eduID.cz Federation Policy

Version 1.1

Table of Contents

1. Introduction

1.1. *eduID.cz* is a Czech National Academic Identity Federation providing its members with a framework for sharing user identities while controlling access to network services, adhering to personal data protection principles.

1.2. This Document defines the organization Policy to be used in the operation of the *eduID.cz* Federation.

2. Definition of Terms

The Policy relies on the following terms:

2.1. Identity Federation

An association of Identity Providers and/or Service Providers.

2.2. Identity Provider

A service producing or managing identity information and providing authentication services to Service Providers.

2.3. Service Provider

Provides a service (such as network connectivity, application, computing power, data store access, etc.); relies on authentication and user *attributes* provided by Identity Providers to control access to that service.

2.4. Attribute

A data structure used to describe object properties. *Service Providers* typically rely on *attributes* provided by Identity Providers, describing *users*, to control access to their services.

2.5. Federation Operator

Provides central services to the federation (registering members, maintaining *Metadata*, etc.).

2.6. Metadata

Details of Federation members, their roles, services provided, technical specifications for their services, contacts and other operation-related information.

2.7. eduID.cz

The official title of the Czech Academic Identity Federation.

2.8. Federation Member

An organization that has joined the Federation to act as an *Identity Provider* or a *Service Provider*.

2.9. Identity/Service Provider Operator

Federation Member operating an *Identity Provider* or a *Service Provider*.

2.10. Administrative Contact

A person appointed by a Federation Member. Acts on behalf of the Federation Member, appoints Technical Contacts for that Member.

2.11. Technical Contact

A person appointed by an *Administrative Contact* of an Operator of an Identity/Service Provider. Represents the Identity Provider or the Service Provider, dealing with the Federation Operator.

2.12. National Research and Educational Network Access Policy (further referred to as "AP")

A document defining conditions for entities accessing the National Research and Educational Network.

2.13. Identity

The sum of attributes describing the given entity (typically a *User*).

2.14. Authentication Data

Information used by *Identity Providers* to verify the identities of *Users* (Typically user names and passwords).

2.15. User

A person accessing the service provided by a *Service Provider.*

3. General Provisions

3.1. *eduID.cz* is used by organizations connected to the CESNET2 Network, pursuing their research and education-related objectives.

3.2. *eduID.cz* Members must adhere to this Policy while using the Federation's services. Policy violations will result in cancelling the offending party's membership in the Federation.

3.3. *eduID.cz* Members using the services of the Federation are obliged to maintain the security of their Users' personal data, at least to the extent defined by Law and this Policy.

3.4. Federation Members adhere to technical conditions declared by the Federation Operator while operating their technical equipment.

4. The Definition of Federation Member Roles and Obligations

4.1. Federation Operator

4.1.1. The Role of the *eduID.cz* Federation Operator (further referred to as the *Federation Operator*) is fulfilled by the CESNET Association.

4.1.2. The Federation Operator co-ordinates the functioning of the Federation, and oversees adherence to the Federation Policy.

4.1.3. The Federation Operator provides technical support to member organizations, regarding the connection of their technical equipment into the Federation, and resolving possible security incidents.

4.1.4. Based on discussions with Members, the Federation Operator defines technical rules for the operation of *eduID.cz*.

4.1.5. Based on discussions with Members, the Federation Operator defines the syntax and semantics of mandatory and recommended attributes to be used within *eduID.cz*.

4.1.6. The Federation Operator registers and de-registers Federation Members.

4.1.7. The Federation Operator maintains and publishes Federation Metadata based on details provided by Members.

4.1.8. The Federation Operator is not responsible for data transferred between Identity Providers and Service Providers.

4.1.9. If absolutely necessary (e.g. for security or operation-related reasons), the Federation Operator is entitled to excluding individual Members from Metadata published.

4.1.10. Based on discussions with Members, the Federation Operator enters *Inter-Federation Peering* contracts. Members must be advised of any such contract concluded.

4.1.11. The Federation Operator has the right to resolve disputes between Federation members.

4.1.12. All communication with the Federation Operator is carried out through contacts listed at the www.eduID.cz information portal.

4.2. Identity Providers

4.2.1. Identity Providers manage user identities, including authentication data. The Identity Provider Operator is responsible for securing such data and protecting them against abuse.

4.2.2. In case of compromised user authentication data, or a reasonable suspicion thereof, the Identity Provider blocks authentication services for affected users immediately, until a new set of authentication data is issued.

4.2.3. Identity Providers keep records of user authentication as well as attributes provided to individual Service Providers, making it possible to determine the actual identity of a user. Such records must be kept for the period of three months.

4.2.4. Identity Provider Operators are responsible for the correctness and entirety of data provided to Service Providers.

4.2.5. Identity Providers provide attributes as defined by the list of mandatory and recommended attributes published by the Federation Operator. If agreed with a Service Provider, other attributes may be provided as well.

4.2.6. Identity Provider Operators impose *eduID.cz* rules, including this Policy, on their users.

4.2.7. Identity Provider Operators co-operate with Service Provider Operators and with the Federation Operator to resolve security incidents and Federation rules violations.

4.2.8. Identity Provider Operators provide users with technical support and information necessary to use the Federation's services. Identity Provider Operators are particularly responsible for instructing their users on proper and secure handling of authentication data.

4.2.9. Each Identity Provider Operator appoints at least one person as an Identity Provider's technical contact (to extend availability, appointing more than one technical contact is preferable). Technical contacts communicate with the Federation Operator and technical contacts of Service Providers, resolve technical issues and security incidents. Replacements of technical contacts need to be communicated to the Federation Operator without delay.

4.3. Service Providers

4.3.1. Only attributes necessary for the provision of their service may be requested by Service Providers from Identity Providers. Lists of required attributes will be handed over to the Federation Operator, together with a description of the service.

4.3.2. Service Provider Operators undertake to use data provided by Identity Providers solely for the purpose of facilitating access to their services. Most importantly, data must not be shared with third parties.

4.3.3. Service Provider Operators co-operate with Identity Provider Operators and with the Federation Operator to resolve security incidents and Federation rules violations.

4.3.4. In case of a security incident occurring on an equipment or in a system used to provide a service, the Service Provider Operator immediately notifies the Federation Operator as well as all Identity Providers whose users access the affected service.

4.3.5. Each Service Provider Operator appoints at least one person as a Service Provider's technical contact (to extend availability, appointing more than one technical contact is preferable). Technical contacts communicate with the Federation Operator and technical contacts of Identity Providers, resolve technical issues and security incidents. Replacements of technical contacts need to be communicated to the Federation Operator without delay.

4.4. Users

4.4.1. Users are obliged to observe rules defined by their Identity Provider Operators and Service Provider Operators. In case these rules differ, more restrictive option applies.

4.4.2. Users are fully responsible for their authentication data as well as for possible abuse thereof. Users need to act in such a way that prevents abuse of their authentication data. In case of authentication data compromise, users are obliged to notify their Identity Provider Operators without delay.

4.4.3. Users are obliged to follow instructions issued by their Identity Providers, Service Providers and the Federation Operator.

5. Joining the Federation

5.1. The *eduID.cz* Federation may be joined by any organization that fulfils the AP. Such an organization also needs to meet technical conditions and adhere to this Policy. Final decision on admitting an organization into the *eduID.cz* Federation belongs to the Federation Operator.

5.2. Organizations that do not fulfil the AP may join the federation in case they provide services to members who have joined under section 5.1. Organizations joining the Federation in this manner are not allowed to run identity provider services. Final decision on admitting an organization into the *eduID.cz* Federation belongs to the Federation Operator.

5.3. For the purpose of this Policy, the act of “joining” is understood to be carried out by officially appointing an administrative contact, i.e. a person representing the organization in its dealing with the Federation Operator, and appointing technical contacts responsible for individual Identity Providers and Service Providers operated by the organization.

5.4. By joining the *eduID.cz* Federation, an organization agrees with this Policy in full and without reservations.

5.5. *eduID.cz* membership is free of charge for organizations.

5.6. Organizations need to provide technical infrastructure that meets conditions published at the www.eduID.cz information portal.

5.7. By joining the *eduID.cz* Federation, an organization agrees to co-operate with the Federation Operator, and follow the Operator's instructions in due course.

6. Leaving the Federation

6.1. Should a member organization decide to leave the Federation on its own volition, the intention needs to be communicated to the Federation Operator in writing, at least one month in advance. The Federation Operator will make preparations for technical disconnection of the member within that time frame and publish the information at the www.eduID.cz information portal.

6.2. Should the Federation Operator decide to cancel an organization's membership, that decision needs to be communicated to the affected Member and published at the www.eduID.cz information portal. Data concerning services provided by that Member will be removed from Metadata.

7. Security Incident Resolution Guidelines

Once a security incident (or a violation of the Policy, AP or other binding rules regarding the operation of the network or services) is identified, all Federation Members need to put maximum effort into resolving the incident as quickly as possible. Breaching this obligation will be considered as a violation of this Policy by parties responsible. The Federation Operator needs to be notified of all security incidents without delay.

8. Competence, Adherence to Policy, Sanctions

8.1. This Policy is being executed by the Federation Operator, i.e. the CESNET Association.

8.2. There can be no legal claim of *eduID.cz* Federation membership.

8.3. All modifications to this Policy need to be announced three months in advance and discussed with all federation members as possible. In case of a new rule being deemed unacceptable by a member, that member is obliged to leave the federation by the date the new rule becomes effective (following Section 6 of this Document). Parties that fail to do so agree with the new wording of the Federation Policy without reservations.

8.4. 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.

9. Responsibility

Neither the *eduID.cz* Czech National Academic Identity Federation, nor the CESNET Association acting as its Operator, provide any guarantee as to the availability or functionality of systems connected to the Federation.

10. Final Provisions

This document becomes effective on 1 October 2008.

Done in Prague on 10 September 2008

Ing. Jan Gruntorád, CSc.,
Director General, CESNET Association