پژوهشگاه‌دانش‌های‌بنیادی (مرکز تحقیقات فیزیک نظری و ریاضیات)

INSTITUTE FOR RESEARCH IN FUNDAMENTAL SCIENCES

Iranian Identity Federation Policy

IRFED

IRANET

Authors	IPM / IRANET
Publication Date	6 – JULY - 2017
Version	1.0

License

Table of Contents

1 Definitions and Terminology 3

2 Introduction 4

3 Governance and Roles 4

3.1 Governance 4

3.2 Obligations and Rights of Federation Operator 5

3.3 Obligations and Rights of Federation Members 5

3.4 Obligations and Rights of Federation advisory group 6

3.5 Obligations and Rights of International Service Providers 6

4 Eligibility 7

5 Procedures 7

5.1 How to Join 7

5.2 How to Withdraw 7

6 Legal conditions of use 8

6.1 Termination 8

6.2 Liability and indemnification 8

6.3 Jurisdiction and dispute resolution 8

6.4 Interfederation 8

6.5 Amendment 9

7 Copyright 9

8 APPENDIX 1 9

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 *Iranian Research and Education* Identity Federation (IRFED) is introduced to facilitate and simplify the offering of shared services across the Federation. This is accomplished by using Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation.

The Federation Policy document defines the Federation by specifying procedures and 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, resources and other objects in the Federation.

The IRFED policy has three main parts:
This document (1), which describes governance, membership and scope, and a set of (federation) Technology Profiles http://www.irfed.ir/ (2). The Technology Profiles are based on current and evolving standards and best practices and are described in separate documents, available at http://www.irfed.ir/Technologies.html.
And Legal Policy Template (3) which describes the legal liability between federation members and federation operator.

The Technology Profiles describe concrete realizations of the policy in terms of specific technologies (e.g. SAML, eduroam etc.). By employing specific choices of technologies for identification and authorization this policy MAY be used to support federated identity for a wide range of applications.
Technology Profiles govern the use of federation technology.

The IRFED has also a set of membership agreement forms to be signed by participating members, available at http://www.iranet.ir/Membership.html.

The IRFED Advisory Group is a place for collaboration and sharing ideas regarding federation services and consists of representatives of federation members. Advisory Group consists of two sub-groups, Administrative Group and Technical Group.

3 Governance and Roles

3.1 Governance

The governance of IRFED is delegated to the Institute for Research in Fundamental Sciences (IPM).
IRANET (Networking division of IPM) is the Federation Operator in Iran.
The operational and legal entity for IRANET is the institute for Research in Fundamental Sciences (IPM).

IPM as IRFED governing party is responsible for:

- Setting criteria for membership for the Federation.
- Whether to grant or deny an application for membership in the Federation.
- 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.
- Entering into inter-federation agreement.

- Maintaining formal ties with relevant national and international organisations.
- Address financing of the Federation.
- Approves the fees to be paid by the Federation Members to cover the operational costs of the Federation (non-profit).
- Deciding on any other matter referred to it by the Federation advisory group.

3.2 Obligations and Rights of Federation Operator

IRANET 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 centre 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.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.

IRNAET 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.

3.3 Obligations and Rights of Federation Members

All Federation Members:

- Shall appoint and name an administrative contact and a technical contact for interactions with the Federation Operator. These contacts will become members of Advisory Group.
- 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 1.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws.

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.

- Must 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.
- 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.

3.4 Obligations and Rights of Federation advisory group

Advisory Group is constituted of federation members contact persons introduced in 3.3 and representatives of federation operator. Advisory group members:

- Should participate in group meeting at least once a year.
- Should be in contact with other members using necessary media (email, phone, …).
- Must collaborate with other members and federation operator to address any issues related to federation services functionality.
- May participate in federation technical support team. Technical support team will help new members to set up their services, and to resolve technical issues for federation services operations.

Advisory group members have the right to:

- Suggest new services to be used in federation.

3.5 Obligations and Rights of International Service Providers

In order to become a member of the IRFED Identity Federation as a Service Provider only, and to receive identity information from IRFED Identity Federation Identity Providers, a Service Provider is NOT REQUIRED to become a participant of IRFED.

eduGAIN service providers have right to provide IRFED Identity Provider services according to eduGAIN regulations and policies.

External service providers may join IRFED identity provider by signing the agreement provided in http://irfed.ir/.

4 Eligibility

Academic and research organizations inside the border of Islamic republic of Iran approved by respected ministry are eligible to become a federation member. A federation member may act as a Service Provider or Home organization.

eduGAIN members and service providers are eligible to provide IRFED Identity Provider services.

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.

Each application for membership including the Identity Management Practice Statement is evaluated by the Federation Operator.

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 within a reasonable time interval.

If Federation Operator decides to withdraw its role in IRFED, then:

- FO will inform all members and will invite them for a meeting in this regard.
- Meeting should take place within 30 days.
- Members who are interested to take the FO responsibilities, may volunteer.
- In the meeting all members will vote for the new FO.
- Current FO will transfer all necessary documents within next 30 days.
- New FO must provide necessary all equipment / human resources that are needed to act as FO.

6 Legal conditions of use

6.1 Termination

A Federation Member who fails to comply with the Federation Policy 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. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, membership may revoke with a formal notification.

Revocation of a membership implies as soon as possible the revocation of the use of all Technology Profiles for the Federation Member.

6.2 Liability and indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and for any faults and defects meaning amongst other that the Federation Member cannot demand that Federation Operator amend defects, refund payments or pay damages. Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.
Furthermore all federation members must follow Legal Policy Template.

6.3 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy shall be settled primarily through negotiation. If the issue cannot be resolved through negotiation, any disputes shall be submitted to the court of law for IT & Internet Crimes.

If such negotiations do not succeed within eight weeks of the date on which the claim for negotiations was made in writing by one party, each of the parties may bring the dispute before the court of law for IT & Internet Crimes.

If any provision of the Federation Policy is held to be unenforceable by any court of competent jurisdiction, all other provisions will nevertheless continue in full force and effect.

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 shall be communicated to all Federation Members in written form at least 60 days before they are to take effect.

7 Copyright

It is created based on ACOnet federation documents.

8 APPENDIX 1

Membership of IRFED federation is free of charge.

This may change in future and members will be informed before any changes become active.