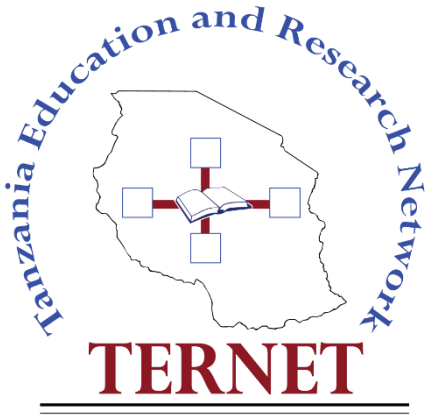

TERNET Identity Federation (TIF)

Identity Federation Policy

Authors	Dr. Frank Seth, Magesa Mihayo
Last Modified	08 July 2024
Version	1.1

Table of Contents

1 Definitions and Terminology

Access Control	A system at the service provider that use the identity information to enforce authorization policies.
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.
Identity Provider (IdPs)	A system entity that creates, maintains, and manages identity information for principals and also provides authentication services to relying on applications within a federation. It is used to authenticate users and provide identity information to service providers.
Inter-federation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
TERNET	Tanzania Education and Research Network
TIF	TERNET 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 TERNET Identity Federation (TIF) is introduced to facilitate and simplify the introduction of shared services between TIF participants with federation technologies, an end user from TIF participant can use his Digital Identity to access Service Providers within the whole federation or base on inter-federation agreements even in other federations. It is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. Federation is related to single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations.

TERNET as Federation Operator coordinates and manages the necessary activities, which in the end enables direct interoperation between end users. TIF is an identity federation service provided by TERNET.

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, https://tif.ternet.or.tz.

3 Governance and Roles

3.1 Governance

The governance of the Federation is delegated to the Tanzania Education and Research Network (TERNET). The Federation Operator is a team constituted from the TERNET service department.

In addition to what is stated elsewhere in the Federation Policy, TERNET 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.
- Deciding on the future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Managing the process of entering into inter-federation agreement.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- There is no fee required to join the TIF. However, only the active members of the NREN will be eligible to join the TIF.
- 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, TERNET 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 TERNET and acts as the secretary of the TERNET meetings.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding inter-federation 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, TERNET 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, and a technical contact, for interactions with the TERNET.
- 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 communicated annually by the TERNET secretariat.
- If a Federation Member processes personal data, the 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.

3.4 Obligations and Rights of Identity Provider

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 TERNET, 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.
- Is responsible for keeping its metadata up to date.
- Must send a list of Service Providers which is related to if there is an intention of cancelling its membership.

3.5 Obligations and Rights of Service Provider

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.
- In addition to the access grant, the Service Provider can use the information retrieved from Identity Providers only for: Customization, Audit, Usage reports, and for any other purpose specifically agreed between the Identity provider and the Service Provider.
- Can make use of the TIF's Discovery Service
- Is responsible for keeping its metadata up to date.
- Must send a list of Identity Providers which it is related to if there is an intention of cancelling its membership.

3.6 Obligations and Rights of End User

End Users MUST comply with the applicable rules of the Federation Policy and the rules by their TIF Member. They are responsible and liable for the misuse of their Digital Identity towards the IdP Operator, the SP Operator and TERNET. The End User is responsible and liable for any misuse of his username and password or other protection of his Digital Identity. The End User has no liability claims or other claims against TERNET if, owing to negligent keeping or management of the access to his Digital Identity or because of its disclosure to third parties, unauthorized actions are made and processed by TERNET or a Federation Member.

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 on the TIF website, https://tif.ternet.or.tz/. Responsibility for setting membership criteria rests with TERNET and may be revised from time to time.

4.1 Rules of Membership

The Federation is operated by the Federation Operator, that also operates the national research network. Further participants are Members of Ethiopian Education and Research Network or members that have joined in a second moment, prior approval by the General Assembly and Federation Members that join prior approval by the Directive Board. Federation Members must have a signed contract with the Operator.
The following institutions may be Members of the federation:

1. Public and private Academic education institutions
2. Research, educational, academic and innovation institutions.
3. Companies from ICT ecosystem.
4. Communities of practice and anchor organization

All Members of the Federation might provide services. Members are entitled to supply user identity information to the federation.

5. Procedure

In this section procedures for joining and withdrawal will be described.

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 has to be sent to TERNET 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 TERNET.

5.2 How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to TERNET. 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.

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 TERNET is aware of a breach of the Federation Policy by a Federation Member, TERNET may issue a formal notification of concern. If the cause for the notification of concern is not rectified within 60 days by Federation Member, TERNET can decide 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

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

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and TERNET 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.

The Federation Operator and TERNET may 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 the agreement. This limitation of liability does not however apply in the case of gross negligence or intent shown by Federation Operator personnel.

Neither the Federation Operator nor TERNET 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 TERNET 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 TERNET 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 inter-federation 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 Operators and Federation Members remain bound only by their respective laws and jurisdictions.

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

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, or if such negotiations do not succeed within four weeks of the date on which the claim for negotiations was made in writing by one party, the disputes shall be submitted, by either party, in writing (with a copy to the other Party) to the Tanzania Arbitration Centre for determination in accordance with law and Regulations governing Arbitrations in Tanzania.

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 Inter-federation

In order to facilitate collaboration across national and organizational borders the Federation may participate in inter-federation agreements.

The Member understands and acknowledges that via those inter-federation 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

TERNET has the right to amend the Federation Policy from time to time. Any such changes need to be approved by the Governing Body and shall be communicated to all Federation Members in written form at least 60 days before they are to take effect.