FEDURUS

Identity Federation Policy

Authors	Andrey Sokolov, Rustam Usmanov
Last Modified	07-08-2018
Version	0.2.2

Table of Contents

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 on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. 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.
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.

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 FEDURUS Identity Federation (the Federation) is introduced to facilitate and simplify the introduction 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.

The FEDURUS Identity Federation founded by ARLICON Association without the formation of a separate legal entity.

The Federation Policy document defines the Federation by defining the Federation Members' obligations and rights to be able to 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.

3   Governance and Roles

3.1   Governance

The FEDURUS Identity Federation is governed by the Nonprofit Partnership "Associated Regional Library Information Consortia" (NPP "ARLICON") performs the functions of organizing secure authentication for organizations that become Members of the Identity Federation, with access to protected resources and services of scientific and educational networks and the Internet.

Information about the Nonprofit Partnership "Associated Regional Library Information Consortia".
Nonprofit Partnership "Associated Regional Library Information Consortia" (NPP "ARLICON")
Location: 29, Politekhnitcheskaya str., St.Petersburg, 195251, Russia
Legal address: 29, Politekhnitcheskaya str., St.Petersburg, 195251, Russia
Tel: +7 (812) 552 7654

In addition to what is stated elsewhere in the Federation Policy the ARLICON is responsible for:
- Setting criteria for membership for the Federation.
- Deciding whether to grant or deny an application for membership in the Federation.
- Deciding whether a Federation Member is entitled to act as Home Organization.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Defining future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Deciding entering into interfederation agreement.

- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Address financing of the Federation.
- Approves the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

3.2 Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, the 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 center 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.
- Prepares and presents issues to the ARLICON and acts as the secretary of the ARLICON meetings.
- 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.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator 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.

3.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in the Federation Policy 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.
- Must pay the fees. Prices and payment terms are specified in Appendix 3.
- 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.

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. Specific requirements may be imposed by Level of Assurance Profiles.
- 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 Home Organization or Attribute Authority, it:

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

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

Legal entities - educational organizations of higher education, scientific organizations and organizations of additional professional education are eligible to become a Member of FEDURUS Identity Federation and are allowed to operate as a Home Organization, and also as a Service Provider.

Legal entities - other organizations that carry out their activities in the interests of educational and scientific organizations are allowed to become a Member of FEDURUS Identity Federation in the role of Service Provider.

Legal entities are able to join or leave the Federation by applying to the Federation Operator. Participation to the Federation requires the agreement with this Federation Policy and compliance with the terms and conditions presented herein that arise from it.

The minimal technical requirements for being able to be affiliated to the FEDURUS Infrastructure are described in the Technology Profile. The Federation Operator reserves the right to alter the Technology Profile at any time. The alterations are published on the website of the Federation and come into effect **two months** after their notification via e-mail by the Federation Operator.

5 Procedures

5.1 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 the Terms of Service Agreement (Appendix 1. of the Federation Policy).

Each applicant for membership shall fill out an Application Form (Appendix 2. of the Federation Policy), indicating in what role (with what role of the Participant) it joins the Federation.

The applicant at its own expense and on its own computer resources deploys the software under the requirements of the Technology Profile in accordance with the role of the Participant specified in the Application Form.

After deployment of the software, the Applicant Organization undergoes the procedure for verifying the correct functioning of the software by the Federation Operator with the elimination of errors identified by the Federation Operator.

After undergoing of the software verification procedure, the Applicant Organization signs the Terms of Service Agreement together with the Authority as the treaty parties, including this Federation Policy.

If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.

5.2 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 use of all Federations Technology Profiles for all Federation Members.

6 Legal conditions of use

6.1 Termination

A Federation Member who fails to comply with the Federation Policy and/or the requirements of the Technology Profiles it implements 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 specifying the period allotted to the Member for the elimination of identified breach. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, the Authority may issue a formal notification of suspension of membership and after 10 working days if the cause for the notification of concern still is not rectified the Authority can make a decision to revoke the membership.

6.2 Liability and indemnification

[Covered by Sections 6-7 of Terms of Service Agreement]

6.3 Jurisdiction and dispute resolution

FEDURUS Identity Federation is developed in accordance with the current legislation of the Russian Federation. [Also see section 5 of Terms of Service Agreement]

6.4 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.

6.5 Amendment

The Federation Operator has the right to amend the Federation Policy from time to time. Any such changes need to be approved by the ARLICON and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.

Appendix 1.

Terms of Service Agreement
(Relying to the Policy of FEDURUS Identity Federation)

NPP ARLICON №_____

"___" _____

The Nonprofit Partnership "Associated Regional Library Information Consortia" (NPP "ARLICON") (hereinafter referred to as the "Operator"), represented by Executive Director Plemnek Alexander Ivanovich acting on the basis of the Charter, on the one hand, and _____ (name of the organization) _____ (hereinafter referred to as the "Participant"), represented by _____ (position) _____ _____ (Name) _____, acting on the basis of _____ (statute or power of attorney No. ___ of 00.00.0000) _____, on the other hand, separately tee referred to as "Party" and together the "Parties", have concluded this Agreement as follows:

1. The Subject of the Agreement.

1.1. The subject of the Agreement is the accession of the Participant in the manner of Art. 428 of the Civil Code of the Russian Federation the Policy of FEDURUS Identity Federation (hereinafter referred to as the Policy). The Policy is exposed on the Operator's website at http://www.fedurus.ru.

1.2. The terms and definitions given in the Policy are applicable to the Agreement.
1.3. Signing the Agreement means that the Participant is familiar with the Policy and its appendices.
1.4. Norms contained in the Policy be come mandatory for the Participant from the moment of signing by the Parties this Agreement. The parties agree that they accept the conditions of the Policy completely without any reservations, exceptions, changes and protocols of disagreements.
1.5. In accordance with the provisions of the Policy, the Operator provides the Service to the Participant (hereinafter - Services):
1.5.1. on the organization of authorization of employees and students of the Participant when accessing the protected resources of scientific and educational computer networks (if the Participant chooses the IdP service).
1.5.2. on the organization of interaction with other legal entities - users of scientific and educational computer networks in the authorization of their employees and students to access the protected resource of the Participant (in case the SP participant selects the service).
1.6. The composition and quantity of the Services is determined by the Participant and is formalized in the form of an Application for accessing the Policy (Appendix 2 to the Policy).

2. Rights and Obligations of the parties.

2.1. The rights and obligations of the Parties are determined by the current legislation of the Russian Federation, this Agreement and the Policy.
2.2. The Operator provisions the Service to the Member in accordance with the procedure provided for by the Policy in accordance with the selected type(s) of Service(s).
2.3. The Participant undertakes to carry out the works listed in the Policy for delivery the Services.

3. Term of the agreement.

3.1. This Agreement is considered concluded and comes into force from the moment it is signed by the parties and is valid for 12 calendar months.
3.2. The Parties have the right to early termination of the Agreement by sending a written notice at least 30 (thirty) calendar days before the date of termination.

4. Ensuring confidentiality.

4.1. The Operator and the Participant guarantee the confidentiality of the information that has become known to them during the implementation of this Agreement.

5. The order of disputes resolution.

5.1. In case of disputes between the Operator and the Participant on the issues stipulated by this Agreement or in connection with it, the Parties take measures to resolve them through negotiations.
5.2. The analysis of conflict situations related to the delivery of services of the Identity Federation is carried out within the procedures of the Policy.
5.3. If it is impossible to resolve disputes by negotiation, these disputes are subject to resolve by the Moscow Arbitration Court.

6. Responsibility of the parties.

6.1. For failure to deliver or improper delivery of obligations under this Agreement, the Parties have a responsibility within the amount of the proved real damage caused to the Party by non-delivery or improper
Delivery of obligations by the other Party. Neither Party shall be liable for lost revenue (loss of profit) that the other Party would receive.
6.2. In case of non-fulfillment or inadequate performance by the Participant of the requirements set in the Policy, compensation for losses incurred as a result of this is the responsibility of the Participant.
6.3. The operator is not liable for the consequences arising from the violation of the provisions of the Policy by the Participant.

7. Circumstances of force majeure.

7.1. The parties are exempted from liability for partial or complete default of obligations under this Agreement, if improper performance by the Parties of obligations is caused by circumstances of force majeure, i.e. extraordinary and unavoidable circumstances beyond reasonable control. A party that is unable to
fulfill its contractual obligations shall immediately inform the other party in writing about the beginning and termination of the above circumstances, but in any case not later than 14 (fourteen) calendar days after the commencement of their operation. The untimely notification of the circumstances of force majeure deprives the relevant party of the right to release from contractual obligations due to the circumstances mentioned.
7.2. A party that has suffered losses due to force majeure circumstances may require the Party, which became the object of force majeure circumstances, to document the extent of the events that occurred, as well as their impact on the fulfillment of obligations under this Agreement.
7.3. If these circumstances last more than one (1) month, each party has the right to early termination of the Agreement, with a warning to the other party for 10 (ten) calendar days.

8. Final provisions.

8.1. The Agreement is made in 2 (two) copies, identical in content and having equal legal force, one for each Party.
8.2. On the change of the actual or legal address and bank details, the Parties shall notify each other in writing within 10 (ten) days from the date (s) of the occurrence of such changes.

9. Requisites and signatures of the parties.

Operator

_____

Participant

_____

Appendix 2.

FEDURUS Identity Federation Application Form

To Federation Operator of FEDURUS Identity Federation
(name of the Applicant Organization) _____ is willing to enter membership of the FEDURUS Identity Federation and is ready to be bound by Federation Policy with signing The Terms of Service Agreement with the appendices.

1	Full name of organization	
2	Abbreviated name of the organization	
3	Organization website URL	
4	Tax ID	
5	Tax ID /sec	
6	OGRN	
7	Region (at the legal address)	
8	Legal address	
9	Legal address index	
10	Mailing address	
11	Postal address index	
12	Phone number	
13	The fully qualified domain name of the organization (unique).	
14	Canonical name of organization to be disclosed in the <md:OrganizationName> element of metadata	(to be checked with Federal Operator)
15	Name of the person responsible for administrative matters for working with the federation	
16	E--mail of the person responsible for administrative matters for working with the federation	
17	Telephone number of the person responsible for administrative matters for working with the federation	
18	Name of the person responsible for technical issues (technical support) for working with the federation	
19	E--mail of the person responsible for technical issues (technical support) for working with the federation	
20	Telephone number of the person responsible for technical issues (technical support) for working with the federation	

Organization _____ is willing to register _____ (qnt) entities

Entity №	Type of entity (SP or IdP)	entityID (an absolute URI using the http, https or urn schemes)

Name of the representative/_____

Signiture _____

Appendix 3.

FEDURUS Identity Federation Pricing

Joining Fee 25 000 ₽   One time only
Annual Fee 10 000 ₽/ year   Paid annually

The discount of 20% is provided to members of ARLICON.