Ričerka Net Identity Federation

Identity Federation Policy

Authors	Muscat Daniel
Last Modified	10/09/2019
Version	1.0

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) ©2012 GÉANT, ©2018 University Of Malta used under a Creative Commons Attribution-ShareAlike license: http://creativecommons.org/licenses/by-sa/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 organisation responsible for managing additional Attributes for an End User of a Home Organization.
Authentication	The process of proving the identity of a previously registered End User.
Authorisation	The process of granting or denying access rights to a service for an authenticated End User.
AUP	RiċerkaNet's Acceptable Use Policy
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 (also referred to as Identity Federation)	An association of organisations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	The organisation governing the Federation and providing the Infrastructure for Authentication and Authorization to Federation Members.
Federation Member	An organisation 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.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Home Organization	The organisation with which an End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management	The process of issuing and managing end-users' digital identities.
IDPC	The Office for the Information and Data Protection Commissioner, Malta.
Inter-federation	The voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
RiċerkaNet	The Maltese National Research and Education Network.
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.
Technology Profiles	Technology Profiles describe how given technologies are implemented within the eduGAIN framework.

2 Introduction

RiċerkaNet's Identity Federation (the Federation)'s objective is 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

Governance and Operations

The Federation is governed and operated by the University of Malta by virtue of its function as the Maltese National Research and Education Network, known as RiċerkaNet. It is administered by the Competent Authority of RiċerkaNet as defined by the RiċerkaNet's Acceptable Use Policy (AUP). The University of Malta will hereinafter after be referred to as the Federation Operator, which for the purpose of this Policy shall be considered one and the same as the governing body of the Federation.

The Federation Operator has the authority to make any final decisions on all matters within the Federation. The Federation Operator is the sole authority that provides the authoritative interpretation of the Federation Policy.

Responsibilities of the Federation Operator as governing body of the Federation include but are not limited to:

- Setting criteria for membership to the Federation.
- Granting or Denying an application for membership in the Federation.
- Revoking of membership where a Federation Member is in breach of the Policy.
- Proposing and Approving changes in the Federation Policy, and any Appendices.
- Future directions and enhancements for the Federation.
- Entering into Inter-Federation agreement/s.
- Maintaining formal ties with relevant national and international organisations.
- Deciding on any other matter related to the Federation

Obligations and Rights of the 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.
- Providing support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- 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 harmonisation.
- 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 the secure and trustworthy operation of the Federation.
- Publishing a list of Federation Members along with information about which profiles each Federation Member fulfils or implements, to promote the Federation.
- Publishing 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.
- At any time, temporarily or permanently shutdown (or downgrade the level of functionality) of any service the operator provides, for reasons of maintenance or other circumstances. In exercising this right the Federation Operator will do its best in minimizing downtimes, and disruption.

Obligations and Rights of Federation Members

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

- Acknowledge:
    - That membership of the Federation does not itself grant Members or End Users automatic access to other Members' resources, that Members will need to establish separate agreements in relation to such access, and that the Federation Operator is not responsible or liable to ensure any such access or to negotiate corresponding terms on Members' behalf
    - That the Federation Operator may introduce a fee to cover administrative and other costs.
- 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.
- Shall, when processing any personal data in their capacity as Federation Members and/or in the context of this initiative, comply with all applicable data protection laws (including the General Data Protection Regulation (Regulation (EU) 2016/679) and the Data Protection Act (Chapter 586, Laws of Malta), as well as with any direction or practice mandated in this regard by the Federation Operator and/or the IDPC. Each Federation Member shall be fully and solely responsible to ensure that the data processing operation/s it, including any person acting under its authority, undertakes in this regard conform/s to all applicable laws and/or directives.
- Shall not include, provide and/or publish any personal data (as defined in Article 4 GDPR) in or with data they provide for technical, and administrative or other purposes. In particular, Federation Members shall

not include any personal data in any data describing infrastructural endpoints of authentication and authorization. Shall authorise the Federation Operator to use, hold and publish such technical and administrative data for the purpose of administering the operation of the Federation, and for promotional purposes.
- Shall agree to be bound by this Federation Policy in writing.

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, 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 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 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 Providers' responsibility to implement those decisions.

4 Eligibility

Eligibility criteria to the Federation are identical to those of RićerkaNet, which are set in the AUP.

5 Procedures

How to Join

In order to become a Federation Member, an organisation applies for membership in the Federation by agreeing to be bound by the Federation Policy in writing by an official representative of the organisation.

The Federation Operator evaluates each application for membership including (if applicable) the Identity Management Practice Statement and decides on whether to grant or deny the application. The decision taken on the application is communicated to the applying organisation.

How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to the Federation Operator. Cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organisation within a reasonable time interval.

The Federation Operator may, at any time, discontinue any service provided for given technology profiles by announcing the termination date to the Federation Members. Until the termination date, the Federation Operator shall support the affected services on a best effort basis. After the termination date, Federation Operator shall cancel the use of the effected Federations Technology Profiles for all Federation Members.

The Federation Operator may dissolve the Federation and cease all operations. In such case, a termination date will be announced to all members. Until the termination date, the Federation Operator shall support the Federation on a best effort basis. After the termination date, the Federation Operator shall cancel all services and technology profiles of all Federation Members.

6 Legal conditions of use

Termination

A Federation Member who fails to comply with the Federation Policy and other binding documents 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 Federation Operator may issue a formal notification of impending revocation after which the Federation Operator can decide to revoke the membership.

Revocation of membership implies the revocation, as soon as possible, of the use of all Technology Profiles for the Federation Member.

Liability and indemnification

Liability and limitation thereof that the Federation Operator has in regard to a Federation Member:

For the avoidance of doubt, the Federation Operator may not be held liable for any loss, damage or cost that arises as a result of the Federation Member's connection to or use of Federation services, or other systems to which the Federation Member obtains access to as a result of joining the Federation. The Federation Operator shall additionally not be held liable for any damage caused by accidental or unlawful processing of personal data, or processing that otherwise infringes applicable data protection laws, on the part of Federation Member and/or any person acting under its authority in the context of this initiative.

Service is provided by the Federation Operator on an 'as is' and best-effort basis and therefore without liability for the Federation Operator for any faults or defects. Consequently, a Federation Member cannot demand that the Federation Operator amend defects, refund payments or pay damages. Notwithstanding the aforesaid, Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.

All liability of Federation Operator for actual and direct losses, costs or damages is excluded in this respect, except where such is the result of gross negligence, bad faith or willful misconduct on the part of the Federation Operator as adjudicated by a court of competent jurisdiction. Provided that in the case of breach of Federation Policy by the Federation Operator, the aggregate liability of the Federation Operator and its directors, officers, employees, agents, and sub-contractors in respect of any losses, costs or damages arising out of said breach shall not exceed 10,000 Euros per calendar year and any such claim(s) must be made within three (3) months of the occurrence of said breach. Provided further that, to the maximum extent permitted under applicable law, the Federation Operator shall not be liable to Federation Member(s) for any incidental, special, punitive, exemplary, consequential or statutory damages, or any damages resulting from lost profits, interruption of business or loss of goodwill howsoever arising, even if the Federation Operator had been advised of the possibility of such damages.

Liability and limitation thereof that the Federation Member has in regard to the Federation Operator:

The Federation Member hereby irrevocably indemnifies and holds the Federation Operator, its directors, officers, employees, agents, and sub-contractors harmless from any damages, losses, costs, liabilities, demands, claims, complaints or legal proceedings brought or threatened, including but not limited to expenses or pecuniary penalties suffered or incurred arising out of the Federation Member's breach of Federation Policy, negligence, bad faith or willful misconduct.

The Federation Member shall not be subjected to any punitive or exemplary damages.

Liability and limitation thereof that a Federation Member has in regard to other Federation Members:

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. The Federation Operator shall not be liable for damages caused by the failure of a Federation Member or its End Users to comply with any such laws relating to the use of the Federation services.

Liability and limitation thereof that a Federation Operator and a Federation Member have in regard to other entities that they are collaborating with via Inter-Federation:

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 within the same federation. Federation Operator and Federation Members remain bound only by this Federation Policy as well as their own respective laws and jurisdictions.

Jurisdiction and dispute resolution

This Policy shall be interpreted in accordance with the Maltese legislative framework, to the exclusion of the law of any other forum.

Any dispute arising from or in connection with the Federation Policy shall be settled by the disputing parties through negotiations. If the dispute cannot be settled within three (3) consecutive calendar months after a party sends a notice to the other party requiring the negotiation thereon, then, either party may refer it to any court having jurisdiction within the Republic of Malta.

Inter-federation

In order to facilitate collaboration across national and organisational 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 organisations 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.

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

Provided that if any portion of this Policy, is for any reason or to any extent, adjudged to be invalid or unenforceable, such invalidity or unenforceability shall not affect or render invalid or unenforceable the other sections of this Policy, and those changes or amendments that may be required to carry out the intention and accomplish the purpose of this Policy shall be carried out by the Federation Operator in accordance with this section.