

Korean Access Federation Identity Federation Policy

JongUk Kong, Jinyong Jo, Heejin Jang
Last modified: 2nd, March 2021, V1.1
support@kafe.or.kr



This work is licensed under a [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

Revision history

| Ver. | Clause | Clause before revision | Issuer | Date |
|------|--------|--|-------------------------------|-------------|
| 1.1 | 3.3.5 | Must ensure its IT systems used in implemented Technology Profiles Must be operated with the most reasonable security measures known to date | J. Jo | Mar 2, 2021 |
| 1.0 | | - | J. Kong, J. Jo, H. Jang | Nov 4, 2016 |

I. Definitions and Terminology

In this section basic terms that are used in this document are defined.

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://www.ietf.org/rfc/rfc2119.txt>.

1. ID Provider: A service/server/organization that authenticates users and collates attributes about them based upon information maintained by the organization and provides these authentication results and attributes to participating organizations (hereinafter called IdP).
2. Service Provider: A server/service/organization that processes identity information received from the IdP, including authentication results and attributes (hereinafter called SP).
3. Metadata: Trust and addressing information for all IdPs and all SPs in the Federation.
4. Attribute: A piece of information describing the End User, his/her properties or roles in an Organization.
5. ID Federation: An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
6. Federation Member: An organization or a part of an organization that has participated ID Federation by agreeing to be bound by the Federation Policy.
7. Federation Operator: Organization providing Infrastructure for Authentication and Authorization to Federation Members
8. Technology Profile: Documents that describe concrete realizations of the Policy and Assurance Profiles in terms of specific technologies (e.g. SAML, eduroam, etc.).

II. Introduction

The Korean Access Federation Identity Federation (KAFE) is introduced to facilitate and simplify the introduction of shared services across KAFE. 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.

This KAFE Policy document defines the Federation by defining the KAFE 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 KAFE.

This document, together with its appendices constitutes KAFE Policy. The current list of all appendices is available on the website of KAFE.

III. Governance and Roles

3.1 Governance

The governance of KAFE is delegated to the KAFE steering committee (hereinafter called the Committee). In addition to what is stated elsewhere in KAFE Policy the Committee is responsible for:

1. Setting criteria for membership for KAFE.
2. Determining whether to grant or deny an application for membership in KAFE.
3. Revoking the membership if a KAFE Member is in a breach of the Policy.
4. Determining the interfederation agreement with other federations.
5. Determining future directions and enhancements for KAFE together with the Federation Operator who prepares the plans.
6. Maintaining formal ties with relevant national and international organisations.
7. Approving changes to the Federation Policy prepared by the Federation Operator.
8. Deciding on any other matter referred to it by the Federation Operator.

3.2 Obligations and Rights of Federation Operator

KAFE is operated by the Korea Research Environment Open NETwork (KREONET). In addition to what is stated elsewhere in KAFE Policy, the Federation Operator is responsible for:

1. Secure and trustworthy operational management of KAFE and providing central services following the procedures and technical descriptions specified in this document and its appendices.
2. Provides support services for KAFE Members' appropriate contact persons to work out operational problems regarding the Federation services.
3. Acts as centre of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within KAFE.

4. Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation activities and work with other Identity Federations in the area of harmonization.
5. Promoting the idea and concepts implemented in KAFE so prospective Federation Members learn about the possibilities of KAFE.

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

1. Move to strike a name off a Federation Member that is disrupting secure and trustworthy operation of KAFE.
2. Move to amend KAFE Policy.
3. Publish a list of KAFE Members along with information about which profiles each KAFE Member fulfills or implements, for the purpose of promoting KAFE.
4. Publish some of the data regarding KAFE Member using specific Technology Profile. Definition of which data may be published is provided in appropriate Technology Profiles.

3.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in KAFE Policy all KAFE Members:

1. Shall appoint and name an administrative contact for interactions with the Federation Operator.
2. 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 KAFE or any of its Members.
3. Must comply with the obligations of KAFE Policy.
4. Must comply with the obligations of the Technology Profiles which it implements.
5. Shall use all reasonable efforts to work towards ensuring that its IT systems used in implemented Technology Profiles are operated with the most reasonable security measures known to date.
6. If a KAFE Member processes personal data, the Member Must comply with applicable data protection laws of Korea.

IV. Eligibility

The Committee sets out eligibility criteria that determines who is able to become a KAFE Member.

An eligible member is an organization or a part of an organization that qualifies under any of the following items.

1. A Korean university, junior college, college of technology, or inter-university research institute that intends to deploy an IdP or SP.
2. A Korean national or public research and development organization; or, a government-affiliated corporation that is dedicated to research or support of research that intends to deploy an IdP or SP.
3. An organization deploying an SP for the purpose of providing R&E applications and services to organizations defined in the preceding items 1 and 2.
4. An organization deploying an IdP for the purpose of using R&E applications and services provided by the organizations defined in the preceding items 1 to 3 and whose participation in KAFE is decided by the Committee to be beneficial to all KAFE members (in case of this organization, its IdP metadata is not exported to other federations from KAFE).

V. Procedures

5.1 How to Join

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

The Committee shall recognize the application if an organization is eligible.

If the application is denied, this decision and the reason for denying the application are communicated to the applying organization by the Federation Operator.

5.2 How to Withdraw

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

VI. Legal conditions of use

6.1 Termination

The Committee may revoke the membership of a KAFE Member who submitted the application with false entry, impeded KAFE operation and damaged trust of KAFE, was disqualified, or failed to comply with the Policy.

If the Federation Operator is aware of the cases stated above, the Federation Operator may issue a formal notification of concern within five working days. If the cause for the notification of concern is not rectified within 60 days, the Committee may issue a formal notification of the membership revocation.

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

6.2 Liability and indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and the Committee for any faults and defects meaning amongst other that KAFE 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 and the Committee may not be held liable for any loss, damage or cost that arises as a result of KAFE Member connection to or use of Federation services, or other systems to which KAFE Member obtains access in accordance with the agreement. This limitation of liability does not however apply in the case of gross negligence or intent shown by Federation Operator personnel.

Neither the Federation Operator nor the Committee shall be liable for damage caused to the KAFE Member or its End Users. KAFE Member shall not be liable for damage caused to the Federation Operator or the Committee 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 KAFE Members, KAFE Member will have no liability to any other KAFE Member solely by virtue of KAFE Member's membership of the Federation. In particular, membership of KAFE alone does not create any enforceable rights or obligations directly between KAFE Members. Federation Operator and the KAFE Member shall refrain from claiming damages from other KAFE Members for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. KAFE Member may, in its absolute discretion, agree variations with any other KAFE Member to the exclusions of liability. Such variations will only apply between those KAFE Members.



KAFE Member is required to ensure compliance with applicable Korean laws. Neither the Federation Operator nor the Committee shall be liable for damages caused by failure to comply with any such laws on behalf of KAFE 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 interfederation 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 KAFE Members remain bound only by their own respective laws and jurisdictions.

KAFE Member and Federation Operator shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

6.3 Jurisdiction and dispute resolution

Disputes concerning KAFE Policy shall be settled primarily through negotiation. If the issue cannot be resolved through negotiation, any disputes shall be resolved through applicable Korean laws.

6.4 Interfederation

In order to facilitate collaboration across national and organizational borders KAFE 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 KAFE.

6.5 Amendment

The Federation Operator has the right to amend KAFE Policy from time to time. Any such changes need to be approved by the Committee and shall be communicated to all KAFE Members in written form at least 90 days before they are to take effect.

VII. Copyright

This work is © KREONET used under the Creative Commons Attribution-ShareAlike 3.0 Unported license (<http://creativecommons.org/licenses/by-sa/3.0/>). It is heavily based on the “Identity Federation Policy template document”, written by Marina Vermezovic, Mikael Linden, Natalija Radosevic, Peter Schober, and Brook Schofield available <http://www.terena.org/activities/eurocamp/oct12/slides/Identity%20Federation%20Policy%20Template%20v0.3.docx>



This English version policy is for reference only. The Korean version take priority over the English version if there are discrepancies between them.