Identity Federation Policy

Authors	Mwotil Alex, Omo Oaiya, Mario Reale, Eriko Porto
Last Modified	20 May 2021
Version	v0.1

Table of Contents

Terminology & Definitions

Introduction

Governance and Roles Governance

Eligibility

Procedures

- How to Join
- How to Withdraw

Legal conditions of use

- Termination
- Liability and indemnification
- Jurisdiction and dispute resolution
- Interfederation
- Amendment

1 Terminology & Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT","SHOULD", "SHOULD NOT","RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119, see http://tools.ietf.org/html/rfc2119.

The following are the terms and definitions used in this document:

Federation: A group of organizations that come together to collaborate and facilitate resource access under a set of defined and agreed rules.

Federation Operator: UbuntuNet Alliance, WACREN & ASREN service portfolio units that provide infrastructure for authentication and authorization to federation members.

eduID.africa Identity Federation: The African continental catch-all identity federation.

Federation Member: An organization that runs an identity provider(s)/service provider(s) that has joined eduID.africa and agreed to be bound by the eduID.africa federation policy.

Interfederation: A collaboration between identity federations to ease access to service providers and hence services/resources.

Identity Provider (IdP): The IdP authenticates members of a home organization against an existing identity management system and providers and makes assertions on what attributes should be relayed to a service provider.

Service Provider (SP): The SP provides/grants access to end users to services or resources available on the eduID.africa federation.

Attribute: An end user piece of information that identifies his/her properties managed within a home organization (Attribute Authority).

End User: A person affiliated to a home organization based on their role and makes use of a service provider.

2 Introduction

The African catch-all federation (confederation) eduID.africa is an identity federation that covers Africa and is designed to:

- Facilitate and simplify the introduction of shared services across the federation
- Fastrack the rollout of identity federations in Africa
- Provide guidelines/best practices to constituent countries in establishing national federations
- Onboard institutions within the region and without a national federation in order to support collaboration

This is achieved through the following components which all constitute the federation policy:

1. eduID.africa identity federation policy document: This document defines the federation members' obligations and rights in using the available federation technologies in the resource access cycle (request, identification, authentication, authorization and access) in the federation. It does not directly describe practices or procedures for any specific federation technology.
2. The Assurance Profile: This describes the levels of trust allowing service providers to determine certainty of identification between subjects and their claimed identities.
3. The Technology Profile: This describes the realizations of the policy and assurance profiles and govern the use of federation technologies.

All these components are based on current and evolving technologies and shall be updated from time to time with the latest and archived versions available on
https://www.eduid.africa/policies

3 Governance and Roles

Governance

The governance of the eduID.africa identity federation is delegated to the three Regional Research & Education Networks (UbuntuNet Alliance (East, Central and South Africa), WACREN (West Africa) and ASREN (North Africa)) all operating within the African continent and mandated to plan, manage and run the regional networks. The legal services for the federation shall be provided by UbuntuNet Alliance. The management team shall be drawn from the three entities. In addition, the management team shall:

- Set criteria for membership and admission to the federation performing grant, deny and revoke actions where appropriate.
- Approve changes to the Federation Policy prepared by the Federation Operators. ● Maintain formal ties with relevant national and international organisations.

- Provide future directions and enhancements for the Federation with support from the operations team.
- Coordinate and sign Interfederation agreements.
- Address financing of the Federation.
- Approve the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Decide on any other matter referred to it by the Federation Operator.

The eduID.africa identity federation operations team shall consist of 1 technical team member from each of the three RRENs and shall provide line support to the federation members. The team shall also be responsible for publishing the federation member list along with the assurance profiles and technology profiles. In addition, the federation operations team shall:

- Support the 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.
- Provide support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Act as centre of competence for the 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.
- Maintain relationships with national and international stakeholders in the area of Identity Federations.
- Promote the idea and concepts implemented in the Federation so that prospective Federation Members learn about the possibilities of the Federation.

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting secure and trustworthy operation of 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.

The federation member shall be duly approved by the management team on grounds of service offering (IdP or SP), region of operation and assessment of its ability to support the service or its end users. Regardless of the service being offered, the service provider:

- 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 where required
- If a Federation Member processes personal data, the 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, as may be further specified in Level of Assurance Profiles.
- 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.
- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy (AUP).
- Shall operates a helpdesk for its End Users regarding Federation services related issues.

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 for releasing the Attributes to Service Providers.

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

- Is responsible for making decisions on which End Users can access the services they operate and which access rights are granted to an End User. It is the Service Provider's responsibility to implement those decisions.

4 Eligibility

The Federation aims at providing a continental workspace for users, services and institutions to get direct experience and gain familiarity with consuming and providing federated services and identities. Furthemore, the Federation sets out eligibility criteria that determines who is able to become a Federation Member:

- All Research and Education related Services and Identity Providers willing to promote the adoption of Federated Identity Management (FIM) in Africa, with the purpose of promoting identity federations and eduGAIN in the continent.
- In addition, relevant services and identity providers who would benefit to join eduGAIN and FIM, who do not have a corresponding national identity federations are eligible and encouraged to join the African catch-all federation.

For the above, the institutions must provide formal evidence of registration within the country of operation.

This criteria is fully described on the eduID.africa website https://www.eduid.africa/policies

Responsibility for setting membership criteria rests with the Federation Operators and may be revised from time to time.

5 Procedures

5.1 How to Join

In order to become a Federation Member, an eligible organization (as per Section 4) 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 (if applicable) the Identity Management Practice Statement is evaluated by the Federation Operators. The Federation Operators present a recommendation for membership with an evaluation report to federation management 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 Operators.

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 Operators. 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 Operators shall run the Federation on a best effort basis. After the termination date, Federation Operators 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 Operators 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, a formal notification of impending revocation is issued after which the Federation Operators 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

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

The Federation Operators 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.

The Federation Operators offer this service on an "as is" basis, without any warranties or liabilities to the Federation Member or its End Users. The Federation Operators shall not 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 Operators 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 Operators 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. The Federation Operator 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 Operators and Federation Members remain bound only by their own respective laws and jurisdictions.

The Federation Member and Federation Operators 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 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 Chairman for the time being of the Centre for Litigation and Dispute Resolution, Malawi, who will appoint an arbitrator. 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 regional divides, 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 Operators have 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.