



SIFULAN[©] Malaysian Access Federation

Identity Federation Policy [DRAFT]

Authors	Suhaimi Napis, Muhammad Farhan Sjaugi, Zahira Mohd Ishan
Last Modified	17 January, 2018
Version	1.0



Copyright

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007-2013) under Grant Agreement No. 238875 (GÉANT).

This work is based on the "SWAMID Federation Policy v2.0", written by L. Johansson, T. Wiberg, V. Nordh, P. Axelsson, M. Berglund available at <http://www.swamid.se/11/policy/swamid-2.0.html> ©2010 SUNET (Swedish University Computer Network) ©2016 SIFULAN[©] Malaysian Access Federation used under a Creative Commons Attribution-ShareAlike license: <http://creativecommons.org/licenses/by-sa/3.0/>.

Table of Contents

1. Definitions and Terminology	3
2. Introduction	4
3. Governance and Roles	5
4. Eligibility	7
5. Procedures.....	7
6. Legal conditions of use.....	8

1. Definitions and Terminology

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 RFC 2119 [RFC2119].

The following definitions are used in this document:

Attribute	A piece of information describing the End User, his/her properties or roles in an organization or institution.
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. (not limited to) as an employee, researcher or student making use of the service of a Service Provider, including government servant entrusted with the administration of education, research or research and development or of the extended scope of the Federation)
Federation	A group of organizations or institutions that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Policy	A set of rules and regulations governing the Federation.
Federation Operator	Organization or Company providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Member	An organization or institution 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 or institution 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.
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.
Service Provider	An organization, institution or company 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

The SIFULAN© Malaysian Access Federation (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.

2.1 The purpose of SIFULAN® from here on referred to as the Federation is to provide a mechanism for connecting members of the education and research sectors (including academics, researchers, students and government servants) from here on referred to as ("End Users") securely and reliably to online information, infrastructure, services and resources.

2.2 Subscription to the Federation is available to organisations and institutions from here on referred to as ("Federation Member") which undertake or support education, research or research and development in Malaysia and agree to be bound by the Federation Policy ("Policy") and these Rules ("Rules").

2.3 The Federation relies on Federation Members, as Identity Providers, correctly and accurately asserting information about the identity of its End Users to other Federation Members who, as Service Providers, will use that information to grant (or deny) access to the services and resources they offer to End Users.

2.4 The scope of the Federation MAY be extended over time to include a broader range of Federation Member beyond the education and research sectors.

2.5 The electronic exchange of authentication information between End Users, Identity Providers and Service Providers and the provision of support services for Federation Members MAY be managed by an Operator on behalf of the Federation.

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 authoritative, final decision is always up to the Federation Operator, especially when deciding on admitting an organisation into the Federation, cancelling an organization's membership, or applying sanctions. The Federation Operator also provides an authoritative interpretation of the Federation Policy.

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

- Setting criteria for membership for the Federation.
- Determining whether to grant or deny an application for membership in the Federation.
- Determining 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.
- Recommending future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Evaluating and recommending the Federation on entering into inter-federation agreement.
- Maintaining formal ties with relevant national and international organisations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Addressing financing of the Federation.
- Approving the fees to be paid by the Federation Members to cover the operational costs of the Federation, based upon the proposal of Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

3.1 Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator is responsible for following:

- 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' appointed contact persons to work out operational problems regarding the Federation services.
- Acts as centre of competence for the Federation to provide supports such as, and not limited to, testing software, recommending and documenting solutions, providing 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 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 and benefits of the Federation.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator reserves the right to:

- Temporarily suspend 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 Profiles. Definition of which data MAY be published is provided in appropriate Technology Profiles.

3.2 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 within four (4) hours via email after the incidence is discovered 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. Federation Operator will resolve appropriately within the next working day as gazetted by the Malaysian Government.
- MUST comply with the obligations of the Technology Profiles which it implements.
- MUST ensure its IT systems that are used in implemented the Technology Profiles are operated securely.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws in force in Malaysia or mutually agreed laws and MUST follow the practice presented in Data Protection Profile.

If a Federation Member is acting as a Home Organization or Attribute Authority, 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.
- MUST 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. Specific requirements MAY be imposed by Level of Assurance Profiles.
- Ensures an End User is complies 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 appointed Home Organization contacts.

If a Federation Member is acting as an Identity Provider, 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 authoritative, final decision is always up to the Federation Operator, especially when deciding on admitting an organization into the Federation, cancelling an organization's membership, or applying sanctions. The Federation Operator also provides an authoritative interpretation of the Federation Policy.and MAY be revised from time to time.

5. Procedures

5.1 How to Join

In order to become a Federation Member, an organization as applicant applies for membership in the Federation by agreeing to be bound by the Federation Policy in writing by an official representative of the organization using the download-able form provided.

Each application for membership including (if applicable) the Identity Management Practice Statement SHALL be evaluated by the Federation Operator and MUST pass technology implementation compliance test. The Federation Operator SHALL present a recommendation for membership with an evaluation report on whether to grant or refuse the application.

If the application is refused, this decision and the reason for refusal SHALL be communicated to the applicant by the Federation Operator.

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 within a reasonable time interval.

The Federation Operator MAY cancel its participation in the Federation by announcing the termination date to the Federation Members at Ninety (90) days before the actual termination date. 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, it MAY issue a formal notification of impending revocation after which 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 Operator 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 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 bad intent shown by Federation Operator personnel.

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 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 Operator 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 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 Malaysian laws or mutually agreed laws. Federation Operator SHALL NOT 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 Operator and Federation Members remain bound only by their own respective laws and jurisdictions.

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

6.3 Jurisdiction and dispute resolution

For disputes concerning the Federation Policy, parties SHALL amicably settle their agreement via negotiation. If negotiation is unsuccessful, disputes SHALL be settled via Arbitration. This provision do not oust the Malaysian court of the respective jurisdiction to settle dispute for gross negligence and bad intent by Federation Operator via Arbitration in accordance with the Rules for Arbitration of the Kuala Lumpur Regional Centre for Arbitration

If any provision of the Federation Policy is declared 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. How the potential inter-federation agreement is administratively and technologically reflected for certain technology is described in appropriate Technology Profiles.

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

The Federation Operator has the right to amend the Federation Policy from time to time and SHALL be communicated to all Federation Members in written form at least 90 days before they are to take effect.

7. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119 , March 1997.
-----------	---