as defined above) or using a memorised secret (or an inherent authentication factor) in combination with either:

- a Single-Factor OTP Device as defined in NIST 800-63B;
- a Single-Factor Cryptographic Software as defined in NIST 800-63B; or

- a Single-Factor Cryptographic Device as defined in NIST 800-63B.

All factors used to perform a combined Multi-Factor authentication MUST be independent.

A Subject MAY have more than one valid set of credentials, e.g. a memorised secret and one or more Single-Factor Cryptographic Devices.

5.1.2 Subjects MUST be actively discouraged from sharing credentials with other subjects either by using technical controls or by requiring users to confirm policy forbidding sharing of credentials or acting in a way that makes stealing credentials easy.

Guidance*: A strong recommendation is that the Acceptable Use Policy or Password Policy explicitly forbids Subjects to share their credentials with other subjects or re-use their memorised secrets in other systems.*

5.1.3 The organisation MUST take into account applicable system threats and apply appropriate controls to all relevant systems.

Guidance: *Example of system threats are:*

- *the introduction of malicious code;*
- *compromised authentication arising from insider action;*
- *out-of-band attacks by other users and system operators;*
- *spoofing of system elements/applications; and*
- *malfeasance on the part of Subscribers and Subjects.*

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

5.2.1 Each Subject assertion MUST include a unique representation of one or more administrative domain(s) owned by the Member Organisation or which the Member Organisation has delegated usage of.

Guidance: *Normally the DNS top level domain of the Member Organisation is used to provide scope to all scoped attributes, e.g., eduPersonPrincipalName and eduPersonScopedAffiliation.*

5.2.2 Each Identity Provider instance MUST have a globally unique identifier

Guidance: *ALL LAIFE technology profiles fulfil this requirement, for example entityID in SAML and radius server DNS name in eduroam.*

5.2.3 Each Subject MUST be represented by one or more globally unique identifiers. Subject identifiers MUST NOT be re-assigned.

Guidance: *Multiple Subject identifiers (i.e. usernames) for the same Subject can be used to represent different affiliations (for example both employee and student) at the same Member Organisation.*

5.2.4 If the Subject have more than one unique identifier within the Identity Provider the Subject MUST be able to choose which one to be used at login.

5.2.5 The Member Organisation MUST maintain a record of all changes regarding Assurance Level of Subjects.

5.2.6 The Subject MUST be able to update stored self-asserted personal information.

Guidance: *This follows by the General Data Protection Regulation (EU) No 679/2016, i.e., if the Subject has provided a private email address, he/she must be able to update it.*

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

5.3.1 All Subjects MUST be allowed to renew their credentials.

5.3.2 Subjects MUST actively demonstrate possession of current credentials in the process of credential renewal.

Guidance: *Single sign-on authentication should be disabled during the credential renewal process.*

5.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

5.4.1 The Member Organisation MUST be able to revoke a Subject's credentials either by request by the Subject or by decision from the Member Organisation.

Guidance: *Possible reasons for revocation can be, for example, by request of the Subject, Subject leaving the Member Organisation or security related incidents.*

5.4.2 In the event of a Credential Revocation caused by a security related incident the Member Organisation MUST take precautions to prevent the incident from reoccurring.

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.5.1 The Member Organisation MUST maintain a record of all credentials issued.

Guidance: *All changes, such as password changes and/or new/closed credentials shall be stored in accordance with Latvian legislation.*

5.5.2 The Identity Provider MUST have an availability that allows the Member Organisation to use it for internal systems.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.

5.6.1 The Identity Provider MUST provide validation of credentials to a Relying Party using a protocol that:

1. requires authentication of the specified service or of the validation source;

2. ensures the integrity of the authentication assertion;

3.protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture; and which, specifically:

4.creates assertions which are specific to a single transaction;

5.where assertion references are used, generates a new reference whenever a new assertion is created;

6.when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion; and

7.requires the secondary authenticator to:

1.be signed when provided directly to Relying Party, or;

2.have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).

5.6.2 The Identity Provider MUST not authenticate credentials that have been revoked.

5.6.3 The Identity Provider MUST force the Subject to demonstrate possession of current credentials in the process of authentication.

5.6.4 The Identity Provider MUST force the Subject to authenticate at least once every 12 hours to maintain an active session.

Guidance: *This means that Single Sign-On sessions must not be valid for more than 12 hours. This balances user experience against security risks.*

6 Conformity, Syntax and Technical representation

Authentication at this Identity Assurance Profile MUST NOT be asserted unless the following criteria are met:

- the Member Organisation is approved at this Identity Assurance Profile, or higher, by the LAIFE Board;
- the Subject has been identity proofed at this Identity Assurance Profile, or higher; and
- all Credentials used during the authentication are issued at this Identity Assurance Profile, or higher.

A Subject fulfilling this Identity Assurance Profile also fulfils LAIFE Identity Assurance Level 1 Profile. The Identity Provider SHOULD assert LAIFE Identity Assurance Level 1 Profile compliance.

Syntax and Technical representation of conformity with this Identity Assurance Profile are defined in the LAIFE Technology Profiles.