KAFE

기술프로파일

- Korean Access Federation (KAFE) -

조진용, 장희진

coreen@kreonet.net

한국과학기술정보연구원

KAFE

목 차

제 1 장 SAML 기술표준

제 2 장 프로토콜

제 3 장 사용자 속성(Attribute) 정보

제 4 장 메타데이터

제 5 장 서비스 탐색

제 6 장 기술지원

제 7 장 인증서의 사용

제 8 장 보안

부록

KAFE

기술프로파일

[최근 갱신: 2019-05-28 v1.1]
2015. 08. 20. - 초안

제 1 장 SAML 기술표준

KAFE 에서 이용되는 SAML(Security Assertion Markup Language) 표준은 OASIS 보안서비스기술위원회(Security Services Technical Committee)에서 규정한 다음의 표준에 기초하고 있다. 본 운용정책은 시험 페더레이션 기간에 한해 적용하며 정식 서비스 시행 시 수정될 수 있다.

1.1 절 SAML v2.0 Core

SAML v2.0 표준 준수를 위해 필요한 기술적 요구사항을 규정하고 있다.
(http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

1.2 절 SAML v2.0 Profiles

시스템들 간에 이용되는 식별자, 바인딩 지원, 인증서와 키들의 이용을 규정하고 있다.
(http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

1.3 절 SAML v2.0 Metadata

메타데이터의 표준 표기법 작성 규칙을 규정하고 있다.
(http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

제 2 장 프로토콜

본 지침은 KAFE 에 참여하는 ID 제공자 또는 서비스 제공자(이하 엔터티)들이 가급적 넓은 범주의 서비스를 제공하고 활용할 수 있도록 설계되어 있다. 이를 위해, KAFE 에 참여하는 모든 엔터티들은 KAFE 에서 규정한 표준 프로토콜의 이용을 권고한다. 표준 프로토콜은 인증 요청과 인증 응답에 대한 필요사항들을 반드시 만족해야 한다.

KAFE 는 표준 프로토콜의 준수를 위해 simpleSAMLphp 또는 Shibboleth SAML2.0 소프트웨어의 이용을 권장한다.

[수정 - 2019.05.28.]

2.1 절 Authentication Request

HTTP-bound SAML 프로토콜의 인증 요청(Authentication Request) 메시지는 SAML 기술 표준 "SAML 2 Profiles" 4.1.3 및 4.1.4 에 정의된 Web Browser SSO 프로파일이 충족되도록 구현해야 한다.

2.2 절 Authentication Response

SAML assertions 를 포함하는 HTTP-bound 인증 응답(Authentication Response) 메시지들은 "SAML 2 Profiles" 4.1.3 및 4.1.4 에 정의된 Web Browser SSO 프로파일이 충족되도록 구현해야 한다.

또한 SAML 응답 메시지 또는 SAML assertion 은 반드시 서명되어야 하고, SAML assertion 은 암호화할 것을 권고한다.

[조항수정 - 2019.05.28.]

2.3 절 SAML 소프트웨어

simpleSAMLphp 와 Shibboleth 는 SAML 소프트웨어 패키지 또는 모듈이다. simpleSAMLphp 는 UNINETT, Shibboleth 는 Shibboleth 콘소시엄에 의해 개발 관리되고 있다. 최신 버전의 SAML 소프트웨어 이용을 권장한다.

[조항수정 - 2019.05.28.]

제 3 장 사용자 속성 정보

사용자 속성정보는 사용자의 권한을 부여하기 위해 개별 엔터티들이 이용하는 정보이다. KAFE 에서 사용되는 속성 정보는 본 문서의 부록 "지원되는 속성 정보 목록"을 참조한다.

3.1 절 속성 정보의 이용

[권고] KAFE 에 정의된 모든 사용자 속성정보는 고유 URI 를 가지고 있다. 각 엔터티들은 본 문서의 부록 "지원되는 속성 정보 목록"에서 사용자 속성 정보를 선택하여 이용하는 것을 권장한다. 만약 이용하려는 속성이 "지원되는 속성 정보 목록"에 존재하지 않는 경우 각 엔터티는 KAFE 에 새 속성의 추가를 신청할 수 있다. 신청된 새 속성 정보는 KAFE 에서 검토하고 "지원되는 속성 정보 목록"에 편입여부를 결정한다. KAFE 에 참여하지 않는 경우, "지원되는 속성 정보 목록"에 명시된 속성 이외의 속성 정보들을 이용할 수 있다.

3.2 절 속성 정보의 신뢰성

[권고] ID 제공자는 제공 중인 사용자 속성 정보에 대한 신뢰성을 보장해야 한다. ID 제공자 기관의 내부 구성원이 아닐 경우 속성 정보를 보장하지 않을 수 있다. 하지만 서비스 제공자에 대한 불법적, 악의적 접근을 방지하기 위해 해당 사용자에 대한 속성 관리를 수행해야 한다.

3.3 절 속성 정보의 확인

[권고] 서비스 제공자는 제공받은 모든 속성 정보들이 신뢰할 수 있는 기관(Trusted Authority)에서 전달받은 것인지 검증할 수 있는 방법을 확보해야 한다.

3.4 절 속성 정보의 등급 및 저장 기간

[필수] 서비스 제공자는 개인정보보호정책을 통해 이용하는 속성 정보를 사용자에게 고지해야 한다. 속성 정보는 “필수(required)”, “권장(recommended)”, “선택(optional)”으로 분류하고 이용 목적과 함께 명확하게 기재해야 한다. 서비스 제공자는 속성 정보를 저장할 경우, 저장 기간에 대해 명확하게 기재해야 한다.

[조항수정 - 2019.05.28.]

3.5 절 사용자의 소속 범위

[필수] 속성 정보를 제공할 사용자의 소속 범위(즉, shibmd:Scope)는 EntityID 에 기록된 도메인의 범위와 일치해야 한다. 예를 들어, EntityID 의 도메인 정보가 info.school.ac.kr 일 경우, ID 제공자는 정보통신공학과에 소속된 사용자의 속성정보만 제공해야 한다. 서비스 제공자는 ID 제공자의 메타데이터에 포함된 사용자 속성의 범위와 SAML assertion 에 기재되어 있는 범위를 비교하여 제공되는 범위를 판단해야 한다.

[조항수정 - 2016.10.30.]

3.7 절 eduPersonTargetedID 의 규격

[필수] eduPersonTargetedID 는 NameQualifier, SPNameQualifier, Opaque ID 를 포함한다. 다음 규격을 준수한다.

- eduPersonTargetedID

  <saml:NameID xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

  NameQualifier="[IDP의 entityID]" SPNameQualifier="[SP의 entityID]">

  [opaque ID]</saml:NameID>

[조항추가 - 2015.9.17.]

제 4 장 메타데이터

KAFE 는 다음에 규정된 메타데이터를 이용한다.

4.1 절 메타데이터의 규격

[필수] SAML v2.0 메타데이터 규격(SAML v2.0 Metadata)에 따라야 한다.

4.2 절 메타데이터의 종류

[필수] KAFE 는 다음 두 종류의 메타데이터를 이용한다.

1. 엔터티 메타데이터
개별 엔터티들이 KAFE 에 제출한 메타데이터로, 각 엔터티들에 대한 정보를 포함

2. 페더레이션 메타데이터
KAFE 에 의해 생성된 메타데이터로, KAFE 에 참여하는 모든 엔터티들의 메타데이터를 포함

4.3 절 엔터티 메타데이터의 제출

[필수] KAFE 에 참여하는 모든 ID 제공자 및 서비스제공자들은 엔터티 메타데이터를 KAFE 에 제출해야 한다.

[조항수정 - 2019.05.28.]

4.4 절 엔터티 메타데이터의 내용

[필수] KAFE 에 참여하는 기관의 서버임을 인정하는 서버 인증서를 갱신하거나 기관의 메타데이터를 변경했을 경우, 해당 기관은 KAFE 에 최신 메타데이터 파일을 반드시 제출해야 한다.

[권고] 메타데이터에 개인정보의 입력이 필요한 부분은 예를 들어, 운용 담당자의 email 주소 등에 가급적 개인 정보가 나타나지 않도록 할 것을 권장한다.

[필수] KAFE 에 제출된 엔터티 메타데이터는 내부에 포함된 개인정보를 포함해 웹에 공개된다. 따라서 운용 책임자는 엔터티 메타데이터의 제출 시에 엔터티 메타 데이터에 포함된 개인정보에 대해 함께 공개한 것으로 간주하며 개인정보의 제 3 자 제공에 동의한 것으로 간주한다.

개별 기관에서 제출한 메타데이터 정보는 다음과 같은 목적에 이용된다.

- 엔터티 메타데이터에 포함된 항목들의 검증
- KAFE 의 관리 운영
- 페더레이션 메타데이터에 추가 및 갱신
- KAFE 회원 기관에 대한 페더레이션 메타데이터의 배포 또는 Web 을 통한 공개
- 탐색 서비스(Discovery Service), ID 제공자, 서비스 제공자의 등록

4.5 절 엔터티 메타데이터의 제공기관 관련 요소

[필수] ID 제공자는 KAFE 에 제출하는 엔터티 메타 데이터에 제공 기관관련 요소에 다음의 사항을 기재해야 한다. 기관 내에 여러 개의 엔터티들이 존재할 경우 각 엔터티들을 구분할 수 있어야 한다.

- OrganizationName
  예: <md:OrganizationName xml:lang="en">name</md:OrganizationName>

- OrganizationDisplayName:
  예: <md:OrganizationDisplayName xml:lang="en">name</md:OrganizationDisplayName>

- OrganizationURL
  예: <md:OrganizationURL xml:lang="en">http://www.kreonet.net/</md:OrganizationURL>

- ContactPerson
  예:
  <md:ContactPerson contactType="technical">
  <md:GivenName></md:GivenName>
  <md:SurName></md:SurName>
  <md:EmailAddress></md:EmailAddress>
  </md:ContactPerson>

- SecurityContact
  예:
  <md:ContactPerson contactType="other">
  <md:GivenName></md:GivenName>
  <md:SurName></md:SurName>
  <md:EmailAddress></md:EmailAddress>
  </md:ContactPerson>

[조항수정 및 추가 - 2016.10.11.]

4.6 절 엔터티 메타데이터의 Scope 설정

[권고] ID 제공자는 사용자 소속정보의 scope 를 기재한다.

- Scope
  예: <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false">kreonet.net</shibmd:Scope>

[조항수정 - 2016.1.6.]

4.7 절 엔터티 메타데이터의 개인정보보호정책 고지관련

[필수] 서비스 제공자는 개인정보처리방침을 고지하고 엔터티 메타데이터에 고지 URL 을 기재해야 한다. 고지되는 개인정보처리방침은 대한민국 개인정보보호법을 준수해야 한다.

- PrivacyStatementURL
  예: <mdui:PrivacyStatementURL xml:lang="ko"> [URL] </mdui:PrivacyStatementURL>

[조항수정 - 2015.11.18.]

4.8 절 엔터티 메타데이터의 엔터티 ID

[권고] 엔터티 메타데이터의 EntityID 는 다음의 규정을 따른다. 예를 들어, ID 제공 기관인 my.school.ac.kr 에서 simpleSAMLphp 소프트웨어를 이용할 경우 https://my.school.ac.kr/idp/simplesamlphp 로 EntityID 를 정의한다.

[기관 URL]/[IdP 또는 SP]/[SAML 2.0 소프트웨어]

4.9 절 페더레이션 메타데이터의 제출 및 공개

KAFE 는 제출된 엔터티 메타데이터를 검증한 후, 페더레이션 메타데이터에 추가한다.

[필수] 제출된 메타데이터는 모든 회원기관에 공개된다.

페더레이션 메타데이터의 유효기간의 4 일이고, validUntil 속성에 유효기간이 기재된다. 페더레이션 메타데이터 그룹의 이름과 공개 URL 은 다음과 같다.

- 테스트 페더레이션
  - Name = "KAFE-testfed“
  - 공개 URL
    https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-testfed/metadata.xml

- 프로덕션 페더레이션
  - Name = “KAFE-profed“
  - 공개 URL
    https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-profed/metadata.xml

페더레이션 메타데이터는 "페더레이션 메타데이터의 제출 및 발간" 절에 포함된 공개 URL 을 통해 배포된다.

[조항수정 - 2015.11.18.]

4.10 절 페더레이션 메타데이터의 갱신

[권고] 오래된 페더레이션 메타데이터를 이용할 경우, 서비스제공자 사이트에 대한 접속 불가 및 보안 등급의 하락 등이 발생할 수 있다. KAFE 회원 기관은 페데레이션 메타데이터를 주기적으로 업데이트해야

한다. 페더레이션 메타데이터에 기재된 validUntil 속성값의 만료일 이전에 페더레이션 메타데이터가 갱신되어야 한다.

4.11 절 페더레이션 메타데이터의 검증

[권고] KAFE 회원 기관은 7.2 절의 내용을 참고해 다운받은 페더레이션 메타데이터의 유효성을 검증해야 한다.

[조항추가 - 2015.11.9.]

제 5 장 탐색 서비스

KAFE 는 서비스제공자들이 최적의 방법으로 ID 제공자를 검색할 수 있도록 탐색 서비스(Discovery service)를 제공한다. 서비스 URL 은 다음과 같다.

- 탐색 서비스 URL = https://ds.kreonet.net/kafe

[조항수정 - 2019.05.28.]

제 6 장 기술 지원

KAFE 에 참여하는 개별 엔터티들은 본 문서에서 규정한 표준을 따르는 어떠한 SAML 소프트웨어라도 사용할 수 있다. SAML ID 제공자와 서비스 제공자를 구성하기 위해 필요하면 KAFE 에서 기술 지원이 가능하다. 상용 제품에 대해서는 기술 지원을 하지 않는다.

제 7 장 인증서의 사용

KAFE 는 각 엔터티의 신뢰성을 담보하기 위해 인증서를 이용한다.

7.1 절 페더레이션 메타데이터의 인증서

[권고] KAFE 는 게시, 배포하는 페더레이션 메타데이터에 대해 자체서명 인증서(Self-signed certificate)를 이용해 서명한다. 서명에 사용할 인증서 내용은 각 기관이 페더레이션 메타데이터의 서명을 검증할 목적으로 KAFE 에서 안전하게 배포해야 한다.

KAFE 는 웹을 통해 해당 인증서를 공개한다. 페더레이션 메타데이터에 이용된 인증서의 배포 URL 은 다음과 같다.

- 배포 URL
  https://fedinfo.kreonet.net/cert

[조항추가 - 2019.05.28.]

7.2 절 페더레이션 메타데이터의 인증서 검증

[필수] 배포된 인증서의 fingerprint 가 다음과 같지 않을 경우, 개별 엔터티는 해당 인증서를 이용해서는 안 된다.

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:0
3:59

최신 fingerprint 값과 확인방법은 다음 웹사이트에서 확인할 수 있다.

- 배포 URL = https://coreen.kreonet.net/join

[조항추가 - 2019.05.28.]

7.3 절 Certificate Authority

[권고] 상용 Certificate Authority(CA)에서 발급받은 인증서는 상호호환성의 문제를 야기할 수 있으므로 사용을 권장하지 않는다.

[조항추가 - 2015.11.9.]

[필수] 개인키가 분실되었거나 유출되었을 경우에는 즉시 KAFE 에 통보하여야 하고 해당 인증서를 폐기해야 한다. 또한 새로운 인증서를 즉시 재발급받아야 한다.

[조항추가 - 2015.11.9.]

제 8 장 보안

[필수] 보안 관리를 위해 모든 참여 엔터티들은 다음 사항을 반드시 준수해야 한다.

8.1 절 사용자의 신원정보 관리

[필수] 제공되는 모든 사용자의 신원정보는 실제 사용자의 정보와 일치해야 한다. 각 엔터티의 사용자 신원정보는 유효 기간이 종료된 후 또는 사용자의 서비스 이용 의사 철회가 있는 경우 지체 없이 삭제되어야 한다.

8.2 절 사용자 ID 의 재사용

[권고] 사용 중이거나 이미 사용되었던 uid, eduPersonPrincipalName, eduPersonTargetedID 가 다른 사용자에게 할당되기 위해서는 마지막 사용일로부터 적어도 12 개월 이상 지나야 한다.

8.3 절 서비스 제공자의 사용자 ID 이용

[필수] 서비스 제공자는 중복된 사용자 ID 를 갖는 사용자들을 구분 가능하도록 충분한 기술적 조치를 강구해야 한다.

8.4 절 개인정보의 저장 및 이용목적 고지

[권고] 개인정보의 보호, 개인정보의 유지, 개인정보의 유출 방지를 위해, 서비스 제공자는 꼭 필요한 경우가 아니면 사용자 정보를 저장하지 않아야 한다.

[필수] 서비스 제공을 위해 사용자의 개인정보를 저장할 경우, 개인정보의 수집 목적, 항목, 보유 및 이용기간, 거부권 및 불이익 등이 사용자에게 고지되어야 한다.

8.5 절 개인정보제공에 대한 사용자 동의

[필수] 사용자의 개인정보가 처리될 때, 개인정보의 전송 시, 개인정보의 이용 고지, 이용 목적, 사용자 동의를 얻는 절차가 반드시 제공되어야 한다.

[필수] 각 엔터티는 사용자 동의 없이 제 3 자에게 개인정보를 제공할 수 없다. 개인정보의 제 3 자 제공을 위해서는 필수 고지 항목(제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익)을 사용자에게 고지하고 정보 주체의 사전 동의를 받아야 한다.

8.6 절 로그파일의 저장

[필수] 서비스에 대한 접근 로그(access log)는 최소 6 개월 이상 저장되어야 한다.

8.7 절 회원 기관의 책임

[필수] KAFE 에 참여하는 회원기관은 상호 협력하여 ID 페더레이션을 실현하도록 한다. 각 회원기관은 송신하는 정보의 신뢰성이나 정확성을 확보하기 위한 의무를 갖는다. 고의 또는 중대한 과실에 의한 경우를 제외하고 전송한 정보의 신뢰성이나 정확성이 미비하여 발생한 손해에 대해서는 회원기관이 책임을 지지 않는다.

KAFE 와 별개로, 참여 기관 간 별도의 협정(agreement)에 의해 연동된 개별 엔터티들의 책임에 대해서 명문화 할 수 있다

부록
- 권장 속성정보 목록 -

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	예; "s9709015", "admin", and "student"

2. eduPersonTargetedID

Name	eduPersonTargetedID
oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
Description	사용자 가명(가독 불가)
Schema	eduPerson Object Class Specification
Value or type	최대 256 바이트, 서비스 제공자마다 다른 persistent ID를 제공
Multiple values	Multiple
Remarks	예; "KxxI8QLncKbguy5xjNLRSkdBc12="

3. sn

Name	sn
oid	urn:oid:2.5.4.4
Description	성(family name)
Schema	RFC4519
Value or type	String
Multiple values	Multiple
Remarks	예; Hong

4. givenName

Name	givenName
oid	urn:oid:2.5.4.42
Description	이름(first name)
Schema	RFC4519
Value or type	String
Multiple values	Multiple
Remarks	예; “Gil-dong”

5. displayName

Name	displayName
oid	urn:oid:2.16.840.1.113730.3.1.241
Description	화면표시 이름
Schema	RFC2798(inetOrgPerson)
Value or type	String
Multiple values	Single value
Remarks	예; "Kildong Hong"

6. mail

Name	mail
oid	urn:oid:0.9.2342.19200300.100.1.3
Description	Email 주소
Schema	RFC2798(inetOrgPerson)
Value or type	string@domain, 최대256 바이트
Multiple values	Single value
Remarks	예; "kildong_hong@kafe.or.kr"

7. eduPersonAffiliation

Name	eduPersonAffiliation

oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
Description	사용자 직무 형태
Schema	eduPerson Object Class Specification
Value or type	"faculty", "staff", "student", "member", "employee", none
Multiple values	Multiple
Remarks	상위 6개 직무 타입이 값이 된다. 필요할 경우 타입을 추가할 수 있다. 예; "staff, member"

8. organizationName

Name	organizationName
oid	urn:oid:2.5.4.10
Description	기관명
Schema	RFC4519
Value or type	String
Multiple values	Single value
Remarks	예; "KISTI", "Korean Access Federation"

9. schacHomeOrganization

Name	schacHomeOrganization
oid	urn:oid:1.3.6.1.4.1.25178.1.2.9
Description	기관의 도메인 이름
Schema	RFC1035
Value or type	String
Multiple values	Single value
Remarks	예; "KISTI", "kafe.or.kr"

10. schacHomeOrganizationType

Name	schacHomeOrganizationType
oid	urn:oid:1.3.6.1.4.1.25178.1.2.10
Description	기관 형태

Schema	SCHAC
Value or type	String
Multiple values	Mutiple value
Remarks	urn:schac:homeOrganizationType:<country-code>:<string> 예; 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	도메인 내 사용자 식별 정보
Schema	eduPerson Object Class Specification
Value or type	[unique and persistent identifier]@scope
Multiple values	Single value
Remarks	예; "kildong-home2015@kafe.or.kr"

12. eduPersonScopedAffiliation

Name	eduPersonScopedAffiliation
oid	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.9
Description	기관내 사용자 직무형태
Schema	eduPerson Object Class Specification
Value or type	String@scope
Multiple values	Multiple
Remarks	예; "staff@kafe.or.kr"

13. eduPersonEntitlement

Name	eduPersonEntitlement
oid	SAML2: urn:oid:1.3.6.1.4.1.5923.1.1.1.7
Description	자원에 대한 권한(right)을 나타내는 URI (URL 또는 URN)
Schema	eduPerson Object Class Specification

Value or type	String
Multiple values	Multiple
Remarks	예; "http://xstor.com/contracts/HEd123", "urn:mace:k.ac:confocalMicroscope"

[조항추가 - 2016.7.19]