RUNNetAAI

RUNNetAAI

Identity Federation Policy

Authors	Alexey Abramov Ilya Vasiliev Vasiliy Porhachev
Last Modified	30.03.2018
Version	0.3.0

Table of Contents

1 Definitions and Terminology

Authorization	Process of granting certain person rights to perform certain actions, as well as the process of verifying (and confirming) these rights when trying to perform these actions.
Attribute	Information describing the End User, characterizing her / his role in the Home Organization. The list of required and recommended attributes is given in the Technological Profile(s) and must be reflected in the Member's Identity Management Practice statement.
Authentication	Procedure for authenticating a user by comparing the secret data he entered with the data stored in the users' database.
Home organization	Organization which End User is affiliated with as employee or student. This organization is responsible for authenticating the End User and managing his Digital Identity.
Interfederation	Voluntary cooperation of two or more Identity Federations to ensure the access of End Users of one Identity Federation to the resources of Service Providers of another Identity Federation.
The authorization and authentication infrastructure	is a set of organizational, technical and legal solutions provided by the Identity Federation Operator to its Members for the authorization and authentication of the End Users.
Incident	A situation in which Service Providers need to resolve the issues of recognition or non-recognition of the authorship and/or authenticity of Digital IDs when authenticating End Users of the Home Organization - Member of the Identity Federation.
The end user	is an individual who is an employee, faculty member, researcher or student of the Home Organization and uses the resources of the Service Provider of the Identity Federation in its activity.
The Operator of the Identity Federation (Operator)	Organization that provides the Authorization and Authentication Infrastructure for the Members of the Identity Federation. Within the framework of this Policy - the Federal State Autonomous Institution "State Research Institute of Information Technologies and Telecommunications".
Identity Management Practice statement	Document adopted by the Member of the Identity Federation that defines the rules for using the account, the basic rights, duties and responsibilities of the End User with respect to the account. The account provision should describe the administrative procedures, practices and technologies used in the life cycle of the management of credentials to ensure the secure and consistent management of credentials.
Member of Identity Federation (Member)	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the framework of the Identity Federation, a Member can act as a Home Organization and/or Service Provider.
Service provider	Organization responsible for providing End users with access to their protected resources. The service provider uses Digital IDs and End User Attributes issued by Home Organizations for End User Authorization.

Identity Federation Policy	The main document of the Identity Federation, describing the principles of construction, the procedure for entry and exit of the Federation Members, and also including Technological Profile(s) that are binding on the Federation Members.
Identity Federation RUNNetAAI (AAI Federation)	An association of organizations that come together to securely exchange information as appropriate about their users and resources to enable collaborations and transactions and who have joined this Policy.
Identity Management	The process of entering, modifying (updating) and deleting data about End Users.
Digital ID (Account)	Information that identifies the End User. The Digital Identity is composed of attributes. A digital certificate is issued and managed by the Home Organization, the employee or student of which is the End User.
EduGAIN	is an association (Interfederation) of Identity Federations under the management of GEANT.

2 Introduction

An Identity Federation RUNNetAAI 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. This interaction is based on the identity management, including common policies and practices.

The Federation relies on Home Organizations 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 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 http://runnet.ru/en/services-en/runnetaai-en.

3 Governance and Roles

3.1 Governance

The RUNNetAAI Identity Federation is governed by the Federal State Institution «Scientific Research Institute for System Analysis of the Russian Academy of Sciences» (SRISA) (hereinafter referred to as The Authority) 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 Federal State Institution «Scientific Research Institute for System Analysis of the Russian Academy of Sciences (SRISA)
Reg. number 1027700384909
Address: Nakhimovsky pr., 36, bldg. 1
117218, Moscow, Russia

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:

- Management of the Federation and maintenance of central services in accordance with the procedures described in the Policy and Technological Profile(s).
- Providing technical support to the contact persons of the Members for resolving operational issues of interaction with the Operator.
- Functioning as a Federation competence center: testing software, recommending and documenting solutions, providing instructions for installing and configuring the Software and Operating Systems selected for the Federation.
- Maintaining relationships with relevant national and international operator organizations of Identity Federations, especially including contacts related to inter-federation interaction and cooperation with other Identity Federations with the goal of harmonizing information exchange.
- Promotion of ideas and concepts implemented in the Federation, to attract new members of the Federation.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator reserves the right to:

- Temporarily suspend the operation of all Identity Federation’s services to a Member of the Federation that violates safety standards when carrying out activities within the Federation.
- Publish a list of Federation Members with information on the Profiles that each Member implements to promote the Federation.
- Publish certain data of Federation Members in the context of the specific Technological Profile(s). The list of data permitted for publication is contained in the relevant Technology Profile.

3.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in the Federation Policy all Federation Members:

- Shall provide the Federation Operator with the name and contact details of the administrator for communication.
- Shall cooperate with the Federation Operator and other Federation Members in the resolution of incidents, and inform the Federation Operator of incidents, if they can adversely affect the security and reputation of the Federation as a whole and its individual Members.
- Should comply with the requirements of the Technological Profiles that the Member implements.
- Shall ensure the security of the functioning of information systems in accordance with the implemented Technological Profiles.

If a Federation Member is acting as a Home Organization, it:

- Shall create and manages the credentials of End Users, and authenticate them.
- Shall provide the Identity Management Practice statement to the Federation Operator, who in turn has the right to submit this statement to any Member of the Federation at his request.
- Shall ensure that End Users comply with the requirements of the Profiles when using Identity Federation services.
- Shall provide end-user support service on the functioning of Identity services. Home organizations should provide support for End User requests, at least during business hours at local time. Home organizations should not redirect user requests directly to the Federation Operator. Only the requests that correspond to the activities of the Federation Operator and only through the administrator of the Home Organization should be redirected to the Federation Operator.
- Shall assign the attributes to End Users, manage attributes, ensuring that they are up-to-date.
- Is responsible for providing attributes to the Service Provider.

If a Federation Member is acting as a Service Provider, it:

- Is responsible for deciding whether to grant access to SP's resource for the end user.
- May define the scope of the rights granted to the End-user.

4 Eligibility

- Legal entities - educational organizations of higher education, scientific organizations and organizations of additional professional education are eligible to become a Member of RUNNetAAI 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 RUNNetAAI Identity Federation in the role of Service Provider.

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 writing by an official representative of the organization the Terms of Service Agreement together with the Federation Policy as the appendix.
- Each applicant for membership shall fill out an RUNNetAAI Application Form, 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 Technological Profile(s) 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 and the implemented Technological Profile(s) as the appendices.
- 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 a request sending to the Federation Operator. The request shall be made in a written form addressing to the Director of the Federation Operator and signed by an authorized representative of a Member. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization within a reasonable time interval.

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 of time 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

RUNNetAAI 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 promote inter-federation cooperation, the Federation can participate in agreements with other Federations. The Participant understands and acknowledges that through Interfederative mechanisms the Participant can interact with organizations that are connected and committed to foreign laws regulating the activity of the Federations. These laws may differ from the laws governing the activities of the Federation of which he is a party.

Neither inter-federal agreements nor inter-federative information exchange, in accordance to these agreements, create for the Federation Operator and Federation Members any new obligations to operators of other Federations.

6.5 Amendment

This Policy is drawn up in writing form and is put into effect by order of the Authority. The notice on the introduction of appendices (additions) to the Policy is carried out by obligatory placement of the new edition of the Policy on the website of the Authority at the address http://runnet.ru/en/services-en/runnetaai-en. The new wording with amendments becomes mandatory for all Federation Members, including those who joined the Policy earlier than the date of the amendments (additions) coming into force.

All changes (additions) made by the Federation Operator to the Policy on their own initiative and not related to changes in the current legislation of the Russian Federation shall enter into force and become binding upon the Members of the Federation after 10 (ten) calendar days from the date of placement of the said changes and additions to the website of the Federation at the address http://runnet.ru/en/services-en/runnetaai-en.

All changes (additions) made to the Policy in connection with the change in the current legislation of the Russian Federation, come into force simultaneously with the entry into force of the amendments (additions) in these acts.