Policy Framework for joining eduGAIN

일자	2016년 10월 20일
부서	첨단연구망센터 첨단연구망응용지원실
작성자	공정욱, 조진용, 장희진, 이경민

Policy Framework for joining eduGAIN

1. Introduction

1.1. Purpose of this Paper

KAFE decided to join eduGAIN so that the Korean research and education community could access to global contents, services and resources related to research and education. Therefore, the Korean students, researchers and educators can access online services while minimizing the number of accounts users and service providers have to manage – reducing costs, complexity and security risks.

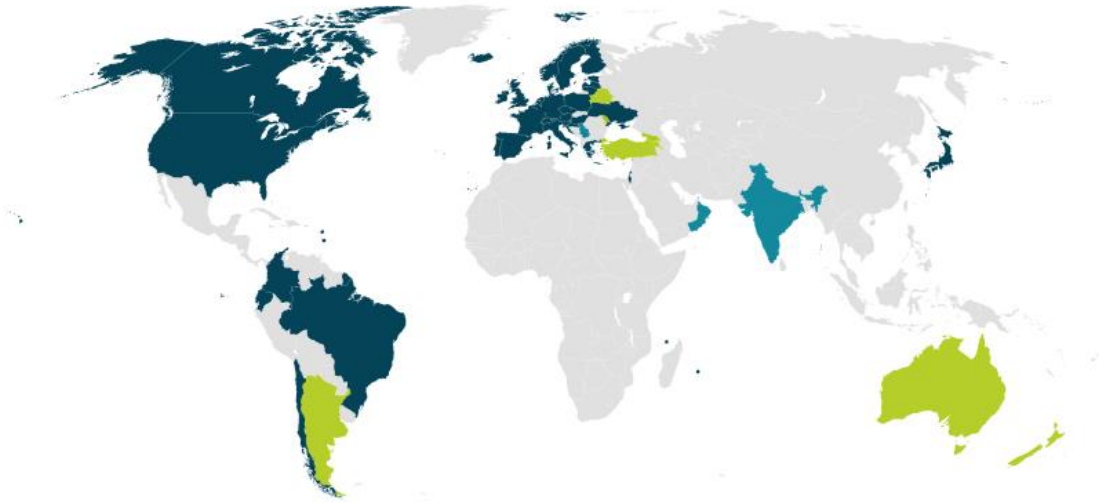
This technical paper lists the documents for joining eduGAIN: eduGAIN Declaration, the English version of the Federation Policy, the English version of Metadata Registration Practice Statement, and optional profiles like metadata profile, attribute profile, SAML 2.0 WebSSO profile, etc.

KAFE staff have worked for many months to write the documents. This paper presents the result of that work.

1.2. What is eduGAIN?

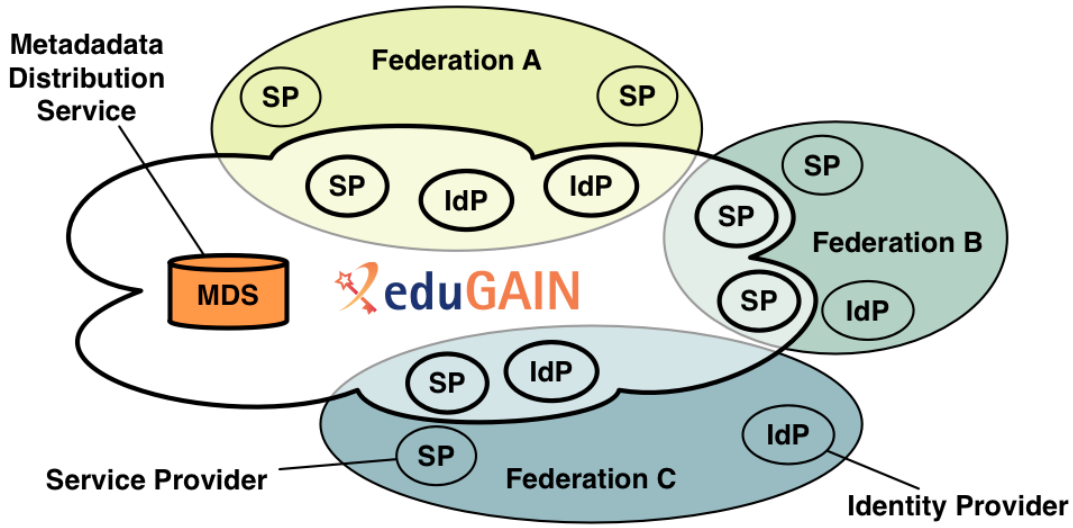
eduGAIN is a service developed within the GÉANT Project - a major collaboration between European national research and education network (NREN) organisations and the European Union.

eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.



eduGAIN World Map - eduGAIN Joining Candidate

This exchange of information contributes to the seamless operation of services, whether they are developed within the GÉANT Project, provided by other communities represented by, or associated with, the GÉANT partners, or provided by commercial Service Providers.



eduGAIN Service diagram - How eduGAIN works

Features:

- Enables trustworthy exchange of information between federations without many bilateral agreements
- Reduces the costs of developing and operating services
- Improves the security and end-user experience of services
- Enables service providers to greatly expand their user base
- Enables identity providers to increase the number of services available to their users

2. Policy Declaration

GÉANT

eduGAIN Policy Declaration

The Federation named below ("the Federation") hereby declares, in respect of other federations participating in eduGAIN as listed on the eduGAIN website ("the Participating Federations") that it wishes to participate in eduGAIN, and that it will comply with the eduGAIN Policy Framework, and that:

1. It will publish technical descriptions of networked computers that act as AAI endpoints (for example to provide the functions of identity provider, attribute provider or service provider) ("the Entities") which have been validated for use in the Federation according to its normal operational standards. These descriptions will be treated as non-confidential.

2. It will make some or all Entity descriptions provided to eduGAIN by other Participating Federations available to Members[1] of the Federation, who may make use of them at their own discretion to establish trusted communications between Entities.

3. It will promptly publish any subsequent changes to Entity descriptions previously published.

4. It will inform the eduGAIN Operational Team promptly of any changes affecting either the validation of Entities or the process for publishing Entity descriptions.

5. It will provide such assistance to other Participating Federations as they may reasonably request concerning the publication or use of Entity Descriptions.

6. It will provide the eduGAIN Operational Team on request with such documentation or agreements as necessary to clarify the Federation's registration procedures and thus the levels of trust which may be placed in the Federation's registered metadata.

7. The behaviour of any Member of any Participating Federation whose Entity description is published shall continue to be bound only by the rules of that Participating Federation.

8. In particular any complaint about a Member shall be made to the operator of its Participating Federation and dealt with between that Member and that operator according to the rules of that Participating Federation and subject only to that Participating Federation's governing law and jurisdiction.

9. Neither the existence of this declaration, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Members and operators remain bound only by their own respective laws and jurisdictions.

10. In particular this declaration creates no rights of membership, nor of access to services, between Members of any federation.

---

[1] Throughout the eduGAIN Policy Framework, the term Member refers to any organisation that has signed an agreement with a federation operator to cover the registration, verification and publication of Entity descriptions. This may include organisations referred to as Members, Participants or otherwise by those federation operators.

11. Any disagreement between Participating Federations shall be resolved by discussion between the respective Participating Federations or their successors and assigns.

12. No financial consideration will be expected between the Federation and other Participating Federations as federation operators and any financial consideration between Members or Members and operators is outside the scope of this declaration.

13. It will, in the event that it no longer wishes to participate in eduGAIN, give timely advance notice to the eduGAIN Operational Team in accordance with the eduGAIN constitution.

In case of translations, the authoritative version of this Declaration shall remain the version in English.

Should any provision of this Declaration be found invalid, illegal or unenforceable in any jurisdiction, this will not affect the validity, legality or enforceability of any other provision. The Federation agrees to replace any such provision with a provision having substantially the same effect but which is not invalid, illegal or unenforceable.

Signed on behalf of

KAFE (Korean Access FEderation) ..... (the Federation)

on August 18, 2016 ..... (Date)

by 박형우 ..... (Signature)

HYOUNG WOO PARK, Director ..... (the name in capital letters)

of KREONET, KISTI ..... (Organisation)

3. KAFE Policy

KAFE

Korean Access Federation Policy

KREONET

Republic of Korea

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. Collaboration Applications Services: Application Softwares and Services that support researchers who are away from each other for online collaboration.

6. ID Federation: An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.

7. Federation Member: An organization or a part of an organization that has participated ID Federation by agreeing to be bound by the Federation Policy.

8. Federation Operator: Organization providing Infrastructure for Authentication and Authorization to Federation Members

9. 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. Must ensure its IT systems that are used in implemented Technology Profiles are operated securely

6. If a KAFE Member processes personal data, the Member Must comply with applicable data protection laws and must follow the regulation determined separately by the Committee.

7. Must agree to provide third parties with a operation contact by the Federation Operator for enhancing the usage of KAFE services.

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 academic collaboration applications services to organizations defined in the preceding items 1 and 2.

4. An organization deploying an IdP for the purpose of using collaboration applications 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.

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.

_____

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

4. Metadata Registration Practice Statement

Metadata Registration Practice Statement for KAFE

Federation Name: KAFE
Federation Operator: KREONET, Republic of Korea
Federation Web Page: https://coreen.kreonet.net
Date of last change: 20160816

KREONET operates identity federation (KAFE) on behalf of research and educational institutions in the Republic of Korea.

This document describes the Registration practices for both Identity Providers and Service Providers, as well as information on metadata aggregation for eduGAIN.

1. Identity Provider Practices

1.1 Identity Provider Registration Practices

For an Identity Provider to join KAFE, the following requirements must be met:

- The institution must have submitted a completed membership service agreement signed by official representative(s).
- The institution must have passed technical validation to KAFE test environment.
- The institution must provide technical and administrative contact information.
- KAFE operates an opt-in model for institutions, where the institution must agree explicitly to be connected to a specific Service Provider and to release attributes to this specific Service Provider.

1.2 Identity Provider Registration Practices for eduGAIN

There are no additional eduGAIN practices for Identity Providers.

2. Service Provider Practices

2.1 Service Provider Registration Practices

For a Service Provider to join KAFE, the following requirements must be met:

- The Service Providers must have signed KAFE Service Provider contract.
- The Service Provider must provide KAFE with a description of the service.
- The Service Provider must provide KAFE with a description of the technical and administrative contact details.
- The Service Provider must provide KAFE with the list of minimally required attributes for using the service.

2.2 Service Provider Registration Practices for eduGAIN

The practices below are in addition to the “Service Provider Registration Practices” above.

- KREONET will only publish metadata to eduGAIN for Service Providers that are connected to KAFE production environment.
- The Service Provider must explicitly request to connect to eduGAIN through KAFE.
- The Service Provider must provide eduGAIN compliant SAML 2.0 metadata to KAFE.
- The metadata provided by the Service Provider that is re-published by KAFE to eduGAIN is updated by KAFE operational team by request of the Service Provider. Service Providers can request an update of their metadata by contacting the KAFE operational team.

KREONET validates the Service Provider information including the attribute requirements, before accepting the Service Provider to the production environment.

5. Technology Profile

Technology Profile for KAFE

Federation Name: KAFE
Federation Operator: KREONET, Republic of Korea
Federation Web Page: https://coreen.kreonet.net
Date of last change: 20160816

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL in this document are to be interpreted as described in RFC 2119.

1. SAML Technical Standards

The SAML technical standards used in KAFE SHALL be based on the following standards specified by the OASIS Security Services Technical Committee.

1.1 SAML 2.0 Core

Specifies the technical requirements for conformance with SAML 2.0 and the documents of which they consist.
(http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

1.2 SAML 2.0 Profiles

Specifies the identifiers used between systems, binding support, and use of certificates and keys.
(http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

1.3 SAML 2.0 Metadata

Specifies the rules for standardized notation of metadata.
(http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

2. Protocol

These Standards are designed so that an IdP or SP (hereinafter called an "entity") participating in KAFE will be able to provide as broad a range of services as possible. To this end, all entities participating in KAFE SHOULD use the protocol standardized within KAFE. The protocol SHALL meet the requirements herein for authentication request and authentication response.
As software for use in KAFE, SimpleSAMLphp is RECOMMENDED as software implementing the above kind of protocol.

2.1 Authentication Request

HTTP-bound SAML protocol authentication request messages SHOULD be implemented in conformity with the Web Browser SSO Profile specifications stipulated in the SAML technical standards SAML 2.0 Profiles 4.1.3 and 4.1.4.

2.2 Authentication Response

HTTP-bound authentication response messages containing SAML assertions SHOULD be implemented in conformity with the Web Browser SSO Profile specifications stipulated in the SAML technical standards SAML 2.0 Profiles 4.1.3 and 4.1.4.

Either the authentication response message or the authentication assertion SHOULD be signed, and the authentication assertion SHOULD be encrypted.

2.3 SimpleSAMLphp

SimpleSAMLphp (simplesamlphp.org) is a SAML-based software package led by UNINETT (www.uninett.no). The main focus of SimpleSAMLphp is providing support for SAML 2.0 as a Service Provider (SP) and SAML 2.0 as an Identity Provider (IdP).

SimpleSAMLphp 1.13 or newer are RECOMMENDED for SAML 2.0 IdP and SP.

3. Attribute Information

Attribute information is information used by each entity in deciding whether to authorize a user.

See the appended list of Supported Attribute Information Specifications for the attribute information that can be used in KAFE.

3.1 Using Attribute Information

All attribute information defined in KAFE has a unique URI. The attributes used by entities SHOULD to the extent possible be selected from the appended list of Supported Attribute Information Specifications.

In case a desired attribute is not on the list of Supported Attribute Information Specifications, an entity SHALL be able to issue a request to KAFE for adding a new attribute. KAFE SHALL then decide on whether to add the attribute to the list.

Note that attributes other than the listed ones MAY be used for services not going through KAFE.

3.2 Attribute Information Trustworthiness

An IdP SHOULD guarantee the attributes of users belonging to its own organization. It SHOULD NOT guarantee the attributes of users not belonging to its own organization. If, however, an organization manages a user not belonging to it, such a user's attributes MAY be guaranteed by performing special attribute management to prevent illegal access to an SP.

3.3 Attribute Information Validation

A SP SHOULD perform a validation to ensure that all incoming attribute information has been issued by a trusted authority.

3.4 Attribute Information Levels

An SP, in providing services, SHOULD make clear to users the required attribute information and the level of that attribute information. It is RECOMMENDED that the levels "required," "recommended" and "optional" beclearly indicated along with the purpose for use of the attribute information.

3.5 Scope

A scope MUST match the domain indicated in the EntityID. Each IdP MUST indicate this scope in the metadata, and MUST make use of the same scope when using a scoped attribute. An SP SHALL determine the scope of an attribute received in an assertion by comparing it with the scope included in IdP metadata.

3.6 Specification of eduPersonTargetedID

eduPersonTargetedID MUST include NameQualifier, SPNameQualifier and Opaque ID, and MUST conform the following specification.

- eduPersonTargetedID

  <saml:NameID xmlns:saml = "urn:oasis:names:tc:SAML:2.0:assertion" NameQualifier = “[entityID of IdP]” "SPNameQualifier = "[entityID of SP]"> [opaque ID]</saml:NameID>

4. Metadata

KAFE uses the metadata specified below.

4.1 Metadata Specifications

The SAML 2.0 metadata specifications (see 1.3 SAML 2.0 Metadata) SHOULD be followed.

4.2 Kinds of Metadata

The following two kinds of metadata are used in KAFE.

- Entity metadata: Metadata submitted to KAFE by each entity, and indicating information
- Federation metadata: Metadata created by KAFE including that of all participating entities

4.3 Submission of Entity Metadata

All organizations participating in KAFE MUST submit entity metadata for each of their entities to KAFE.

4.4 Contents of Entity Metadata

In case of renewal of a server certificate that certifies the server of an organization participating in KAFE or changes to the organization's metadata, the organization MUST submit the latest version of the metadata promptly to KAFE.

It is RECOMMENDED that, to the extent possible, information identifying individuals not be included in the metadata. For example, in metadata such as the <ContactPerson> tag that requires personal information.

Note that the entity metadata submitted to KAFE, including any personal information included in it, will be made public on the Web (repository). Accordingly, the administrator SHALL be assumed to have consented to this at the time of submitting the entity metadata or at the time of application.

KAFE SHALL use the entity metadata submitted by each organization for the following purposes only:

- Validating the items included in the entity metadata
- KAFE administration, management, and operation
- Addition and updating of federation metadata
- Distributing federation metadata to KAFE member organizations or making it public on the Web (repository)
- Registration in a discovery service (DS), IdP, or SP

4.5 Entity Metadata <Organization> Element

An IdP SHOULD include the following information in the <Organization> element of the submitted entity metadata. In case the organization has multiple entities, each entity MUST be identified.

- OrganizationName
  : <md:OrganizationName xml:lang="en">name</md:OrganizationName>
- OrganizationDisplayName:
  : <md:OrganizationDisplayName xml:lang =
  "en">name</md:OrganizationDisplayName>
- OrganizationURL
  : <md:OrganizationURL xml:lang =
  "en">http://www.kreonet.net/</md:OrganizationURL>
- ContactPerson:
  <md:ContactPerson contactType="technical">
  <md:GivenName></md:GivenName>
  <md:SurName></md:SurName>
  <md:EmailAddress></md:EmailAddress>
  </md:ContactPerson>

4.6 Notification of Personal Information Protection Policy

SP MUST notify personal information protection policy and put the URL in the entity metadata. Notified personal information protection policy MUST comply with Korean personal information protection law.

- E.g., 'privacypolicy' => 'https://my.school.ac.kr/privacypolicy'

4.7 Entity ID of Entity Metadata

When compiling federation metadata, the Committee MAY assign an ID distinguishing each of the submitted entity metadata, as an <EntityDescriptor> ID attribute in entity metadata.

4.8 Submission and Publishing of Federation Metadata

The Committee MUST validate all the submitted entity metadata, then add it to the federation metadata, sign it, and create the latest federation metadata, thereby making this metadata available to each member organization.

Federation metadata is valid for 14 days, and this MUST be indicated in the validUntil attribute of the <EntitiesDescriptor> element in the federation metadata.

The federation metadata group name (=Name attribute of <EntitiesDescriptor> element) and URL for publishing are as follows.

- Name = "KAFE"
- URL = https://metainfo.kreonet.net/kafe-metadata.xml“

Each member organization SHOULD obtain the federation metadata published by KAFE, and

install it in its entities.

4.9 Updating of Federation Metadata

If an entity uses old federation metadata, not only will it be unable to interoperate with other sites but also the entity security level may be lowered. For this reason, it is strongly RECOMMENDED that each member organization regularly update the federation metadata, and that updating take place at least before the deadline in the federation metadata validUntil attribute.

4.10 Federation Metadata Signature Validation

Validation of signature on federation metadata downloaded by each member organization, by using the certificate defined in 7.1, is strongly RECOMMENDED.

5. Discovery Service

KAFE SHALL provide a discovery service enabling all entities in KAFE to confirm authentication information by the optimal means.

The URL of the discovery service provided in KAFE is as follows:

- Service URL = https://ds.kafe.coreen.or.kr/

6. Technical Federation Support

Each entity participating in KAFE is able to select and use at its own discretion software supporting the protocol specified in these Standards. Technical support is provided as necessary in KAFE for configuring the IdP or SP of each member organization, but support SHALL NOT be offered for commercial products.

7. Certificate Use

Certificates are used in KAFE to ensure the trustworthiness of each entity.

7.1 Certificate for Federation Metadata Signature

KAFE SHALL sign federation metadata with an XML signature when publishing and distributing the metadata. The certificate used with this signature SHALL be a self-signed certificate managed and administered by KAFE. The certificate used with the signature SHOULD also be distributed by KAFE to each entity securely so that each organization can validate the federation metadata signature; but the certificate MAY be published on the Web (repository) without distributing it directly.

The URL for publishing the certificate used with the federation metadata signature is as follows:

- Publication URL = https://metainfo.kronet.net/

7.2 Validation of a Federation Metadata Signature Certificate

An entity MUST NOT use a signature certificate having a fingerprint value different from the value below.

- Fingerprint (SHA-256) = 9F::00

The latest value is given on the following website:

- https://metainfo.kronet.net/

7.3 Certification Authority

An entity SHOULD not use a certificate issued by a certification authority except KAFE because of compatibility issue.

7.4 Compromise of a Private Key

If a private key used by an entity is compromised, the entity MUST immediately notify KAFE, revoke the associated certificates, and take alternative measures after reissuing of new certificates without delay.

8. Security

In order to maintain security in KAFE, a participating entity MUST observe the following items.

8.1 User ID Management

All user information MUST be for actual users. Each entity MUST terminate the use of a user ID without delay when the valid term of the user ID has expired or when the user revokes the intention to use the ID.

8.2 User ID Recycling

In case a previously used uid, eduPersonPrincipalName or eduPersonTargetedID is going to be used by another user, the identifier SHOULD NOT be reused until at least 12 months have elapsed from the last use.

8.3 ID Use in SP

An SP providing service using an ID MUST take sufficient care to avoid collision, etc., due to incorrect ID assignment in a database or by an assignment algorithm.

8.4 User Information Maintenance

To protect personal information, keep information up to date, and avoid the risk of data leaks, it is RECOMMENDED that an SP don't store user information other than the minimum necessary. When it is necessary to store personal information for the sake of service provision, this MUST be indicated to users.

8.5 User Consent

In handling attributes in an entity, in particular when sending and receiving attributes, a function MUST be implemented for indicating the attributes to be used and the purpose of their use and for obtaining user consent. An entity MUST NOT provide the third party with personal information without user consent.

8.6 Log Storage

It is RECOMMENDED that the access logs of a service for at least three months. It is RECOMMENDED that each entity stipulates the access log storage period.

8.7 Member Organization Responsibilities

The organizations participating in KAFE SHALL cooperate with each other in authentication interoperation. To this end, each organization SHALL have the duty of ensuring the trustworthiness and accuracy of the information they send. Beyond this general obligation, however, except in the case of willful or major negligence, they SHALL bear no liability for damages arising from deficiency in the trustworthiness or accuracy of sent information.

References

1. Gakunin Technical Profile
2. eduPerson Object Class Specification, http://middleware.internet2.edu/eduperson

Appendix. Recommending Attribute Information List

1. uid

Name	uid
oid	urn:oid:0.9.2342.19200300.100.1.1
Description	computer system login names
Schema	RFC4519
Value or type	String
Multiple values	Single value
Remarks	e.g., "s9709015", "admin", and "student"

2. eduPersonTargetedID

Name	eduPersonTargetedID
oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
Description	A pseudonym of an entity in KAFE
Schema	eduPerson Object Class Specification
Value or type	256 bytes max, a privacy-preserving and persistent identifier unique in each IdP and different for each SP
Multiple values	Multiple
Remarks	e.g., "Kxxl8QLncKbguy5xjNLRSkdBc12="

3. sn

Name	sn
oid	urn:oid:2.5.4.4
Description	Family name
Schema	RFC4519
Value or type	String
Multiple values	Multiple
Remarks	e.g., Hong

4. givenName

Name	givenName
oid	urn:oid:2.5.4.42
Description	First name
Schema	RFC4519
Value or type	String
Multiple values	Multiple
Remarks	e.g., “Gildong”

5. displayName

Name	displayName
oid	urn:oid:2.16.840.1.113730.3.1.241
Description	Indicates the name displayed in English
Schema	RFC2798(inetOrgPerson)
Value or type	String
Multiple values	Single value
Remarks	e.g., "Gildong Hong"

6. mail

Name	mail
oid	urn:oid:0.9.2342.19200300.100.1.3
Description	Email address
Schema	RFC2798(inetOrgPerson)
Value or type	string@domain, maximum 256 bytes
Multiple values	Single value
Remarks	e.g., "gildong_hong@kafe.or.kr"

7. eduPersonAffiliation

Name	eduPersonAffiliation
oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
Description	Indicates the user's occupation type, etc

Schema	eduPerson Object Class Specification
Value or type	"faculty", "staff", "student", "member", "employee", none
Multiple values	Multiple
Remarks	Any of five values may be used to indicate the user's position. The addition of other values such as "staff, member" will be considered as necessary.

8. organizationName

Name	organizationName
oid	urn:oid:2.5.4.10
Description	Organization Name
Schema	RFC4519
Value or type	String
Multiple values	Single value
Remarks	e.g., "KISTI", "Korean Access Federation"

9. schacHomeOrganization

Name	schacHomeOrganization
oid	urn:oid:1.3.6.1.4.1.25178.1.2.9
Description	Domain name of the organization
Schema	RFC1035
Value or type	String
Multiple values	Single value
Remarks	e.g., "KISTI", "kafe.or.kr"

10. eduPersonPrincipalName

Name	eduPersonPrincipalName
oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
Description	Uniquely identifies an entity in KAFE
Schema	eduPerson Object Class Specification
Value or type	[unique and persistent identifier]@scope

Multiple values	Single value
Remarks	e.g., "gildong-home2015@kafe.or.kr"

11. eduPersonScopedAffiliation

Name	eduPersonScopedAffiliation
oid	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.9
Description	Indicates the user's occupation type within the organization
Schema	eduPerson Object Class Specification
Value or type	String@scope
Multiple values	Multiple
Remarks	e.g., "staff@kafe.or.kr"

6. Conclusion

In this paper, we present our work about eduGAIN policy template. After the completion of this work, we submitted the whole document to GEANT who operates eduGAIN system, and now we are waiting for peer review. After the review, we may amend this paper. But, sooner or later, we look forward to deciding to join eduGAIN. Thus We wish to help the Korean students, researchers and educators to access online services while minimizing the number of accounts users and service providers have to manage – reducing costs, complexity and security risks.