교육ID연합(SICHIMI) 기술프로파일

정책위원회

2022.12.

한국교육정보화재단(KREN)

- 목 차 -

기술프로파일

ver. 1.0

제 1 장 SAML 기술표준

SICHIMI에서 이용되는 SAML(Security Assertion Markup Language) 규격은 OASIS 보안서비스기술위원회(Security Services Technical Committee)에서 규정한 다음의 표준에 기초하고 있다.

1.1 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 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 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 SICHIMI에 참여하는 ID 제공자 또는 서비스 제공자(이하 Entity)들이 가급적 넓은 범주의 서비스를 제공하고 활용할 수 있도록 설계되어 있다. 이를 위해 SICHIMI에 참여하는 모든 Entity들은 SICHIMI에서 규정한 표준 프로토콜의 이용을 권고한다. 표준 프로토콜은 인증 요청과 인증 응답에 대한 필요사항들을 반드시 만족해야 한다.

SICHIMI는 표준 프로토콜의 준수를 위해 SAML2.0기반의 Shibboleth 또는 simpleSAMLphp 소프트웨어의 이용을 권장한다.

2.1 Authentication Request

HTTP-bound SAML 프로토콜의 인증 요청(Authentication Request) 메시지는 SAML 기술 표준 “SAML v2.0 Profiles“ 4.1.3 및 4.1.4에 정의된 Web Browser SSO 프로파일이 충족되도록 구현해야 한다.

2.2 Authentication Response

SAML Assertions를 포함하는 HTTP-bound 인증 응답(Authentication Response) 메시지들은 “SAML2 Profiles“ 4.1.3 및 4.1.4에 정의된 Web Browser SSO 프로파일이 충족되도록 구현해야 한다.
또한 SAML 응답 메시지 또는 SAML Assertion은 반드시 전자서명 되어야 한다.

2.3 SAML 소프트웨어

Shibboleth와 simpleSAMLphp는 SAML 소프트웨어 패키지 또는 모듈이다.
Shibboleth는 Internet2 Shibboleth 컨소시엄, simpleSAMLphp는 UNINETT에 의해 개발 관리되고 있다. 최신 버전의 SAML 소프트웨어 이용을 권장한다.

제 3 장 사용자 속성 정보

사용자 속성정보는 사용자의 권한을 부여하기 위해 개별 Entity들이 이용하는 정보이다. SICHIMI에서 사용되는 속성 정보는 본 문서의 부록 “지원되는 속성 정보 목록“을 참조한다.

3.1 속성 정보의 이용

[권고] SICHIMI 에 정의된 모든 사용자 속성정보는 고유 URI를 가지고 있다. 각 Entity들은 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 Entity는 SICHIMI에 새 속성의 추가를 요청할 수 있다. 신청된 새 속성 정보는 기술분과위원회 검토를 거쳐 정책위원회 에서 승인한다.

3.2 속성 정보의 신뢰성

[권고] ID 제공자는 제공 중인 사용자 속성 정보의 신뢰성을 보장해야 한다. 또한 서비스 제공자에 대한 불법적 접근이 발생하지 않도록 사용자에 대한 속성 관리를 수행해야 한다.

3.3 속성 정보의 확인

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

3.4 개인정보보호정책의 제공

[필수] 서비스 제공자는 개인정보보호법 및 정보통신망법 등 유관 법령에 부합하는 개인정보보호정책을 수립하고 웹 페이지 등을 통해 공개해야 한다.

3.5 사용자의 소속 범위

[필수] 속성 정보를 제공할 사용자의 소속 범위(즉, shibmd:Scope)는 EntityID에 기록된 도메인의 범위와 일치해야 한다. 서비스 제공자는 ID 제공자의 메타데이터에 포함된 사용자의 소속 범위와 SAML Assertion에 기재되어 있는 범위를 비교하여 제공되는 범위의 유효성을 판단해야 한다.

3.6 필요 속성정보 제공

[필수] 서비스 제공자는 필요 속성정보를 이용 목적과 함께 운영센터에 제출해야 하며, 운영센터는 각 서비스 제공자별로 어떤 속성정보를 이용하는가를 웹사이트를 통해 공지한다.

제 4 장 메타데이터

SICHIMI는 다음에 규정된 메타데이터를 이용한다.

4.1 메타데이터의 규격

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

4.2 메타데이터의 종류

[필수] SICHIMI 는 다음 두 종류의 메타데이터를 이용한다.

4.2.1. Entity 메타데이터

개별 Entity들이 SICHIMI에 제출한 메타데이터로, 제출한 Entity에 대한 정보를 포함 한다.

4.2.2. 페더레이션 메타데이터

SICHIMI에 의해 생성된 메타데이터로, SICHIMI에 참여하는 모든 Entity들의 메타

데이터가 포함 된다.

4.3 Entity 메타데이터의 제출

[필수] SICHIMI에 참여하는 모든 Entity들은 Entity 메타데이터를 SICHIMI 운영센터에 제출해야 한다. 개별 Entity의 Entity ID는 타 Entity와 중복되지 않도록 정의되어야 한다.

4.4 Entity 메타데이터의 내용

[필수] SICHIMI에 참여하는 기관의 서버임을 인정하는 서버 인증서(사설)를 갱신하거나 기관의 메타데이터를 변경했을 경우, 해당 기관은 SICHIMI운영센터에 최신 메타데이터 파일을 반드시 제출해야 한다.

[권고] 메타데이터에 포함되는 관리자 email 주소 등에 개인정보가 노출되지 않도록 한다(예, security@abc.ac.kr 과 같은 공용 이메일 주소의 이용 권장).

[필수] SICHIMI에 제출된 Entity 메타데이터는 페더레이션 메타데이터의 형태로 일반에 공개된다. SICHIMI에 참가신청서를 제출하는 것으로 Entity 메타데이터에 포함된 관리자 개인정보의 제3자 제공에 동의한 것으로 간주한다.

개별 기관에서 제출한 Entity 메타데이터는 다음과 같은 목적으로 이용된다.

- Entity 메타데이터에 포함된 항목들의 검증
- SICHIMI의 관리 운영
- 페더레이션 메타데이터에 추가 및 갱신
- SICHIMI 참여 기관에 대한 페더레이션 메타데이터의 배포 또는 Web을 통한 공개
- 탐색 서비스(Discovery Service), ID 제공자, 서비스 제공자의 등록

4.5 Entity 메타데이터의 구성 요소

[필수] SICHIMI에 제출하는 Entity 메타데이터에는 다음 항목이 필수적으로 기재되어야 한다. 기관 내에 다수의 Entity들이 존재할 경우, 다음 항목들은 각 Entity들을 구분할 수 있게 기재되어야 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.abc.ac.kr
  </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>

4.6 Entity 메타데이터의 소속 범위(Scope) 설정

[필수] ID 제공자는 Entity 메타데이터에 소속 범위(Scope)를 기재한다.

- Scope
  예: <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexp="false"> univ.ac.kr </shibmd:Scope>

4.7 Entity 메타데이터의 개인정보보호정책 고지

[필수] 서비스 제공자는 제공하는 서비스 내에 개인정보처리방침을 고지하고 Entity메타데이터에 고지URL을 기재해야 한다. 고지되는 개인정보처리방침은 대한민국 개인정보보호법 및 정보통신망법 등 관련 법령을 준수해야 한다.

▪ PrivacyStatementURL

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

4.8 Entity 메타데이터의 고유식별자(EntityID)

[권고] Entity 메타데이터의 EntityID는 다음의 규정을 따른다.

예를 들어, ID제공기관인 idp.[도메인명].ac.kr에서 shibboleth 소프트웨어를 이용할 경우 https://idp.[도메인명].ac.kr/idp/shibboleth 로 EntityID를 정의한다.

[기관 URL]/[IdP 또는 SP]/[SAML 2.0 소프트웨어]

4.9 페더레이션 메타데이터의 제출 및 공개

SICHIMI운영센터는 제출된 Entity 메타데이터를 검증한 후, 페더레이션 메타데이터에 추가하고, 페더레이션 메타데이터의 형태로 일반에 공개된다.

[필수] 페더레이션 메타데이터의 기본 유효기간은 7일이며 validUntil 속성에 기재된다. 페더레이션 메타데이터 그룹의 이름과 공개 URL 은 다음과 같다.

▪ 테스트 페더레이션

- Name = “SICHIMI-testfed”
- 공개 URL

https://metadata.sichimi.kr/signedmetadata/federation/SICHIMI-testfed/metadata.xml

▪ 프로덕션 페더레이션

- Name = “sichimi”
- 공개 URL

https://metadata.sichimi.kr/signedmetadata/federation/sichimi/metadata.xml

4.10 페더레이션 메타데이터의 갱신

[권고] 기간이 만료된 페더레이션 메타데이터를 이용할 경우, 보안문제 등이 발생할 수 있다. SICHIMI 회원기관은 페더레이션 메타데이터를 주기적으로 다운받아 Entity에 적용해야 한다. 페더레이션 메타데이터에 기재된 validUntil 속성값의 만료일 이전에 페더레이션 메타데이터가 갱신되어야 한다.

4.11 페더레이션 메타데이터의 검증

[권고] SICHIMI 참여 기관은 7.2의 내용을 참고해 다운받은 페더레이션 메타데이터의 유효성을 검증할 것을 권고한다.

제 5 장 탐색 서비스

서비스제공자들이 자체 탐색서비스를 제공하는 것을 권고한다. SICHIMI운영센터는 보조적 방법으로 별도의 탐색 서비스(Discovery service)를 제공한다. 서비스 URL은 다음과 같다.

▪ 탐색 서비스 URL = https://ds.sichimi.kr/rr3

제 6 장 기술 지원

SICHIMI는 권장 SAML 소프트웨어를 이용하는 회원기관 및 참여 중인 기관에 대해서 기술 지원을 할 수 있다. 상용 제품 및 솔루션에 대해서는 기술 지원을 하지 않는다. 다만, 솔루션 공급업체 제품이 SICHIMI와 시험 검증을 한 경우에 기술 가이드 제공을 할 수 있다.

제 7 장 인증서의 사용

SICHIMI는 각 Entity의 신뢰성을 담보하기 위해 인증서를 이용한다.

7.1 페더레이션 메타데이터의 인증서

SICHIMI는 페더레이션 메타데이터에 대해서 서명한다. 서명에 사용하는 인증서는 SICHIMI에서 안전하게 배포하며 Entity들은 페더레이션 메타데이터의 서명을 검증할 목적으로 해당 인증서를 이용할 수 있다.

SICHIMI는 웹을 통해 해당 인증서를 공개한다. 페더레이션 메타데이터에 이용된 인증서의 배포 URL은 다음과 같다.

▪ 배포 URL https://www.sichimi.kr/cert

7.2 페더레이션 메타데이터의 인증서 검증

[필수] 배포된 인증서의 fingerprint가 다음과 같지 않을 경우, 개별 Entity는 해당 메타데이터를 이용해서는 안 된다.

배포 인증서(예, 메타데이터내 signing 인증서: fed-sichimi.crt) Fingerprint (SHA-1) 코드 적시

```
88727ef182bdc8654d4edb4986693ec481551e79
```

```
예) 배포 인증서 다운로드 후 Fingerprint (SHA-1) 코드 확인 방법
$ openssl x509 -noout -in fed-sichimi.crt -fingerprint -sha1
SHA1 Fingerprint=88:72:7E:F1:82:BD:C8:65:4D:4E:DB:49:86:69:3E:C4:81:55:1E:79
```

7.3 인증서 발급(Certificate Authority)

[권고] 각 Entity에서 메타데이터 생성시 사용하는 인증서는 Self Signed Certificate 사용을 권장한다. 상용 Certificate Authority(CA)에서 발급받은 인증서는 상호호환성의 문제를 야기할 수 있으므로 사용을 권장하지 않는다.

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

제 8 장 보안

[필수] 보안 관리를 위해 모든 참여 Entity들은, 본 항에서 정의하는 사항들을 반드시 준수해야만 한다.

8.1 사용자의 ID 관리

[필수] 제공되는 모든 사용자의 ID는 실제 사용자의 계정 정보여야만 한다. 각 Entity에 대해, 사용자 ID의 유효기간이 종료된 경우 또는 사용자로부터 서비스 이용 의사 철회가 있었을 경우, 지체 없이 그 사용자의 ID를 사용정지 또는 삭제시켜야 한다.

8.2 사용자 ID의 재사용

[권고] 사용 중이거나 이미 사용되었던 uid, eduPersonPrincipalName, eduPersonTargetedID에 관하여, 과거에 사용했으나 현재 사용하지 않는 사용자 ID를 타인이 사용할 경우, 최종 사용일로부터 24개월간은 재사용할 수 없다.

8.3 사용자 ID 동일성 보증

[권고] 전 항에 언급한 재사용의 경우를 제외하고, IdP는 동일 ID에 의한 접근이 동일 인물임을 보증할 충분한 기술적 조치를 강구해야 한다.

8.4 개인정보의 저장 및 이용목적 고지

[필수] 서비스 제공을 위해 사용자의 개인정보를 보관할 경우, 국내 개인정보보호법 및 정보통신망법 등 관련 법령을 준수하고 그 내용을 명시해야 한다.
[권고] 개인정보의 보호, 개인정보의 유지, 개인정보의 유출 방지를 위해, 서비스 제공자는 개인정보 수집을 최소화해야 한다.

8.5 개인정보제공에 대한 사용자 동의

[필수] 개인정보 처리 시, 국내 개인정보보호법 및 정보통신망법 등 관련 법령에 따라 사용자의 동의를 얻는 절차가 반드시 제공되어야 한다. 또한 각 Entity는 사용자 동의 없이 제3자에게 개인정보를 제공할 수 없다.

8.6 로그파일의 저장

[필수] 개별 Entity는 ID 이용기록 또는 접근 기록 등 보안로그를 최소 6개월 이상 보관해야 한다.

8.7 참여 기관의 책임

[필수] SICHIMI에 참여하는 각 참여기관들은 상호 협력하여 ID 페더레이션을 실현하도록 한다. 각 참여기관들은 정보의 신뢰성이나 정확성을 확보하기 위한 관리의무를 갖는다. 고의 또는 중대한 과실에 의한 경우를 제외하고 정보의 신뢰성이나 정확성이 미비하여 발생한 손해에 대해서는 참여기관간 책임을 묻지 않는다. 또한 이 규정은 참여기관 간 송수신 정보의 신뢰성과 정확성 책임에 대한 별도협의를 금하지 않는다.

SICHIMI와 별개로, 개별 기관 간의 협정에 의해 개별 Entity들이 연동되는 경우, SICHIMI 정책과 지침이 적용되지 않으므로 이해 당사자들은 의무와 책임에 대해

서 충분히 인지한 후에 연동을 추진해야 한다.

제 9 장 시험용 Entity제공

SICHIMI는 운영에 필요한 SICHIMI IdP의 운영 및 각 참여기관이 운영 접속 시험 등 수행 시 필요로 하는 속성 값을 제공한다.

9.1 SICHIMI 시험용 IdP

SICHIMI IdP는, 참여기관의 서비스 제공자(이하 SP)에 대해 아래의 목적으로 운영된다.

· 페더레이션의 운영에 필용한 SP 접근 · SP와의 접속 확인 SICHIMI IdP의 Entity ID는 아래와 같다. · Entity ID: https://idptest.sichimi.kr/idp/shibboleth SICHIMI IdP는, 운영센터가 페더레이션 운영을 위해 필요한 계정을 제공할 수 있다.

9.2 SICHIMI 시험용 속성 서비스

Shibboleth2.0 프로토콜을 통한 접속시험을 위해, 각각의 프로토콜에 송신 가능한 모든 속성을 표시하는 서비스이며, 각 참여기관이 이용 가능하다.

속성표시 · URL: https://sptest.sichimi.kr/ · 프로토콜: Shibboleth 2.0

부록

속성값(Attribute)

❑ Attribute Profile

IdP와 SP간에 CoT(Community of Trust) 및 이용자가 참여한 IdP와 SP간의 Authentication Request와 Authentication Response 발생 시 사전에 정의된 속성: 값 쌍의 메시지 집합

❑ 사용 스키마

- eduPerson: 고등교육에서 널리 사용되는 개인 및 조직 특성을 포함하도록 설계된 LDAP스키마(Internet2 => REFEDS)
- inetOrgPerson : 사용자의 별칭으로 설계된 LDAP스키마
- eduMember : 그룹 구성원 표현을 위해 설계된 LDAP스키마
- schac : 학계를 위한 스키마(REFEDS)

❑ 국제표준 속성이 아닌 경우 규약

- 국내에서만 사용되고 타연합과 공유될 수 있는 속성 : ko+첫글자 대문자
- 연구기관 페더레이션인 KAFE와의 향후 연동을 고려 KAFE에서 정의한 것 사용
- SICHIMI에서만 사용되는 속성 : KREN Private Enterprise Number(59751)사용

* 필수속성, **권고속성, ***부가속성

순번	Attribute명 SAML Name	값 정의
1*	eduPersonTargetedID uid:oid:1.3.6.1.4.1.5923.1.1.1.10	Persistent identifier (자동생성)
2*	commonName urn:oid:2.5.4.3	개체의 이름으로, 개체가 사람인 경우, 일반적으로 전체 이름 표시(GilDong HONG)
3*	eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	전자메일주소 형태이나 전자메일이 아닐 수 있음 uid@abc.ac.kr
4**	mail urn:oid:0.9.2342.19200300.100.1.3	abcd@abc.ac.kr 실제 전자메일주소
5*	displayName urn:oid:2.16.840.1.113730.3.1.241	영문 성명 GilDong HONG 또는 Prof. GilDong Hong 도 가능

6*	eduPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1	직무정보 - student :학부, 대학원생 - faculty :교원(교수, 비전임교원, 조교) - researcher : 연구원 - staff :직원(비정규 포함) - alum :졸업생
7**	uid urn:oid:0.9.2342.19200300.100.1.1	Login ID (기관에서 사용하는 로그인ID)
8**	schacHomeOrganization urn:oid:1.3.6.1.4.1.25178.1.2.9	소속기관 최상위도메인 예, abc.ac.kr
9**	schacHomeOrganizationType urn:oid:1.3.6.1.4.1.25178.1.2.10	기관형태 예, university, universityhospital 등
10**	eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	조직내 직무 - student@abc.ac.kr - faculty@abc.ac.kr - researcher@abc.ac.kr - staff@abc.ac.kr - alum@abc.ac.kr
11**	eduPersonEntitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7	서비스이용 자격 정보(추후논의) 예시 system_x:workgroup_y
12**	organizationName urn:oid:2.5.4.10	영문 조직(대학) 명칭 예, Chonnam National University
13**	koCommonName urn:oid:1.3.6.1.4.1.14305.1.10.1.4.3	한글 성명 (KAFE와 일치) 홍길동
14**	koOrganizationName urn:oid:1.3.6.1.4.1.14305.1.10.1.4.10	조직(대학)의 한글 명칭(KAFE와 일치) 한국대학교
15**	koOrganizationUnitName urn:oid:1.3.6.1.4.1.14305.1.10.1.4.11	조직내 소속명칭(한글, KEFE와 일치) -학부 전공 (학부인 경우) -기계공학과 (학과인 경우)
16**	sichimiScopedInSchoolStatus urn:oid:1.3.6.1.4.1.59751.1.10.1.1.1	재학 및 재직상태(sichimi 연합사용) -재학, 휴학, 자퇴, 수료, 졸업 (학생) -재직, 퇴직 (교직원)
17***	koResearcherNumber urn:oid:1.3.6.1.4.1.14305.1.10.1.1.16	과학기술인등록번호(KEFE와 일치) NTIS(ntis.go.kr)에 따른 국가연구자번호
18***	schacGender	성별구분

	urn:oid:1.3.6.1.4.1.25178.1.2.2	0 Not known 1 Male 2 Female 9 Not specified
19***	schacDateOfBirth urn:oid:1.3.6.1.4.1.25178.1.2.3	생년월일 예, YYYYMMDD
20***	mobileNumber urn:oid:0.9.2343.19200300.100.1.41	핸드폰번호
21***	employNumber urn:oid:2.16.840.1.113730.3.1.3	사번, 학번
22***	eduPersonOrcid urn:oid:1.3.6.1.4.1.5923.1.1.1.16	국제연구자번호(예, ORCID 발급 번호) -http://orcid.org/0000-0002-1825-0097
23	organizationalUnitName urn:oid:2.5.4.11	영문 조직내 소속 명칭 예, Department of Mechanical Engineering
24	isMemberOf urn:oid:1.3.6.1.4.1.5923.1.5.1.1	그룹식별자(소속그룹ID를 URI로 표시)
25	givenName urn:oid:2.5.4.42	영문이름(예, GilDong)
26	surName(sn) urn:oid:2.5.4.4	영문 성(예, HONG)
27	koHomePostalAddress urn:oid:1.3.6.1.4.1.14305.1.10.1.1.39	한글 집주소(KEFE와 일치)
28	koPostalAddress urn:oid:1.3.6.1.4.1.14305.1.10.1.4.16	한글 직장주소(KEFE와 일치)
29	koOrganizationCode urn:oid:1.3.6.1.4.1.14305.1.10.1.4.12	기관표준코드(KEFE와 일치) 행정표준코드관리시스템(code.go.kr)에 따른 기관코드

1. eduPersonTargetedID

명 칭	eduPersonTargetedID
개 요	페더레이션 내의 Entity를 약명으로 표시한다.
참조스키마	eduPerson Object Class Specification(200806)
name(Shib 1.3)	urn:mace:dir:attribute-def:eduPersonTargetedID
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
frindlyName	eduPersonTargetedID
형 식	<IdP의 entityID>!<SP의 entitiyID>![각 IdP내의 유일, 각 SP별로 상이한 암호화된 영속적 식별자], 256바이트 이하
조합순서	caseExactMatch
복수값	복수값
설명	페더레이션 내에 유일하고, SP사이트별로 서로 다른 영속적인 이용자 식별자를 송신한다. 이는 SP간의 이용자 특징을 방지하기 위한 것으로 식별자의 값은 해시(hash)코드 등을 통해 사용자 암호화가 요구된다. 포맷은 <IdP의 entityID>, <SP의 entityID> 및 해시된 식별자를 “!”로 결합한 것이다. 설정예: https://idp.sample.ac.kr/idp/shibboleth!https://sp.sample.ac.kr/shibboleth-sp!+Lxxl7QLnCkaKguy5xjNLRBkdDc

2. commonName

명 칭	commonName(cn)
개 요	개체의 이름
참조스키마	eduPerson, RFC4519
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:2.5.4.3
frindlyName	cn
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	복수값
설명	사람의 경우, 전체이름 표기

3. eduPersonPrincipalName

명 칭	eduPersonPrincipalName
개 요	페더레이션 내의 Entity를 유일하게 정의한다.
참조스키마	eduPerson Object Class Specification(200806)
name(Shib 1.3)	urn:mace:dir:attribute-def:eduPersonPrincipalName

name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.6
frindlyName	eduPersonPrincipalName
형 식	[각 IdP에 유일한, 영속적 식별자]@[Scope]
조합순서	caseIgnoreMatch
복수값	단일값
설명	페더레이션 내에 유일한, 영속적인 이용자 식별자, 「조직 내의 유일한 이용자 식별자」와 스코프를 합친 것으로, 페더레이션 내에 유일성을 보증한다. 설정예: uid@b-univ.ac.kr

4. mail

명 칭	mail
개 요	전자메일
참조스키마	RFC2798
name(Shib 1.3)	urn:mace:dir:attribute-def:mail
name(Shib 2.0)	urn:oid:0.9.2342.19200300.100.1.3
frindlyName	mail
형 식	문자열@도메인, 256바이트 이하
조합순서	caseIgnoreMatch
복수값	단일값
설명	전자메일주소를 표시하는 속성이다. 설정예: mymail@b-univ.ac.kr

5. displayName

명 칭	displayName
개 요	영문이름을 표기한다.
참조스키마	RFC2798(inetOrgPerson)
name(Shib 1.3)	urn:mace:dir:attribute-def:displayName
name(Shib 2.0)	urn:oid:2.16.840.1.113730.3.1.241
frindlyName	displayName
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	어플리케이션 상의 표시되는 영문이름(표시명)으로 이용가능 설정예:

	Gildong Hong

6. eduPersonAffiliation

명 칭	eduPersonAffiliation
개 요	이용자의 직종 등을 표기한다.
참조스키마	eduPerson Object Class Specification(200806)
name(Shib 1.3)	urn:mace:dir:attribute-def:eduPersonAffiliation
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
frindlyName	eduPersonAffiliation
형 식	“faculty”, “staff”, “student”, “member”, 없음(공백)
조합순서	caseIgnoreMatch
복수값	복수값
설명	이용자의 직위로, 다섯 개의 값을 이용한다. IdP사이트는 조직내의 실제 상세직위와의 맵핑이 필요하다. 필요에 따라 졸업생 등을 추가로 검토한다. 설정예: staff

7. uid

명 칭	uid
개 요	로그인 ID
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:0.9.2342.19200300.100.1.1
frindlyName	uid
형 식	
조합순서	caseIgnoreMatch
복수값	단일값
설명	로그인 ID

8. schacHomeOrganization

명 칭	schacHomeOrganization
개 요	소속기관 최상위 도메인을 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.25178.1.2.9
frindlyName	schacHomeOrganization
형 식	문자열(1바이트코드)

조합순서	caseIgnoreMatch
복수값	단일값
설명	소속기관 최상위 도메인을 표시하는 속성이다. 설정예: jnu.ac.kr

9. schacHomeOrganizationType

명 칭	schacHomeOrganization
개 요	소속기관 형태를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.25178.1.2.10
frindlyName	schacHomeOrganizationType
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	소속기관의 형태를 표시하는 속성이다. 설정예: university, universityhospital 등

10. eduPersonScopedAffiliation

명 칭	eduPersonScopedAffiliation
개 요	이용자가 소속된 조직내의 직종을 표기한다.
참조스키마	eduPerson Object Class Specification (200806)
name(Shib 1.3)	urn:mace:dir:attribute-def:eduPersonScopedAffiliation
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
frindlyName	eduPersonScopedAffiliation
형 식	문자열@스코프, 문자열은 아래의 값: “faculty”, “staff”, “student”, “member”, 없음(공백)
조합순서	caseIgnoreMatch
복수값	복수값
설명	이용자가 소속 기관과 어떤 관계인가를 정의하는 속성이다. 설정하는 속성값은 「eduPersonAffiliation」와 동일하나 @이하에 스코프를 첨가한다. 설정예: member@jnu.ac.kr, student@jnu.ac.kr

11. eduPersonEntitlement

명 칭	eduPersonEntitlement
개 요	특정 어플리케이션의 이용자격 정보를 표시한다.
참조스키마	eduPerson Object Class Specification(200712)
name(Shib 1.3)	urn:mace:dir:attribute-def:eduPersonEntitlement
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.7
frindlyName	eduPersonEntitlement
형 식	문자열(1바이트코드)
조합순서	caseExactMatch
복수값	복수값
설명	서비스를 이용할 자격정보를 표시한다. 더불어, 본 속성은 SP사이트가 수신할 문자열을 결정하고, IdP사이트별로 그 값을 이용한다. IdP사이트는 SP사이트가 결정한 서비스 이용자격에 따라, 각 사용자의 속성으로 송신값을 설정한다. 설정예: urn:mace:dir:entitlement:common-lib-terms

12. organizaitonName

명 칭	organizationName
개 요	조직명칭을 영어로 표기한다.
참조스키마	RFC4519, RFC2256(LDAPv3)
name(Shib 1.3)	urn:mace:dir:attribute-def:o
name(Shib 2.0)	urn:oid:2.5.4.10
frindlyName	o
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	조직명을 영어로 표시하는 속성이다. 설정예: Chonnam National University National Institute of Informatics

13. koCommonName

명 칭	koCommonName
개 요	한글 성명을 표기한다.
참조스키마	
name(Shib 1.3)	

name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.4.3
frindlyName	koCommonName
형 식	문자열(2바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	한글 성명을 표시하는 속성이다. 설정예: 홍길동

14. koOrganizationName

명 칭	koOrganizationName
개 요	조직(대학)의 한글 명칭을 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.4.10
frindlyName	koOrganizationName
형 식	문자열(2바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	조직(대학)의 한글 명칭을 표시하는 속성이다. 설정예: 전남대학교

15. koOrganizationUnitName

명 칭	koOrganizationUnitName
개 요	조직내 소속명칭을 한글로 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.4.11
frindlyName	koOrganizationUnitName
형 식	문자열(2바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	조직내 소속명칭을 한글로 표시하는 속성이다. 설정예: 기계공학부

16. sichimiScopedInSchoolStatus

명 칭	sichimiScopedInSchoolStatus

개 요	SICHIMI의 소속기관에 속한 사용자의 재학 및 재직상태를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.59751.x.x.x.x.x
frindlyName	sichimiScopedInSchoolStatus
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	SICHIMI의 소속기관에 속한 사용자의 재학 및 재직상태를 표시하는 속성이다. 설정예:

17. koResearcherNumber

명 칭	koResearcherNumber
개 요	과학기술인등록번호를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.1.16
frindlyName	koPostalAddress
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	과학기술인등록번호를 표시하는 속성이다. NTIS(ntis.go.kr)에 따른 국가연구자번호 설정예:

18. schacGender

명 칭	schacGender
개 요	성별구분을 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.25178.1.2.2
frindlyName	schacGender
형 식	“Not known(0)”,“Male(1)”,“Female(2)”,“Not specified(9)”
조합순서	caseIgnoreMatch

복수값	단일값
설명	성별구분을 표시하는 속성이다. 설정예:

19. schacDateOfBirth

명 칭	schacDateOfBirth
개 요	생년월일을 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.25178.1.2.3
frindlyName	schacDateOfBirth
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	생년월일(민감정보) 설정예: YYYYMMDD

20. mobileNumber

명 칭	mobileNumber
개 요	핸드폰 번호
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:0.9.2343.19200300.100.1.41
frindlyName	mobileNumber
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	핸드폰 번호를 표시하는 속성이다. 설정예:

21. employNumber

명 칭	employNumber
개 요	사번 또는 학번을 표기한다.
참조스키마	
name(Shib 1.3)	

name(Shib 2.0)	urn:oid:2.16.840.1.113730.3.1.3
frindlyName	employNumber
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	사번 또는 학번을 표시하는 속성이다. 설정예:

22. eduPersonOrcid

명 칭	eduPersonOrcid
개 요	국제연구자번호를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.1.1.16
frindlyName	eduPersonOrcid
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	ORCID 발급번호 설정예:

23. organizaitonalUnitName

명 칭	organizationalUnitName
개 요	조직내 소속 명칭을 영어로 표기한다.
참조스키마	RFC4519, RFC2256(LDAPv3)
name(Shib 1.3)	urn:mace:dir:attribute-def:ou
name(Shib 2.0)	urn:oid:2.5.4.11
frindlyName	ou
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	조직내 소속 명칭을 영어로 표시하는 속성이다. 설정예: Department of Mechanical Engineering

24. isMemberOf

명 칭	isMemberOf
개 요	소속 그룹명을 표기한다.
참조스키마	eduMember Object Class Specification
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
frindlyName	isMemberOf
형 식	문자열(1바이트코드)
조합순서	caseExactMatch
복수값	복수값
설명	이용자가 소속된 그룹 ID를 URI형식으로 표시한다. 설정예: https://vopplatform.example.ac.kr/gr/FooGroup

25. givenName

명 칭	givenName
개 요	이름을 영어로 표기한다.
참조스키마	RFC4519, RFC2256(LDAPv3)
name(Shib 1.3)	urn:mace:dir:attribute-def:givenName
name(Shib 2.0)	urn:oid:2.5.4.42
frindlyName	givenName
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	설정예: gildong

26. surName

명 칭	surName
개 요	성씨을 영어로 표기한다.
참조스키마	RFC4519, RFC2256(LDAPv3)
name(Shib 1.3)	urn:mace:dir:attribute-def:sn
name(Shib 2.0)	urn:oid:2.5.4.4
frindlyName	sn
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	설정예: Hong

27. koHomePostalAddress

명 칭	koHomePostalAddress
개 요	한글 집주소를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.1.39
frindlyName	koHomePostalAddress
형 식	문자열(2바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	한글 집주소를 표시하는 속성이다. 설정예:

28. koPostalAddress

명 칭	koPostalAddress
개 요	한글 직장주소를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.4.16
frindlyName	koPostalAddress
형 식	문자열(2바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	한글 직장주소를 표시하는 속성이다. 설정예:

29. koOrganizationCode

명 칭	koOrganizationCode
개 요	기관표준코드를 표기한다.
참조스키마	
name(Shib 1.3)	
name(Shib 2.0)	urn:oid:1.3.6.1.4.1.14305.1.10.1.4.12
frindlyName	koOrganizationCode
형 식	문자열(1바이트코드)
조합순서	caseIgnoreMatch
복수값	단일값
설명	행정표준코드관리시스템에 따른 기관코드번호를 표시하는 속성이다. 설정예: