This English version is only a translation of the Japanese version, and is provided for reference only. In case of discrepancy between the Japanese and English versions, the Japanese version shall prevail and be treated as the correct version.

System Administration Standards for the GakuNin（Ver. 2.0)

Table of Contents

These Standards govern matters relating to system administration of an identity provider (IdP) or service provider (SP) participating in the Academic Access Management Federation "GakuNin." They have been drawn up by the Steering Committee for Academic Authentication (hereinafter called "Committee") in the National Institute of Informatics.

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 GakuNin SHALL be based on the following standards specified by the OASIS Security Services Technical Committee.

1.1) SAML V2.0 Core

(http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

Specifies the technical requirements for conformance with SAML V2.0 and the documents of which they consist.

1.2) SAML V2.0 Profiles

(http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

Specifies the identifiers used between systems, binding support, and use of certificates and keys.

1.3) SAML V2.0 Metadata

(http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

Specifies the rules for standardized notation of metadata.

2. Protocol

These Standards are designed so that an IdP or SP (hereinafter called an "entity") participating in GakuNin will be able to provide as broad a range of services as possible. To this end, all entities participating in GakuNin SHOULD use the protocol

standardized within GakuNin. The protocol SHALL meet the requirements herein for authentication request and authentication response.
As software for use in GakuNin, Shibboleth is RECOMMENDED as an example of 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 V2.0 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 V2.0 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) Shibboleth

Shibboleth is a SAML-based software package developed and provided by Internet2 (http://internet2.edu).

Shibboleth 2 (https://wiki.shibboleth.net/confluence/display/SHIB2/Home) or newer, especially usage of versions of the Shibboleth IdP 2.3 and newer and for the Shibboleth SP of 2.5 and newer are RECOMMENDED.

Note that while SAML 2.0 is the primary protocol used by GakuNin, the legacy Shibboleth 1.3 protocol MAY be used for the purpose of using an overseas SP or other service.

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 GakuNin.

3.1) Using Attribute Information

All attribute information defined in GakuNin 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 the Committee for adding a new attribute. The Committee 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 GakuNin or limited to a private federation within an organization.

http://middleware.internet2.edu/dir/docs/draft-internet2-mace-dir-saml-attributes-latest.pdf

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. For example, an IdP of university A SHOULD NOT guarantee the attributes of a student belonging to university B. 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" be

clearly indicated along with the purpose for use of the attribute information.

An SP SHALL apply to the GakuNin Secretariat regarding attribute information necessary for the provided services, by using the application form stipulated separately.

The Committee SHALL notify each entity concerning the attribute information to be used by each SP.

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.

4. Metadata

GakuNin uses the metadata specified below.

4.1) Metadata Specifications

The SAML V2.0 metadata specifications (see 1.3) SAML V2.0 Metadata) SHOULD be followed.

4.2) Kinds of Metadata

The following two kinds of metadata are used in GakuNin.

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

4.3) Submission of Entity Metadata

All organizations participating in GakuNin MUST submit entity metadata for each of their entities to the Committee.

4.4) Contents of Entity Metadata

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

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. It is RECOMMENDED to use a group address as the e-mail address.

Note that the entity metadata submitted to the Committee, 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.

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

- Validating the items included in the entity metadata
- GakuNin administration, management, and operation
- Addition and updating of federation metadata
- Distributing federation metadata to GakuNin 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.

Of the following information, an SP SHOULD include <OrganizationName xml:lang="en"> in the <Organization> element of the submitted entity metadata and MAY include other elements.

- <OrganizationName xml:lang="en">: Official English name of the organization

  In the case of an IdP, this MUST match the name of the IdP operating organization.
- <OrganizationName xml:lang="ja">: Official Japanese name of the

organization

In the case of an IdP, this MUST match the name of the IdP operating organization.

- <OrganizationDisplayName xml:lang="en">: Official English name of the entity

  In the case of an IdP, this is the string displayed by the DS.

- <OrganizationDisplayName xml:lang="ja"> : Official Japanese name of the entity

  In the case of an IdP, this is the string displayed by the DS. If there are multiple IdPs in the same organization, this name SHOULD be able to distinguish them.

4.6) Entity Metadata ID

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.

4.7) Submission and Publishing of Federation Metadata

The Committee MUST validate all the submitted entity metadata, then add it to the federation metadata, validate it, and sign it, thereby creating the latest federation metadata.

It then MUST make 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="GakuNin"

URL="https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml"

4.8) Acquisition and Installation of Federation Metadata

Each member organization SHOULD obtain the federation metadata published by GakuNin, as in 4.7), 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. The RECOMMENDED frequency is once per day. If the update frequency is set longer than this, it is strongly RECOMMENDED 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

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

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

https://ds.gakunin.nii.ac.jp/WAYF

6. Federation Support

Each entity participating in GakuNin 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 GakuNin 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 GakuNin to ensure the trustworthiness of each entity.

7.1) Certificate for Federation Metadata Signature

The Committee 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 GakuNin. The certificate used with the signature SHOULD also be distributed by GakuNin 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://metadata.gakunin.nii.ac.jp/gakunin-signer-2010.cer"

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. To confirm this, it is RECOMMENDED that each entity use the value below to validate the signature certificate.

Fingerprint (SHA-1)

=9F:8D:13:CB:E3:93:57:59:E1:81:8F:A4:26:A5:FD:60:AB:C5:01:00

The latest value is given on the following website:

https://meatwiki.nii.ac.jp/confluence/display/GakuNinShibInstall/signer

7.3) Trusted Certification Authority

An entity MUST use a certificate issued by a certification authority trusted by GakuNin, as listed below, as the certificate for XML digital signing and for TLS （Transport Layer Security） mutual authentication.

- UPKI open domain certification authority
  https://upki-portal.nii.ac.jp/docs/odcert (project website)
- A commercial certification authority compliant with the Web Trust for CA (certification authority) and approved by the Committee
- A private CA such as a university campus certification authority that is approved by the Committee.

7.4) What to Do When a Private Key is Compromised

If a private key used by an entity is compromised, the entity MUST immediately notify the Committee, revoke the associated certificates, and take alternative

measures after reissuing of new certificates without delay.

7.5) Direct SOAP Connection

XML signing and/or TLS mutual authentication SHOULD be used when an SP requests a direct SOAP connection,

8. Security

In order to maintain security in GakuNin, 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 eduPersonPrincipalName or eduPersonTargetedID is going to be used by another user, the identifier SHOULD NOT be reused until at least 24 months have elapsed from the last use.

8.3) Assurance of the Sameness of a Claimant

An IdP MUST provide some mechanism of authentication to assure the sameness of a claimant in the access to the protected transaction or data.

8.4) 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.

8.5) 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 not 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.

8.6) User Consent

In handling attributes in an entity, in particular when sending and receiving attributes, a function MAY be implemented for indicating the attributes to be used and the purpose of their use and for obtaining user consent.

8.7) 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.

8.8) Member Organization Responsibilities

The organizations participating in GakuNin 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.

Note that this provision does not preclude the making of separate agreements between member organizations regarding their responsibility for the trustworthiness and accuracy of sent information.

9. Entities for GakuNin Administrative Use

The Committee SHALL operate a GakuNin IdP necessary for administration of GakuNin, and provide an attribute viewer service enabling each member organization to conduct connection testing.

9.1) GakuNin IdP

A GakuNin IdP SHALL be operated for the use by a SP for the following purposes:

- To provide access to a SP necessary for administration of the Federation

- To test a connection to a SP

  Entity ID of a GakuNin IdP SHALL be the following:

  Entity ID= “https://idp.gakunin.nii.ac.jp/idp/shibboleth”

A GakuNin IdP SHALL hold the accounts of those who have been approved as being necessary to administer the Federation by the Committee. A GakuNin IdP, on exception, MAY hold a test account that is to be used by a SP for the purpose of a connection test. Details of issuing a test account SHALL be stipulated elsewhere.

9.2) Attribute Viewer Service

Attribute viewer service is a service that displays all attributes that can be sent using the Shibboleth 2.0 protocol and Shibboleth 1.3 protocol, for viewing by any member organization, for the sake of connection testing.

Attrviewer20:

EntityID = “https://attrviewer20.gakunin.nii.ac.jp/shibboleth-sp”

Protocol = shibboleth2.0

Attrviewer13:

EntityID = “https://attrviewer13.gakunin.nii.ac.jp/shibboleth-sp”

Protocol = shibboleth1.3

Appendix 1. GakuNin Supported Attribute Information Specifications

1. organizationName

Name	organizationName
Description	Indicates the name of the organization in English
Referenced schema	RFC4519, RFC2256 (LDAPv3)
Name [Shib1.3]	“urn:mace:dir:attribute-def:o”
Name [Shib2.x]	“urn:oid:2.5.4.10”
friendlyName	o
Value or type	String (1-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	An attribute indicating the organization name in English. Examples: Abcdef University National Institute of Informatics

2. jaOrganizationName

Name	jaOrganizationName
Description	Indicates the name of the organization in Japanese
Referenced schema	GakuNin.schema
Name [Shib1.3]	Not defined
Name [Shib2.x]	“urn:oid:1.3.6.1.4.1.32264.1.1.4”
friendlyName	jao
Value or type	String (2-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	An attribute newly defined for GakuNin. As a string in 2-byte code, it

	can be used for indicating organization names in Japanese. Examples: あいうえお大学 国立情報学研究所

3. organizationalUnitName

Name	organizationalUnitName
Description	Indicates the English name of a unit in the organization
Referenced schema	RFC4519, RFC2256 (LDAPv3)
name [Shib1.3]	“urn:mace:dir:attribute-def:ou”
name [Shib2.x]	“urn:oid:2.5.4.11”
friendlyName	ou
Value or type	String (1-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	Examples: Faculty of Technology Cyber Science Center

4. jaOrganizationalUnitName

Name	jaOrganizationalUnitName
Description	Indicates the Japanese name of a unit in the organization
Referenced schema	GakuNin.schema
name [Shib1.3]	Not defined
name [Shib2.x]	“urn:oid:1.3.6.1.4.1.32264.1.1.5”
friendlyName	jaou
Value or type	String (2-byte code)
Collation sequence	caseIgnoreMatch

Multiple values	Single
Remarks	An attribute newly defined for GakuNin. As a string in 2-byte code, it can be used for indicating organizational unit names in Japanese. Examples: 工学部 サイバーサイエンスセンター

5. eduPersonPrincipalName

Name	eduPersonPrincipalName
Description	Uniquely identifies an entity in GakuNin
Referenced schema	eduPerson Object Class Specification (200806)
name [Shib1.3]	“urn:mace:dir:attribute-def:eduPersonPrincipalName”
name [Shib2.x]	“urn:oid:1.3.6.1.4.1.5923.1.1.1.6”
friendlyName	eduPersonPrincipalName
Value or type	[A unique and persistent identifier of each IdP]@[Scope]
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	A user ID assigned uniquely and persistently within GakuNin. Uniqueness in GakuNin is guaranteed by combining an identifier unique in the organization with a scope. The IdP sends the same value to all SPs participating in GakuNin. Example: t-ninsyo2009@b-univ.ac.jp

6. eduPersonTargetedID

Name	eduPersonTargetedID
Description	A pseudonym of an entity in GakuNin
Referenced schema	eduPerson Object Class Specification (200806)
name [Shib1.3]	“urn:mace:dir:attribute-def:eduPersonTargetedID”
name	“urn:oid:1.3.6.1.4.1.5923.1.1.1.10”

[Shib2.x]	
friendlyName	eduPersonTargetedID
Value or type	<IdP entityID>!<SP entityID>![a privacy-preserving and persistent identifier unique in each IdP and different for each SP], 256 bytes max
Collation sequence	caseExactMatch
Multiple values	Multiple
Remarks	A persistent user identifier unique in GakuNin and different for each SP site is sent. The purpose is to prevent the user from being identified across SP sites, hence the identifier values are required to be hashed or otherwise prevented from being determined. The format consists of the <IdP entityID>, <SP entityID>, and the hashed identifier, joined by "!" Example: https://idp.sample.ac.jp/idp/shibboleth!https://sp.sample.ac.jp /shibboleth-sp!+Lxxl7QLnCkaKguy5xjNLRBkdDc=

7. eduPersonAffiliation

Name	eduPersonAffiliation
Description	Indicates the user's occupation type, etc.
Referenced schema	eduPerson Object Class Specification (200806)
name [Shib1.3]	"urn:mace:dir:attribute-def:eduPersonAffiliation"
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
friendlyName	eduPersonAffiliation
Value or type	"faculty", "staff", "student", "member", none (blank)
Collation sequence	caseIgnoreMatch
Multiple values	Multiple
Remarks	Any of five values may be used to indicate the user's position. In an IdP site, mapping to the actual detailed position of the user in the organization is necessary. The addition of other values such as "graduate" will be considered as necessary.

	Example: staff, member

8. eduPersonScopedAffiliation

Name	eduPersonScopedAffiliation
Description	Indicates the user's occupation type within the organization
Referenced schema	eduPerson Object Class Specification (200806)
name [Shib1.3]	"urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
friendlyName	eduPersonScopedAffiliation
Value or type	string@scope, the string being one of the following values: "faculty", "staff", "student", "member", none (blank)
Collation sequence	caseIgnoreMatch
Multiple values	Multiple
Remarks	This attribute defines the user's relationship to the organization to which he or she belongs. The values that can be set are the same as those for eduPersonAffiliation, but a scope is appended after @. Example: member@nii.ac.jp, student@nii.ac.jp

9. eduPersonEntitlement

Name	eduPersonEntitlement
Description	Indicates qualification to use a specific application
Referenced schema	eduPerson Object Class Specification (200712)
name [Shib1.3]	"urn:mace:dir:attribute-def:eduPersonEntitlement"
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
friendlyName	eduPersonEntitlement
Value or type	String (1-byte code)
Collation sequence	caseExactMatch
Multiple values	Multiple

Remarks	This is information indicating the qualification for using a service. For this attribute an SP site decides the string to be received and the IdP site uses the values decided by each SP site. The IdP sets the value to be sent as each user's attribute in accord with the service use qualification decided by the SP site. Example: urn:mace:dir:entitlement:common-lib-terms

10. surName

Name	surName
Description	Indicates the surname in English
Referenced schema	RFC4519, RFC2256 (LDAPv3)
name [Shib1.3]	"urn:mace:dir:attribute-def:sn"
name [Shib2.x]	"urn:oid:2.5.4.4"
friendlyName	sn
Value or type	String (1-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	Examples: Ninsho Yamada

11. jaSurName

Name	jaSurName
Description	Indicates the surname in Japanese
Referenced schema	GakuNin.schema
name [Shib1.3]	Not defined
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.32264.1.1.1"
friendlyName	jasn

Value or type	String (2-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	An attribute newly defined for GakuNin. As a string in 2-byte code, it can be used for indicating surnames in Japanese. Examples: 認証 山田

12. givenName

Name	givenName
Description	Indicates the given name in English
Referenced schema	RFC4519, RFC2256 (LDAPv3)
name [Shib1.3]	“urn:mace:dir:attribute-def:givenName”
name [Shib2.x]	“urn:oid:2.5.4.42”
friendlyName	givenName
Value or type	String (1-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	Examples: Taro Jiro

13. jaGivenName

Name	jaGivenName
Description	Indicates the given name in Japanese
Referenced schema	GakuNin.schema
name [Shib1.3]	Not defined
name	“urn:oid:1.3.6.1.4.1.32264.1.1.2”

[Shib2.x]	
friendlyName	jaGivenName
Value or type	String (2-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	An attribute newly defined for GakuNin. As a string in 2-byte code, it can be used for indicating given names in Japanese. Examples: 太郎 次郎

14. displayName

Name	displayName
Description	Indicates the name displayed in English
Referenced schema	RFC2798 (inetOrgPerson)
name [Shib1.3]	“urn:mace:dir:attribute-def:displayName”
name [Shib2.x]	“urn:oid:2.16.840.1.113730.3.1.241”
friendlyName	displayName
Value or type	String (1-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	This is intended for use mainly as the name displayed in English in applications. Examples: Ninsho Taro Yamada Jiro

15. jaDisplayName

Name	jaDisplayName
Description	The name, etc., displayed in an application in Japanese

Referenced schema	GakuNin.schema
name [Shib1.3]	Not defined
name [Shib2.x]	“urn:oid:1.3.6.1.4.1.32264.1.1.3”
friendlyName	jaDisplayName
Value or type	String (2-byte code)
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	An attribute newly defined for GakuNin. This is intended for use mainly as the name displayed in Japanese in applications. Examples: 認証太郎 山田次郎

16. mail

Name	mail
Description	E-mail address
Referenced schema	RFC2798 (inetOrgPerson)
name [Shib1.3]	“urn:mace:dir:attribute-def:mail”
name [Shib2.x]	“urn:oid:0.9.2342.19200300.100.1.3”
friendlyName	mail
Value or type	string@domain, 256 bytes max
Collation sequence	caseIgnoreMatch
Multiple values	Single
Remarks	This can be used to set an e-mail address. Example: ninsho_taro@nii.ac.jp

17. gakuninScopedPersonalUniqueCode

Name	gakuninScopedPersonalUniqueCode
Description	The faculty number of faculty and student ID number of student
Referenced schema	GakuNin.schema
name [Shib1.3]	Not defined
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.32264.1.1.6"
friendlyName	gakuninScopedPersonalUniqueCode
Value or type	[affiliation]: [identity number] @[scope]　（Unicode/UTF-8） [affiliation] is "faculty", "student", etc. [identity number] is the faculty number, student ID, etc.
Collation sequence	caseIgnoreMatch
Multiple values	Multiple
Remarks	An attribute newly defined for GakuNin. Halfwidth variants of Japanese characters SHOULD not be used. Fullwidth variants of alpha-numerical characters SHOULD not be used. Examples: faculty:12345@kyoto-su.ac.jp student:abcdefg@kyoto-su.ac.jp student:12 あ 3456@osaka-u.ac.jp

18.isMemberOf

Name	isMemberOf
Description	Identifiers for groups to which he/she belongs
Referenced schema	eduMember Object Class Specification
name [Shib1.3]	Not defined
name [Shib2.x]	"urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
friendlyName	isMemberOf

Value or type	String (1-byte code)
Collation sequence	caseExactMatch
Multiple values	Multiple
Remarks	The values of isMemberOf are identifiers for groups to which the user belongs. They SHOULD be well-formed URIs. Example: https://voplatform.example.ac.jp/gr/FooGroup

Reference URLs

(1)「eduPerson Object Class Specification 」

http://middleware.internet2.edu/eduperson

(2)「GakuNin.Schema」

https://meatwiki.nii.ac.jp/confluence/download/attachments/12158166/gakunin.schema

(3)「eduMember Object Class Specification」

http://middleware.internet2.edu/dir/groups/