



Research and Academic Federation of Identities for Kenyan Institutions (RAFIKI)

Identity Federation Policy

Authors	Kenya Education Network (KENET)
Last Modified	25/02/2022
Version	0.1



This work is licensed under a [Creative Commons Attribution- ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

Table of Contents

1	Definitions and Terminology.....	3
2	Introduction.....	4
3	Governance.....	4
	Obligations and Rights of Federation Operator.....	5
	Obligations and Rights of Federation Members.....	5
4	Eligibility.....	7
5	Procedures.....	7
	How to Join.....	7
	How to Withdraw.....	7
6	Legal conditions of use.....	8
	Termination.....	8
	Liability and indemnification.....	8
	Jurisdiction and dispute resolution.....	10
	Interfederation.....	11
	Amendment.....	11
	Governing Law.....	11

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 Research and Academic Federation of Identities for Kenyan Institutions (RAFIKI) 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 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. The Federation Policy also defines the obligations and rights of the Federation Operator. This document, together with its appendices and any documents referred to herein, constitutes the Federation Policy.

3 Governance

Governance and Roles

Kenya Education Network (KENET) hereafter referred to as the “governing body” or “KENET”, is entrusted with the governance of the Federation.

In addition to what is stated elsewhere in the Federation Policy the **governing body** is responsible for:

- Setting membership selection criteria for the Federation.
- Granting or denying an application for membership in to the Federation.
- Revoking the membership if a Federation Member breaches the Federation Policy.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy.
- Addressing financial needs of the Federation.
- Deciding on any other matter of interest to the Federation e.g. Whether or not members will be required to pay registration fee.
- Develop a Standard Data Protection Policy Template to be adopted with/without modifications by the Federation Members.

- Develop and approve all the necessary Agreements, policies and other documents for the Federation including but not limited to, the Membership Agreement, Federation Participation Agreement *et cetera*.

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 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.
- Prepares and presents issues to KENET and acts as the secretary of the KENET 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.
- Where applicable, the Federation Operator will be responsible for the implementation of Data Protection Compliance Requirements for the Federation in line with the applicable Data Protection laws and regulations.

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.

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.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and regulations thereunder and must comply with the Standard Data Protection Policy developed by the governing body or their own Data Protection Policy that has been approved by the governing body.

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.
- 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.
- 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

The Federation sets out eligibility criteria that determines who is able to become a Federation Member. The responsibility for setting membership criteria rests with KENET and may be revised from time to time. Any institution that qualifies to be a member of KENET also qualifies to become a member of RAFIKI (the Federation). The KENET membership criteria is defined at <https://www.kenet.or.ke/node/166>.

5 Procedures

How to Join

In order to become a Federation Member, an organization applies for membership in the Federation to KENET by agreeing to be bound by the Federation Policy. This is done in writing by an official representative of the organization.

Each application for membership including (if applicable) the Identity Management Practice Statement is evaluated by the Federation Operator. The Federation Operator presents a recommendation for membership with an evaluation report to KENET who in turn decides on whether to grant or deny the application.

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

All Federation Members shall be bound by this Federation Policy (and any other documents referred to herein).

How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a written 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 with immediate effect.

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

Termination

If a Federation Member does not follow the Federation Policy, their membership in the Federation may be canceled.

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, the Governing body may issue a formal notification of impending revocation after which the Governing body can decide to revoke the membership should the said Federation Member fail to comply or rectify the breach.

Revocation of a membership implies the revocation of the use of all Technology Profiles for the Federation Member with immediate effect.

Liability and indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and KENET for any faults, losses, damages, errors and defects meaning, amongst other, that the Federation Member cannot demand that the Federation Operator or the governing body amends defects, refunds payments or pay damages. By accepting membership to the Federation and agreeing to be bound by the Federation Policy, each Federation Member (and End User) agrees that the governing body and the Federation Operator shall not be liable for any errors, damages or losses and that each Federation Member accepts liability for its reliance on the information or data provided in the Federation. The Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period. Further, the Federation Operator will endeavor to put in place sufficient technical, organizational, and structural measures that are reasonably proportionate to the potential risks that the Federation faces.

The Federation Operator and KENET shall not be held liable for any loss, damage or cost that arises as a result of the Federation Member connection to or use of Federation services, or other systems to which the Federation Member obtains access in accordance with this Policy.

This limitation of liability does not however apply in the case of gross negligence or intentional fraudulent act shown by Federation Operator personnel.

Neither the Federation Operator nor KENET shall be liable for damage caused to the Federation Member or its End Users. The Federation Member shall not be liable for damage caused to the Federation Operator or KENET due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services.

Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member's membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members.

Federation Operator and the Federation Member shall not claim damages from other Federation Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.

The Federation Member is required to ensure compliance with applicable laws. Neither the Federation Operator nor KENET shall be liable for damages caused by failure to comply with any such laws on behalf of the Federation Member or its End Users relating to the use of the Federation services.

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

The Limitation of liability for acts or omissions shall not extend to offences under any written law and the offending party will be held individually liable unless the offence was in connivance with another party.

Without prejudice to the limitation of liability under this clause, parties are under obligation to take necessary and reasonable measures with respect to their express and implied obligations.

Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any Federation, except as otherwise advised by the Federation Operator. Federation Operator and Federation Members remain bound only by their own respective laws and jurisdictions.

The Federation Member and Federation Operator shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

Jurisdiction and dispute resolution

Should any dispute arise between the Parties hereto with regard to the interpretation, rights, obligations and/or implementation of any one or more of the provisions of this Federation Policy, the Parties shall in the first instance attempt to resolve such dispute by amicable negotiation between themselves.

Should such negotiations fail to achieve a resolution within fifteen (15) days (or such longer time as the Parties may jointly agree), either Party may declare a dispute by written notification to the other, whereupon such dispute shall be referred to arbitration under the following terms:

-

- a)** Such arbitration shall be resolved in accordance with the rules of the Chartered Institute of Arbitrators Kenya Branch (which rules are deemed to be incorporated by reference into this clause) subject to and in accordance with the provisions of the Arbitration Act of Kenya, 1995 (as amended from time to time);
- b)** The tribunal shall consist of one arbitrator to be agreed upon between the parties failing which such arbitrator shall be appointed by the chairman for the time being of the Kenyan Chapter of Chartered Institute of Arbitrators upon the application of either party.
- c)** The place and seat of arbitration shall be Nairobi and the language of arbitration shall be English;
- d)** The award of the arbitration tribunal shall be final and binding upon the parties to the extent permitted by law and either party may apply to a court of competent jurisdiction for enforcement of such award. The award of the arbitration tribunal may take the form of an order to pay an amount or to perform or to prohibit certain activities; and
- e)** Notwithstanding the above provisions of this clause, a party is entitled to seek preliminary injunctive relief or interim or conservatory measures from any court of competent jurisdiction pending the final decision or award of the arbitrator.

Each of the Parties waives all immunity, sovereign or otherwise, and represents warrants and covenants that it will not assert such immunity at law or equity or urge or allow others on its behalf to assert such immunity, which it may now or in the future enjoy or could claim to the extent permitted by law.

Interfederation

The Federation may participate in interfederation agreements to encourage collaboration across national and organizational borders. The relevant Technology Profiles outline how the possible interfederation agreement is administratively and technologically expressed for specific technologies.

The Federation Member recognizes and knows that through those interfederation agreements, the Federation Member may deal with entities that are bound by and committed to foreign laws and federation policies. Those laws and regulations may differ from those of this Federation.

Amendment

The Federation Operator has the authority to alter the Federation Policy at any moment. Any such changes must be authorized by the Governing Body and must be reported in writing to all Federation Members at least 90 days prior to their implementation (before they take effect).

Governing Law

This Federation Policy shall be governed by and construed in accordance with the laws of the Republic of Kenya.

If any term or provision in this Federation Policy shall be held to be illegal or unenforceable, in whole or in part, under any enactment or rule of law, such term or provision or part shall to that extent be deemed not to form part of this Federation Policy but the validity and enforceability of the remainder of this Federation Policy shall not be affected.