KAFE

Korean Access Federation Technological Profile

JongUk Kong, Jinyong Jo, Heejin Jang
(4th, Nov. 2016, v1.0)
coreen@kreonet.net

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). The latest stable release of SimpleSAMLphp is 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 (i.e., shibmd: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>
- SecurityContact:
  <md:ContactPerson contactType=”other”>
  <md:GivenName></md:GivnName>
  <md:EmailAddress></md:EmailAddess>
  </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 4 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.

- Test federation
  - Name = "KAFE-testfed"
  - URL = https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-testfed/metadata.xml
- Production federation
  - Name =”KAFE-profed”
  - URL = https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-profed/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 MAY 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.kreonet.net/kafe

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) = 93:36:C1:7C:F7:61:AB:3C:41:81:63:AA:82:71:C6:6A:31:B2:D8:0A:E1:F1:0A:C0:7D:0F:8D:29:09:6D:03:59

The latest value is given on the following website:

- https://coreen.kreonet.net/join

7.3 Certification Authority

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

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.

Acknowledgement

This work is © KREONET. It is heavily based on the "System Administration Standards for the GakuNin (Ver. 2.0).

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. schacHomeOrganizationType

Name	schacHomeOrganizationType
oid	urn:oid:1.3.6.1.4.1.25178.1.2.10
Description	Domain name of the organization
Schema	RFC1035
Value or type	String
Multiple values	Multiple
Remarks	urn:schac:homeOrganizationType:<country-code>:<string> e.g., urn:schac:homeOrganizationType:kr:university urn:schac:homeOrganizationType:kr:vho

11. 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"

12. 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"

13. eduPersonEntitlement

Name	eduPersonEntitlement
oid	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7
Description	URI (either URN or URL) that indicates a set of rights to specific resources
Schema	eduPerson Object Class Specification
Value or type	String
Multiple values	Multiple
Remarks	e.g., "http://xstor.com/contracts/HEd123", "urn:mace:k.ac:confocalMicroscope"