

safelD Federation Policy

Document	safelD Federation Policy
Version	1.0
Last Modified	2018-06-22
Status	FINAL
License	Creative Commons BY-SA 3.0

Copyright

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, used under a Creative Commons Attribution-ShareAlike license: <http://creativecommons.org/licenses/by-sa/3.0/>.

Contents

1 Definitions and Terminology.....	2
2 Introduction.....	2
3 Purpose and Scope.....	3
4 Governance and Roles.....	3
4.1 Governance.....	3
4.2 Obligations and rights of Federation Operator.....	3
4.3 Obligations and Rights of Federation Member.....	4
5 Eligibility.....	5
6 Procedures.....	5
6.1 How to join.....	5
6.2 How to Withdraw.....	5
7 Legal conditions of use.....	5
7.1 Termination.....	5
7.2 Liability and Indemnification.....	6
7.3 Interfederation.....	6
7.4 Amendment.....	6

1 Definitions and Terminology

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.
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	A natural person affiliated to a Home Organization, e.g. as an employee, researcher or student accessing the service provided by 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	An organization operating the central components of the Federation, 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 a role of an Identity Provider, i.e., authenticating the End User and managing End Users' identity data.
Identity Management	Process of issuing and managing end users' digital identities.
Interfederation	Collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access services in another Identity Federation.
Level of Assurance Profile	Deals with Identity Management practices in use by Home Organizations and allows a Service Provider to determine with which degree of certainty an End User is truly presented by a digital identity he/she is using.
Service Provider	An organization responsible for operating and offering a service to the End User. Service Providers may rely on the authentication outcome and attributes that Home Organizations and Attribute Authorities assert for their End Users.
Technology Profile	Definition of technical and policy requirements and obligations for a Federation Operator and Federation Members implementing a specific federation technology.

2 Introduction

The Slovak Academic Federation of Identities (the Federation) is introduced to facilitate and simplify the use 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 short-form name of the Slovak Academic Federation of Identities is **safelD**.

The Federation Policy 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.

The Federation Policy has three main parts: this document which describes governance, membership and scope. Further, a set of Level of Assurance Profiles and a set of Technology Profiles. The Level of Assurance Profiles and the Technology Profiles are based on current and evolving standards and are described in separate documents. This document, together with all its appendices constitutes the Federation Policy. The current list of all appendices is available on the [website](#) of the Federation.

3 Purpose and Scope

The purpose of the Federation is to make it possible for Service Providers to provide services to End Users in the Federation. This is accomplished by making infrastructure for federated identification and authentication available to the higher education and research community in Slovak Republic, including but not limited to universities, university colleges, research hospitals, government agencies and private sector organizations involved in education and research.

The scope of the Federation Policy is limited to those technologies which are capable of supporting federated secure authentication and authorization of users as described by the Technology Profiles. The set of procedures and practices described in this document applies equally to all Technology Profiles of the Federation.

4 Governance and Roles

4.1 Governance

Slovakian national research and education network provider, hereafter called "SANET", acts as the Federation Operator. The SANET Board of Directors acts as the governing body of the Federation.

In addition to what is stated elsewhere in the Federation Policy the SANET Board of Directors 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.
- Approving entering into interfederation agreement.
- Maintaining formal ties with relevant national and international organizations.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Address financing of the Federation.
- Deciding on any other matter referred to it by the Federation Operator.

4.2 Obligations and rights of Federation Operator

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

- Co-ordinates the operation of the Federation, and oversees adherence to the Federation Policy. This includes providing central services following the procedures and technical descriptions specified in this document and its appendices.
- Provides support services for Federation Members via the designated contact persons to work out operational issues regarding the Federation services.

- Maintains relationships with national and international stakeholders in the area of Identity Federations. This includes interfederation activities and work with other Identity Federations in the area of harmonization.

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

- Temporarily suspend the use of 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.

4.3 Obligations and Rights of Federation Member

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 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 used in the context of implemented Technology Profiles are operated in a secure manner.
- If a Federation Member processes personal data, Federation Member will be subject to applicable data protection laws and is responsible for fulfilling the requirements present in the Data Protection Act.

If a Federation Member is acting as a Home Organization or an 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.
- 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, all of 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 designated Home Organization contacts.

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

- Is responsible for making decision on which End Users can access the services operated by the respective Member and which access rights are granted to an End User. It is Service Providers responsibility to implement those decisions.

5 Eligibility

An organization must be eligible for SANET membership and must become a Federation Member in order to act as a Home Organization or an Attribute Authority in the Federation. A Federation Member acting as a Service Provider only is not required to qualify for SANET membership in order to consume identity information from other Federation Members. Technology Profiles may impose additional requirements on Home Organizations, Attribute Authorities or Service Providers.

6 Procedures

6.1 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 membership application including (if applicable) the Identity Management Practice Statement is evaluated by the Federation Operator. The Federation Operator presents a recommendation for membership with an evaluation report to the SANET Board of Directors 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 is communicated to the applying organization by the Federation Operator.

6.2 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 automatic and immediate cancellation of the use of all federations Technology Profiles for the organization.

The Federation Operator may cancel its participation in the Federation by announcing the termination date to the Federation Members. Federation Operator shall run the Federation until termination date. After the termination date, Federation Operator shall cancel the use of all federations Technology Profiles for all Federation Members.

7 Legal conditions of use

7.1 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, the governing body of the Federation may issue a formal notification of impending revocation after which the governing body of the Federation can make a decision to revoke the membership.

Revocation of a membership implies the automatic and immediate revocation of the use of all

Technology Profiles for the Federation Member.

7.2 Liability and Indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and the governing body of the Federation for any faults and defects.

The Federation Operator and the governing body of the Federation 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 Federation membership agreement.

Neither the Federation Operator nor the governing body of the Federation 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 the governing body of the Federation due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services. For any other damage, the liability for damages in case of a breach of Federation Policy is limited to one thousand (1000) Euros.

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 the governing body of the Federation 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.

7.3 Interfederation

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

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.

7.4 Amendment

The Federation Operator has the right to amend the Federation Policy. Any such changes need to be approved by the governing body of the Federation and shall be communicated to all Federation Members and published on the website of the federation at least 90 days before they are to take effect.