eduIDM

Identity Federation Policy

Authors	**S. El Haddouti, H. Bouhaddou, R. Merrouch**
Last Modified	**14/05/2018**
Version	**V0.1**

Table of Contents

Acknowledgements:

This document is based on the REFEDS Metadata Registration Practice Statement template and the Creative Commons Attribution-ShareAlike 3.0 Unported (CC-BY-SA 3.0).

1. Definitions and Terminology

Identity Management	Process of issuing and managing End Users' digital identities.
Identity Federation	An arrangement that can be made among multiple organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	Organization which manages the Identity Federation by providing an Infrastructure for Authentication and Authorization to Federation Members.
Identity Provider (IdP)	The organization with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Service Provider (SP)	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 assert for its End Users.
Federation Member	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the federation, a Federation Member can act as an Identity Provider and/or a Service Provider.
End User	Any natural person affiliated to a home organization, e.g. as an employee, researcher or student making use of the service and resources.
Attribute	A piece of information describing the End User, his/her properties or roles in an 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.
Federation Metadata	SAML/XML file which contains information about all Federation Members.

2. Introduction

An Identity Federation is an arrangement that can be made among multiple organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.

The eduIDM Identity Federation is a service offered and managed by MARWAN, the Moroccan National Research and Education Network, in order to provide easy, standard and secure means of user data exchange to facilitate the access to various online resources, offered by different Service Providers, while avoiding multiple credentials for a single End User. In other words, the eduIDM Federation offers an organizational and technical framework to enable federation members sharing several applications and services using identity federation mechanisms. Each member can act as an Identity Provider and/or a Service Provider.

This Federation Policy defines 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.

3. Governance and Roles

3.1. Governance

The governance of the eduIDM Federation is delegated to the National Center for Scientific and Technical Research (CNRST).

In addition to what is stated elsewhere in this Federation Policy, the CNRST is responsible for:

- Setting criteria for membership for the eduIDM federation.
- Evaluating and determining whether to grant or deny an application for membership in the eduIDM federation.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Evaluating and determining future directions and enhancements for the Federation made by the Federation Operator.

- Evaluating and determining the entering into inter-federation agreement by virtue of the interest of eduIDM Federation.
- Maintaining formal ties with relevant national and international organizations.
- Deciding on any other matter referred to it by the Federation Operator.

3.2. Obligations and Rights of Federation Operator

eduIDM federation is managed and operated by MARWAN, the Moroccan National Research and Education Network.

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 Metadata.
- Publish a list of Federation Members.
- 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.
- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting secure and trustworthy operation of the Federation.
- Inform members of the Identity Federation of changes in the policy of the eduIDM service.
- Respect the legislation concerning the personal data in accordance with the law in force.
- Notify Federation Members of service changes and updates.

3.3. Obligations and Rights of Federation Members

In addition to what is stated elsewhere in this Federation Policy, all Federation Members:

- Shall appoint and name administrative and technical contacts for interactions with the Federation Operator.
- Shall 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.

- Shall comply with the obligations of the Technology Profiles, when specified.
- Shall respect the legislation concerning the personal data in accordance with the law in force.
- Shall ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- Must agree in facilitate the use of their names and logos in the communicational channels disposed by MARWAN, for the purpose of promoting the eduIDM Federation;
- In the same way, the Federation Member must commit to mention MARWAN as the Operator of eduIDM Federation.
- Shall inform the Federation Operator, in writing, of any change in the information provided in the Federation Membership Agreement.

If a Federation Member is acting as an Identity Provider, it:

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them.
- Operates a helpdesk for its End Users regarding federation services related issues. IdPs are encouraged to maintain a helpdesk for user queries at least during normal office-hours in the local time zone. An IdP 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 Identity Provider contacts.
- Shall allow the exchange of End User attributes requested by service providers.
- Ensuring the update of End User attributes.

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.
- Provides content serving education and research community.
- Respects intellectual rights (copyright, database law, trademark law, design rights, etc.) and the rights of third parties (protection of personal data, defamation, etc).

4. Eligibility

All institutions and organizations connected to MARWAN network or other academic institutions can join eduIDM federation as members. These institutions can apply, at any time, for membership as Identity Providers and/or Service Providers at any time. Commercial companies and organizations that don’t belong to the MARWAN community, and they would like to contribute to the eduIDM Federation by providing services and resources, can join the eduIDM Federation as Partners.

5. Procedures

5.1. How to Join

In order to become a Federation Member, an organization applies for membership, as an IdP and/or SP, 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 CNRST via postal mail. The application will be evaluated by the Federation Operator within 15 days after its receipt. Upon acceptance, the organization receives, exclusively to the provided postal mail address, the countersigned documents. If the application is denied, the decision and the reason for denying the application are communicated to the applying organization by CNRST.

5.2. How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request, via postal mail, to the CNRST with 2 months' notice. A cancellation of membership in the Federation implies the cancellation of the use of all federation’s Technology Profiles for the organization.

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, it may issue a formal notification of concern. If the cause for the notification of concern is not rectified within 30 days by the Federation Member, the CNRST may issue a formal notification of impending revocation after which the CNRST 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

MARWAN offers the eduIDM service without any liability of CNRST to the Federation Member or its End Users for any faults and defects. In other words, the Federation Members cannot demand that CNRST amend defects or pay damages. MARWAN will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.

MARWAN and CNRST 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 policy.

Neither MARWAN nor the CNRST shall be liable for damage caused to the Federation Member or its End Users, The Federation Members shall not be liable for damage caused to the Federation Operator or the CNRST 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.

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 an authorized court at Rabat that will decide according to Moroccan law.

6.4. Inter-federation

To promote the collaboration and simplify the access to content, services and resources for the research and education community across national and organizational borders, the eduIDM Federation may participate in inter federation agreements. The Members understand and acknowledge that via those inter-federation arrangements, they may interact with organizations which are bound by and committed to foreign laws and federation policies which may be different from the laws and policies in the eduIDM Federation.

6.5. Amendment

The Federation Operator MARWAN has the right to amend this Federation Policy from time to time. Changes are communicated to all Federation Members in written form at least 30 days before they are to take effect.