aconet
Austrian Academic Computer Network

ACOnet Identity Federation policy

1. 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 RFC2119, see http://tools.ietf.org/html/rfc2119.

2. Introduction

The ACOnet Identity Federation is introduced to facilitate and simplify the offering of shared services across the (identity) federation. This is accomplished by using technologies to extend the scope of an (electronic) identity issued by one member of the federation to be valid across the whole federation.

This (federation) policy defines the federation by specifying procedures and practices which allow participating organizations to use available federation technologies for electronic identification and for access to authorization information about individuals, resources and other objects in the federation. This policy does not directly describe practices or procedures specific to any particular choice of federation technology.

Identity Management are the processes by which Identity Providers first issue and then manage identities throughout their life-cycles and by which they also make claims of identity for subjects (e.g. individuals, resources and other objects). A claim of identity is an electronic representation, using a specific identity management technology, of a set of attributes identifying a subject.

The ACOnet Identity Federation policy has three main parts: this document, which describes governance, membership and scope, a set of zero or more (identity) Assurance Profiles and a set of (federation) Technology Profiles. The Assurance Profiles and the Technology Profiles are based on current and evolving standards and best practices and are described in separate documents, available at http://www.aco.net/.

An Assurance Profile describes levels of trust in claims and organizations. An Assurance Profile allows a Service Provider to determine the degree of certainty that the identity of a subject presenting a claim of identity is truly represented by the presented claim. A commonly agreed-upon “Level of Assurance” represents this degree of certainty. Identity assurance is to a large extent independent of the technology used to convey claims of identity.

The Technology Profiles describe concrete realizations of the policy and Assurance Profiles in terms of specific technologies (e.g. SAML, eduroam etc.). By employing specific choices of technologies for identification and authorization this policy MAY be used to support federated identity for a wide range of applications. Technology Profiles govern the use of federation technology.

3. Purpose and Scope

The purpose of the ACOnet Identity Federation is to make it possible for (Application / Information) 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 ACOnet constituency (see http://www.aco.net/teilnehmer.html).

The scope of this 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 ACOnet Identity Federation.

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

4. Governance and Roles

4.1. Federation operator and legal entity

The ACOnet Identity Federation is a service of ACOnet, the Austrian National Research and Education Network. The operational and legal entity of ACOnet is the University of Vienna.

4.2. Federation technical advisory group and steering committee

All federation members are invited to delegate up to two representatives into the technical advisory group of the federation. The governance of the federation is supervised by the ACOnet steering committee, which is appointed by the ACONET association.

Any changes to this policy MUST be discussed in the technical advisory group and MUST be approved by the ACOnet steering committee before they are published on the ACOnet website.

ACOnet is responsible for maintaining formal ties with relevant national and international organizations.

4.3. ACOnet Identity Federation operations team

The operational management of the federation following the procedures described in this document is assigned to the ACOnet Identity Federation operations team. Information about the team members and other contact information are published on the ACOnet web site.

The ACOnet Identity Federation operations team is responsible for maintaining and publishing a list of ACOnet Identity Federation members along with information about which Assurance Profiles each federation member fulfills and which Technology Profiles each federation member implements.

The ACOnet Identity Federation operations team acts as a third line support for support requests from the second line support of federation members. Federation members MUST NOT redirect end user queries directly to the ACOnet Identity Federation operations team but MUST make every effort to ensure that only relevant problems and queries are sent to the ACOnet Identity Federation operations team.

4.4. ACOnet Identity Federation members

In order to become an Identity Provider in the ACOnet Identity Federation an organization MUST be eligible for ACOnet participation and MUST become a participant of ACOnet. In order to become a member of the ACOnet Identity Federation as a Service Provider only, and to receive identity information from ACOnet Identity Federation Identity Providers, a Service Provider is NOT REQUIRED to become a participant of ACOnet.

Federation members operating Identity Providers will have end users associated with them: these are individuals with an employment, student, business or other form of association with the federation member. Each federation member is responsible for its own end users. In particular each federation member is responsible for fulfilling the requirements of applicable laws with respect to its own end users. ACOnet or the ACOnet Identity Federation is not liable for any specific legal requirements of the services described in section 2 (Introduction).

Federation members are responsible for first line (e.g. service desk or equivalent) and second line (technical support and problem classification) support for its end users. Membership in the ACOnet Identity Federation does not mandate any specific service level for this service, but federation members are encouraged to maintain a service desk for normal office-hours in the local time zone of the federation member for user queries. Each end user SHALL BE identified by at least one ACOnet Identity Federation member.

Every federation member SHOULD publish a local acceptable use policy for all services covered by the ACOnet Identity Federation policy. The local acceptable use policy MUST contain information about any activities and/or behavior, which is deemed unacceptable when using the service. Federation members are encouraged to make user acknowledgement of the acceptable use policy a part of the service access process.
Every Service Provider MUST publish a privacy policy for all services covered by the ACOnet Identity Federation policy.

5. Identity Management Practice Statement

Each Identity Provider that wishes to become a member of the ACOnet Identity Federation SHOULD create, publish and maintain an Identity Management Practice Statement. The Identity Management Practice Statement is a description of the Identity Management life cycle, including a description of how identity subjects 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. The processes, practices and technologies described MUST be able to support a secure and consistent identity management life cycle. Assurance Profiles MAY impose specific requirements.
The Identity Management Practice Statement is evaluated against claims of compliance with Assurance Profiles.

6. Procedures

6.1. Membership application

In order to become a member of the ACOnet Identity Federation an organization formally applies for membership. Detailed information and application forms are published on the ACOnet Identity Federation website. For Identity Providers the membership application SHOULD include an Identity Management Practice Statement.
The ACOnet Identity Federation operations team evaluates each membership application, including (if applicable) the Identity Management Practice Statement. The evaluation process involves checking, if the applying organization fulfills the requirements of the ACOnet Identity Federation policy.
The ACOnet Identity Federation operations team communicates acceptance or denial of the membership application to the applying organization in written form, including the reason for denying the application (if applicable).

6.2. Membership cancellation

The ACOnet Identity Federation member MAY cancel an ACOnet Identity Federation membership at any time by sending a written request to the ACOnet Identity Federation Operations Team. A cancellation of the ACOnet Identity Federation membership implies the automatic and immediate cancellation of the use of all Technology Profiles for the organization.

6.3. Membership revocation

A federation member who fails to comply with the ACOnet Identity Federation policy MAY have its membership in the ACOnet Identity Federation revoked by the ACOnet steering committee.
If the ACOnet Identity Federation operations team is aware of a breach of policy by a federation member, the ACOnet Identity Federation operations team MAY issue a formal notification of concern. If the cause for the notification of concern is not rectified within the adequate time specified by the ACOnet Identity Federation operations team, the ACOnet steering committee MAY issue a formal notification of impending revocation, including an adequate time limit specified by the ACOnet steering committee for rectification of the breach by the federation member, after which the ACOnet steering committee MAY choose to revoke the ACOnet Identity Federation membership.
A revocation of the ACOnet Identity Federation membership implies the automatic and immediate revocation of the use of all Technology Profiles for the organization.

7. Audit

The ACOnet Identity Federation policy does NOT REQUIRE any audit. However, Assurance Profiles MAY impose audit requirements on federation members.

8. Fees

The ACOnet steering committee will decide on fees to be paid by the ACOnet Identity Federation members, to cover the operational costs of the ACOnet Identity Federation. Such a fee proposal SHOULD be made no later than on June 15th and the approval by the steering committee MUST be made - and announced to the federation members - no later than on July 1st each year for the following year. In absence of an approved fee proposal the fees for the following year will default to the fees from the current year.

9. Liability

The University of Vienna offers this service on an AS IS basis, without any warranties or liabilities to the ACOnet Identity Federation members or their users. Neither the ACOnet Identity Federation operations team nor the ACOnet steering committee nor the University of Vienna SHALL be liable for damage caused to the federation member or its end user. ACOnet Identity Federation members SHALL not be liable for damage caused to the ACOnet Identity Federation operations team or the ACOnet steering committee due to the use of the ACOnet Identity Federation services, service downtime or other issues relating to the use of the ACOnet Identity Federation services.
The ACOnet Identity Federation member is REQUIRED to ensure compliance with applicable laws. The ACOnet Identity Federation operations team or the ACOnet steering committee SHALL NOT be liable for damages caused by failure to comply with any such laws on behalf of the ACOnet Identity Federation member or its end users relating to the use of the federation services. For any other damage, the liability for damages in case of a breach is limited to one thousand (1000) euros.
The ACOnet Identity Federation operations team and the ACOnet Identity Federation member SHALL refrain from claiming damages from other ACOnet Identity Federation members for damages caused by the use of the ACOnet Identity Federation services, service downtime or other issues relating to the use of the ACOnet Identity Federation services.
Neither party SHALL be liable for any consequential or indirect damage.

10. Governing Law, Dispute resolution

The ACOnet Identity Federation Member Agreement and this policy is governed by the Laws of the Republic of Austria, with the exclusion of its rules regarding international conflict of laws and the UN-Convention on the Trade of Goods. All disputes SHALL be settled before the Commercial Court for Vienna (Handelsgericht Wien).

11. Copyright