FIDERN

FIDERN – Federated ID for Education and Research Networking

Identity Federation Policy

Authors	ZAMREN
Last Modified	30/07/2018
Version	3.0

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 Interfederation	Process of issuing and managing end users' digital identities. 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.
Sponsored Partner	A Sponsored Partner is any entity that is sponsored for participation in the Federation by a participating Higher Education Institutions or Research Organization. A Sponsored Partner typically provides online resources, research data, informational, or other services to the sponsoring higher education organization

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 FIDERN 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 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 governance of the Federation is delegated to the Zambia research and education Network (Zamren). Here after referred to as the governing body.

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

- Setting criteria for membership for the Federation.
- Whether to grant or deny an application for membership in the Federation.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Future directions and enhancements for the Federation.
- Maintaining formal ties with relevant national and international organisations.
- Making changes to the Federation Policy to be approved by Federation Members.
- Addressing financing of the Federation.
- Determining the fees to be paid by the Federation Members to cover the operational costs of the Federation.

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 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.
- 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 Fees.
- 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.
- 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 and who is able to act as Home Organization. The criteria is fully described in the eligibility criteria appendix. Responsibility for setting membership

criteria rests with the governing body of the Federation and may be revised from time to time.

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.

Each application for membership including (if applicable) the Identity Management Practice Statement is evaluated by the governing body 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.

Renewal of participation is automatic as long as the member remains in good standing.

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 a 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 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, the governing body can make a decision to revoke the membership.

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

Federation Operator offers this service on an "as is" basis, without any warranties or liabilities to the Federation Member or its End Users.

Neither the Federation Operator nor the governing body 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 the governing body 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 refrain from claiming 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 the governing body 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.

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. 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.

6.3 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy and between members shall be settled primarily through negotiation as highlighted in the Dispute Resolution Procedure (Appendix 3).

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 for approval in written form at least 90 days before they are due to take effect.

Appendix 1 – Governing Body Constitution

This document describes at a high level how the FIDERN federation is structured and how it operates. Specific details and logistics are left to the discretion of the Federation Operator whose role is fulfilled by the Zambia Research and Education Network (Zamren).

FIDERN Federation Members ("Members") should review this document to guide assessment of potential risks, if any, which might be incurred by their participation in the Federation. By reviewing the policies and practices of the Federation, Members and potential Members can evaluate the level of assurance of the Federation's services to ensure trustworthy operations and determine whether they meet a Member's minimum requirements. Further information about FIDERN's services may be found at http://www.fidern.ac.zm.

1 Role of the FIDERN Organization

The FIDERN Constitution defines the mission of FIDERN and its Federation and the principles and governance structure under which FIDERN and the Federation operates. This Constitution document outlines the activities undertaken by FIDERN on behalf of its Federation Members.

The administrative and operational functions of FIDERN are carried out under direction of the Federation Operator. These responsibilities include development of the federation community (including through expanding such community through peering with other federations that share the same mission as FIDERN such as Research and Education federations in other countries), processing applications, identifying and authenticating eligible organizations and their trusted officers, processing participant Metadata, facilitating the exchange of Metadata between Members in FIDERN and inter-federations, overseeing the operation of FIDERN service platforms, dispute resolution, termination processes, accounting and billing, and other duties as deemed necessary.

2 Organizational Structure

2.1 Management

Responsibility for management of the business and affairs of FIDERN is vested with the FIDERN governing body.

2.2 Committees

The governing body may designate subordinate or advisory committees to make decisions, develop position papers, and/or provide advice on particular matters of importance to the Federation. At least one member of the governing body will participate in each advisory committee to ensure good communication between the committee and the governing body. Additional membership in such committees will be defined by the governing body and typically will be drawn from the participant community. Other individuals may be asked to participate based on their particular knowledge of the subject matter. Current committees are listed on the FIDERN website.

2.3 Offices and Records

The FIDERN Federation office's contact information is:
FIDERN c/o Zamren
University of Zambia, Sch of Education Building, 1st Floor,
Lusaka, Zambia
Email address: fidern@zamren.zm or info@fidern.ac.zm
Telephone: 0211-295928
Website: http://www.fidern.ac.zm/
All records of FIDERN are managed by this office.

2.4 Personnel

All FIDERN Federation administrative and operational functions are performed by the Federation Operator. Other officers may be appointed as need arises.

3 Policies, Requirements, and Standards

The governing body approves all policies, requirements, and standards that apply to the FIDERN federation and its Federation All documents, guidelines, and other papers are available on the FIDERN website.

4 Registration and Management of Participant Policies, Systems, and Technical Components

4.1 Types of Registered Systems: Identity Providers and Service Providers

Within the Federation, Members may offer services as an Identity Provider for their respective user community, as a Service Provider to any participant organization's user community, or both. For instance, a Higher Education Institution serving primarily as an Identity Provider might also make online information or services available to other

FIDERN Members or Inter-Federations. Sponsored Partner that is primarily a provider of online services can act as a service provider and not as an Identity Provider. Members register identity management systems and/or service provider systems.

4.2 Relationship of Systems to Participant

Any identity management system or service provider system registered by a Participant must be under the management hierarchy of the Participant organization. The Participant is responsible for the actions of any system registered with the Federation. Members may only register third party systems that operate services under contract to Participant and for which Participant will be responsible, in accordance with the provisions of the Participation Agreement. Such third party systems might, for example, include outsourced identity management services.

4.3 Required Information Components

4.3.1 Participant Operating Practices

A fundamental expectation of Federation Members is that they provide authoritative and accurate attribute assertions to other Members and that Members receiving an attribute assertion must protect it and respect any privacy constraints placed on it by the Federation or the source of that information.

4.3.2 Metadata

A Participant Administrator registers its Identity Provider and/or Service Provider systems. The data are collected by the Federation Operator, up-to-date, trusted information about all Members and their systems is a core service of the Federation. FIDERN will make reasonable efforts to verify submitted data.

Under special circumstances, Participant Executives or Administrators may make removal requests via e-mail or telephone. FIDERN will verify these requests using trusted communication channels before processing any removal requests.

FIDERN may also collect Metadata from metadata registrars of other Co- Federations and make it available to Members for the purposes of furthering the mission of the Federation.

Transmission of Federation Metadata to Members is not initiated by FIDERN. Instead, Members are expected to retrieve Metadata compiled by the Federation on a regular basis.

5 Operations

The operation and performance of the Federation infrastructure are paramount to maintaining its trust fabric. FIDERN supports certain operational services. As the

Federation gains more experience with federated identity and access management and as requirements for other federation services emerge, the FIDERN Federation's operations will evolve to meet new functional criteria.

5.1 Communications and Support

5.1.1. Posting Material on the FIDERN Website

All FIDERN operating documents and statements are made accessible via the FIDERN website.

5.1.2. Help Desk

FIDERN provides a Help Desk for Participant administrative and technical support. The Help Desk is staffed during normal Zamren business hours. Any end users who inadvertently contact the Federation Help Desk will be referred to their home organization for support in online access to other Members

5.2 Federation Technical Infrastructure

FIDERN is responsible for the secure operation of a number of technology platforms including: a "Discovery Service" (DS) server; a Metadata distribution service; and other necessary infrastructure.

5.2.1 Discovery Service (DS)

The Discovery Service, an optional user interface component, is responsible for allowing users to specify their appropriate Identity Provider for the services they intend to use on-line. Upon selecting an Identity Provider, the user is redirected to the Identity Provider's log in service to authenticate. FIDERN operates a DS service and Web page on which all Identity Providers are listed.

5.2.2 Metadata Distribution

FIDERN publishes Metadata submitted by all Members for interoperation of Identity Provider and Service Provider systems. FIDERN may also make a subset of the Metadata available to peering Federations.

5.2.3 Suspension of Federation Services

If FIDERN suspects compromise of any of its service components, it may take immediate action to remedy the situation or verify non-compromise, including taking components out of service for a limited time for diagnosis and repair. The *Federation Operator* always will endeavor to minimize interruption or inconvenience to Members. Any critical compromise will be communicated to Members in a timely manner.

5.3 Disaster Recovery

FIDERN disaster recovery practices ensure the minimum interruption of availability of Federation services in the event of a disaster. This includes providing redundant hardware and secure data backups.

Appendix 2 – Fees

FIDERN fees are established by the governing body with approval from member institutions. The current fee schedule is as follows:

- No membership or joining fee is paid for the service.
- However individual service providers may charge a fee for access to their services.

Current fee schedules are also available on the FIDERN website.

FIDERN fees are separate from Zamren dues.

Appendix 3 – Dispute Resolution Procedure

Should disputes regarding Federation services or the use of those services arise among Members or between a Member and FIDERN, the following procedure is intended to affect a resolution. This procedure will evolve as the Federation gains more experience with the types of disputes that may occur.
Upon resolution, a brief description of the dispute's issues and the resolution of those will be communicated to Federation Members by email, unless non-publication is requested by any of the disputing Members.

1 Disputes Among Members in FIDERN and/or other Federations

Members are expected to make every reasonable effort to settle disputes among themselves, especially if contractual issues among the Members are involved. If circumstances warrant, (for example, if the dispute centers on the interpretation of Attribute values or the implementation of standards) FIDERN may be asked to act as referee in helping the Members come to resolution. If a FIDERN Participant has a dispute with an organization in a Co-Federation relating to services described in this document that cannot be resolved, FIDERN will use best efforts to work with the Participant, any relevant inter-federation service provider and Co-Federation operator on a mutually agreed-on solution.

The Zamren will serve as the Referee in working with Members. The Referee will gather as much information as possible from each disputing party and then, if necessary, ask for additional information or advice from other operational staff or advisors. The Referee will then document in writing a proposed solution and submit it to the disputing parties for comment. If both parties agree to the resolution the final draft will be filed and documented for future reference.

2 Disputes Between Member(s) and the Governing Body

Any member may submit a written Notice of Dispute to the Zamren regarding any aspect of the operation or services supported by the Federation. The Zamren will make certain that sufficient information exists to define the dispute and then shall appoint a member institution to serve as Negotiator with the disputing Participant(s).
The Negotiator will gather all the facts and rationales for the dispute and, as necessary, seek advice from any Federation advisors or other relevant parties. The Negotiator will prepare a written report, which shall include a recommended resolution of the dispute.

The report shall be submitted to both parties within 30 days of the appointment of the Negotiator unless delayed by the required fact finding.

Zamren shall report its final action to the disputing Member(s) in writing as soon thereafter as is practical. If any disputing party believes it cannot accept the outcome of this process, its only recourse is to discontinue participation in the Federation.

Appendix 4 – Eligibility Criteria

Organizations that wish to participate in FIDERN must be eligible under the requirements defined below. Applications must be submitted and will be processed as described in section 4.2.

1 Eligibility to Become a Member

FIDERN currently has three classes of Members:

1. Higher Education Institutions. Organizations that fall under this category include but is not limited to
    i. Universities
    ii. TEVETA institutions
    iii. Institutions which either govern or manage a collection of accredited, degree-granting institutions. The entity must be commissioned, established, or recognized by a local, or national government to perform this activity or must be a cooperative venture organized by and for the benefit of higher education institutions for the above purposes. Documentation substantiating these criteria may be required, and determinations will be made on a case by case basis.
2. Research Organizations. FIDERN acknowledges that Research Organizations are critical partners in the research and education efforts. A Research Organization is defined as a lab, facility, or center conducting research.
3. Sponsored Partners of any participant in the first two classes. A Sponsored Partner is any entity that is sponsored for participation in the Federation by a participating category 1 or category 2 organization. A Sponsored Partner typically provides online resources, research data, informational, or other services to the sponsoring higher education organization. A sponsorship letter must be received by FIDERN from the sponsoring category 1 or category 2 members either by email or postal mail.

The FIDERN governing body may choose to set eligibility criteria for additional types of organizations or may vote on the approval of any applying organization under special circumstances.

2 Submitting and Processing an Application

Interested organizations may apply for membership by sending an email or submitting an online application for review. FIDERN may request additional information concerning the nature or qualifications of the applying organization.

Eligible applicants will be accepted for membership when a signed copy of the Policy Document has been received by the FIDERN office and has been countersigned by FIDERN.