

신뢰기반 디지털 ID 관리기술

- 아이디제공자의 구축과 관리 -

한국과학기술정보연구원 조진용
jiny92@kisti.re.kr

2024년 8월 29일(목)

Audience

대상

- 아이디제공자를 구축하고자 하는 학연 기관 관계자

수준

- 초급+ α
- IT 관련 기초지식 및 PHP 문법 이해 필요

참고

- 강의자료: <https://edu.kafe.or.kr>

Agenda

1교시 (9:30AM - 10:20AM)

¶ 기초 지식

2교시 (10:30AM - 11:20AM)

¶ 아이디제공자의 구축

3교시 (11:30AM - 12:20AM)

¶ IdP의 검증/관리와 KAFE 가입

1교시: 기초 지식



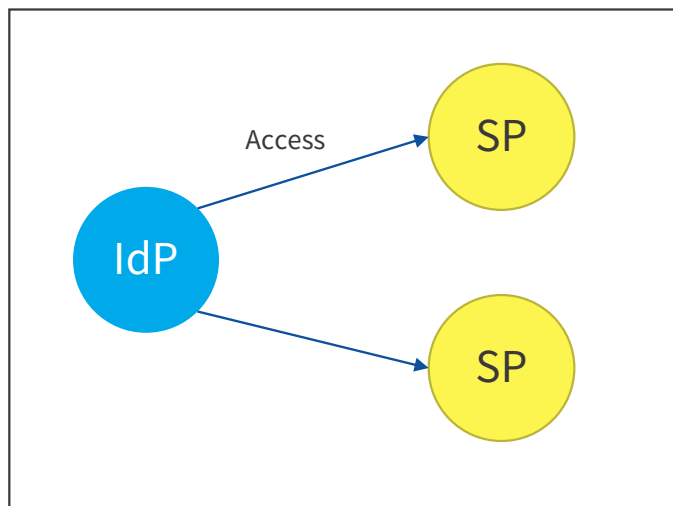
Federated Identity Management (FIM)

- 정의
 - 하나의 디지털 ID를 사용하여;
서로 다른 도메인 내 존재하는 시스템들에 접근케 해주는;
인증 및 인가 프레임워크
- 특징
 - 통합인증
 - 신뢰관계
 - 분산관리
- 작동원리
 - 사용자는 한 시스템(Identity provider, IdP)에서 인증
 - 인증된 사용자 정보는 다른 신뢰할 수 있는 시스템(Service provider, SP)와 공유
 - SP는 인증된 사용자 정보를 신뢰하고 사용자에게 접근 권한을 부여

멀티도메인 접근

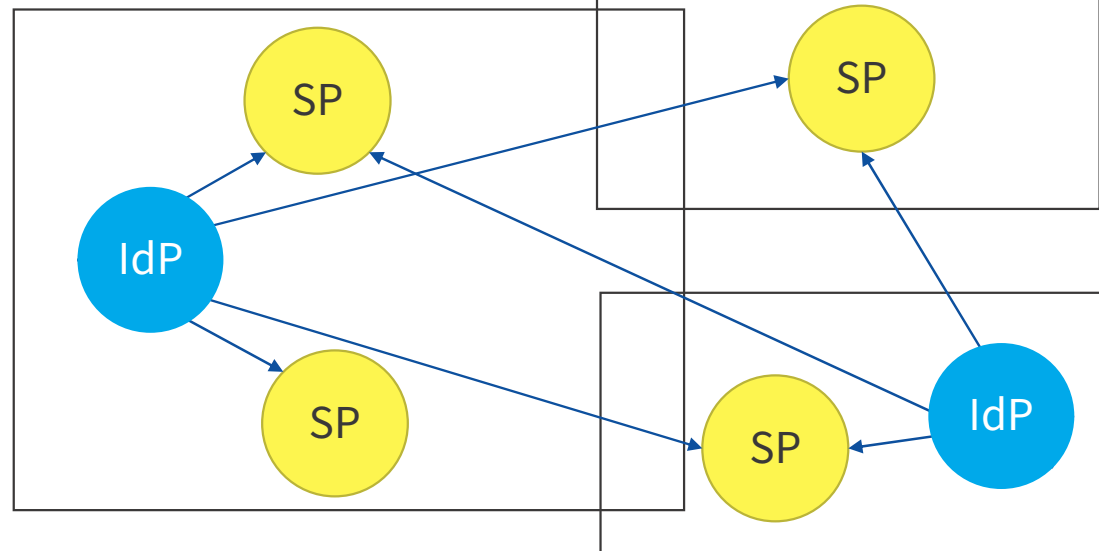
- 인프라 간 상호 운용성 및 접근성 확대
- 안전한 기관 외부 서비스제공자 접근 가능 (클라우드 서비스 등)

Trust domain



SSO(통합인증) in a single domain (e.g., a university)
Centralized identity management

Trust domain #1



SSO(통합인증) in multiple domains (e.g., universities)
Federated identity model

Trust domain #3

FIM의 장점

- 사용자 편의성
 - 여러 계정을 관리할 필요가 없음
- 보안 강화
 - 인증 관리의 중앙화로 기관 외부 서비스에 대한 보안 정책의 일관성 확보
- 관리 효율성
 - 사용자 계정 관리와 접근제어의 간소화
- 비용 절감
 - 여러 시스템에서 중복된 ID 관리 작업을 줄임

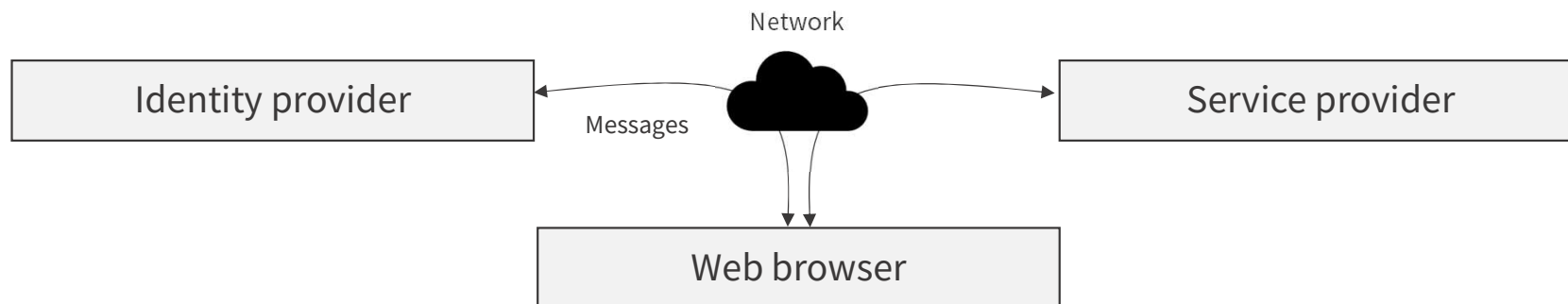
공개 표준

- SAML (Security Assertion Markup Language)
- OIDC/OAuth2 (OpenID Connect)

SAML	OIDC	OAuth2
Developed by OASIS in 2001	Developed by the OpenID Foundation in 2014	Developed by Twitter and Google in 2006
Primary for authentication	Authentication & Authorization	Authorization
XML-based assertions	JSON Web Tokens (JWTs)	JSON Web Tokens (JWTs)
HTTP redirects, GET, POST	Authorization code flow, ID token for authentication	Grant types: authorization code, implicit, password credential, client credentials
Browser, service provider, identity provider	Browser, OIDC provider, OIDC client	Browser, OAuth2 provider, OAuth2 client
Enterprise for web SSO	Web and Mobile SSO	Social SSO

FIM의 개체

Identity provider (IdP)	Service provider (SP)
OIDC provider	OIDC client
Manage user identities and associated attributes	Offers services or resources relying on IdP's identity information (a.k.a., relying party)
Providing identity information to service providers	Trust the IdP to authenticate users
Verifies the user's credentials and issues an assertion or token	Redirects a user to the IdP for authentication. Receives assertion or token and grant access to the user
e.g., social login provider (Google, Facebook, etc.)	Cloud services



데모 I

Inter-federation (Global FIM)

<https://ieeexplore.ieee.org/Xplore/home.jsp>

- Identity provider: KISTI (KR)
- Service provider: IEEEExplore (US)
- Standard: SAML

데모 II

Local-federation (Domestic FIM)

<https://webinar.kafe.or.kr>

- Identity provider: KISTI (KR)
- Service provider: Webinar(KR)
- Standard: SAML

탐색서비스

- Central Discovery Service
 - FIM 운영자가 제공
- Embedded Discovery Service
 - 서비스제공자가 제공

CERN Accelerating Science

Sign in

Directory

Select your login provider

You are authenticating to CERN (European Organization for Nuclear Research) [Privacy Statement](#)

korea

[Why is my Home Institute not listed?](#)

COREEN set.ID by KAFE | 비회원기관 로그인
COREEN/KREONET VHO service

Korea Advanced Institute of Science and Technology
Korea Advanced Institute of Science and Technology

Korea Aerospace Research Institute
Korea Aerospace Research Institute

Korea Astronomy and Space Science Institute
Korea Astronomy and Space Science Institute

Korea Institute of Fusion Energy
Korea Institute of Fusion Energy

LOGIN to Web-based Video conferencing with PPT sharing

Why am I here? ?

Search for an institution



Previously chosen



COREEN set.ID by KAFE | 비회원기관 로그인

Identity Providers with access



COREEN set.ID by KAFE | 비회원기관 로그인



Chungnam National University



Daegu Gyeongbuk Institute of Science and Technology



Everything for Computational Science and Engineering



Gwangju Institute of Science and Technology



Inha University



Institute for Basic Science



KAFESocial - Google



KAFESocial - Naver



Kangwon National University

SAML[샘엘]

SAML (Security Assertion Markup Language)
웹 통합인증(Single Sign On)을 위한 국제 공개표준
Federated authentication에 사용되는 주요 규약

- SAML 1.1(`03), SAML2.0(`05, Errata(정오표)/`19)
 - OASIS 보안서비스 기술위원회 제정
- 연구교육 분야 활용(`05~)
 - SWITCH(스위스 NREN)
- 강화된 보안 vs 적용 어려움
- 웹 환경 지원(모바일 환경 미지원)
 - OAuth2/OIDC 출현



Security Assertion Markup Language (SAML) V2.0 Technical Overview

Committee Draft 02

25 March 2008

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.cd-02.odt>

Previous Version:

N/A

Latest Version:

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf>

<http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.odt>

Technical Committee:

OASIS Security Services TC

Chairs:

Hal Lockhart, BEA

Brian Campbell, Ping Identity

Editors:

Nick Ragouzis, Enosis Group LLC

John Hughes, PA Consulting

Rob Philpott, EMC Corporation

Eve Maler, Sun Microsystems

Paul Madsen, NTT

Tom Scavo, NCSA/University of Illinois

Related Work:

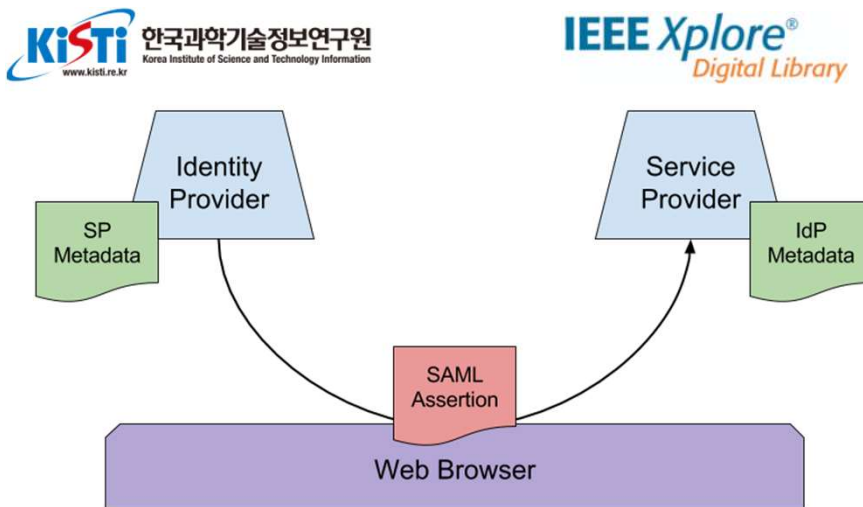
N/A

Abstract:

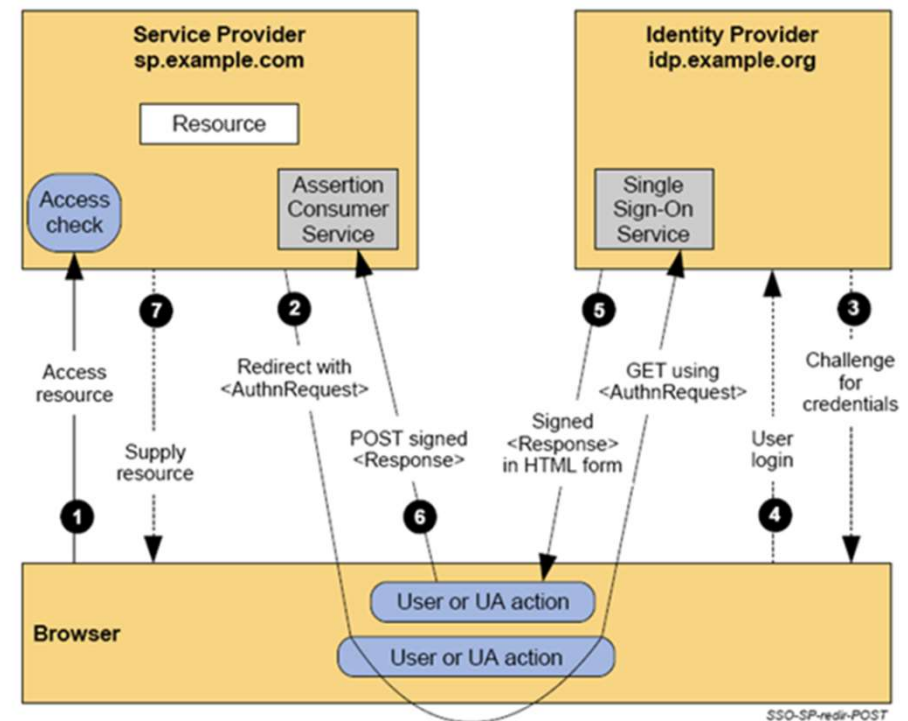
The Security Assertion Markup Language (SAML) standard defines a framework for exchanging

Web SSO profile

- IDP와 SP는 직접 통신하지 않음(사용자 브라우저가 정보 전달)
- SP는 IdP의 계정 DB에 접근할 수 없음
- 메타데이터를 교환하지 않으면 통신 불가능



(1) SAML 메타데이터 교환



(2) 인증메시지 교환

Source: Wikipedia, ECLIPSE Foundation

- ✓ 개체식별자(EntityID)
- ✓ 기관도메인(Scope)
- ✓ 공개키(Signature/encryption)
- ✓ 서비스 주소(Protocol endpoints)
- ✓ Contacts

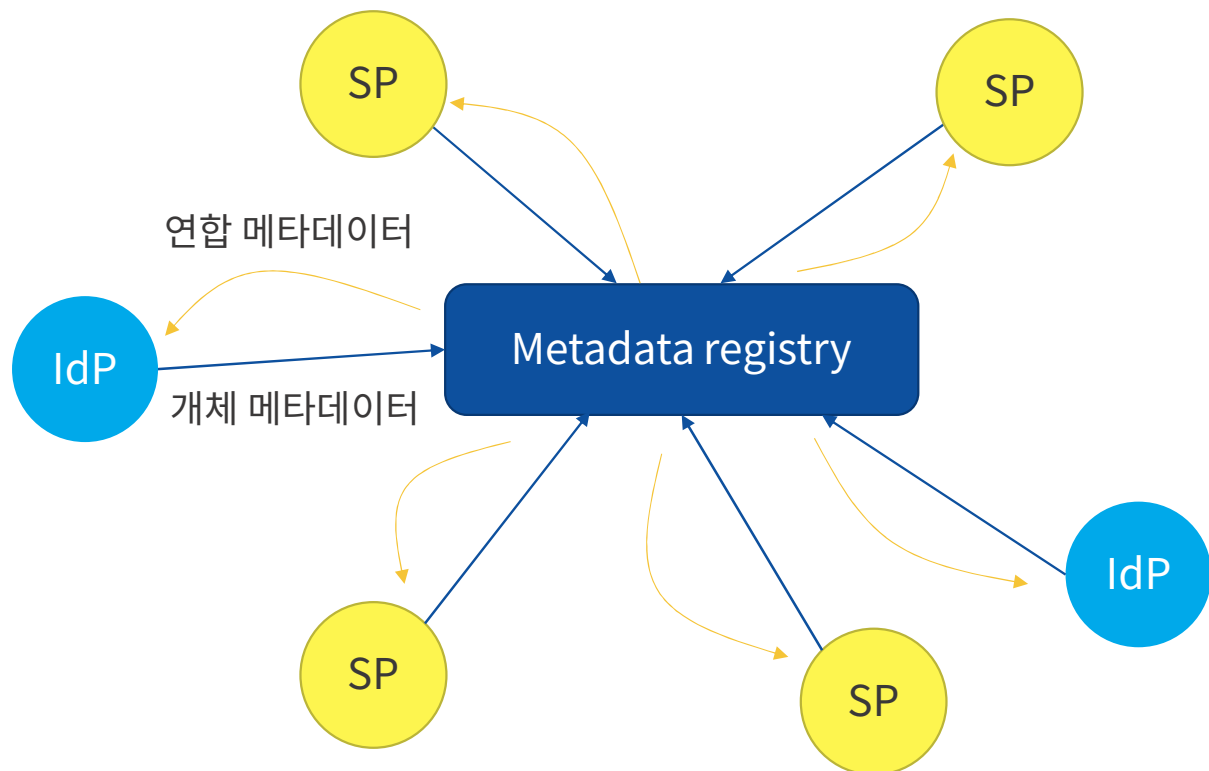
```

<?xml version='1.0'>
<EntityDescriptor xmlns:saml="urn:oasis:names:to:SAML:2.0:metadata" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  ID="https://coreen-idp.kreonet.net/idp/simplesaml.php" ID="pf7e712720-a30c-d1f4-0548-88fe79206281"><ds:Signature>
  <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#pf7e712720-a30c-d1f4-0548-88fe79206281"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:
  <ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIIDuTCCAqGgAwIBAgIJAOCu00jK2GcAMAOGCSqGSIb3DQEBCwUAMB9xGzAJBgNVBAYTAkSMRAwDgYDVQQHDAEYTWVqZW9uMQ4wDAYDVQQDAVNVN1STEhMB0GA1UEAwYw
  <ds:X509Data>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
  <ds:X509Certificate>MIIDuTCCAqGgAwIBAgIJAOCu00jK2GcAMAOGCSqGSIb3DQEBCwUAMB9xGzAJBgNVBAYTAkSMRAwDgYDVQQHDAEYTWVqZW9uMQ4wDAYDVQQDAVNVN1STEhMB0GA1UEAwYw
  <ds:X509Data>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-Redirect" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SingleLogoutService"
  <md:SingleLogoutService Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-POST" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SingleLogoutService"
  <md:NameIDFormat="urn:oasis:names:to:SAML:2.0:nameid-format:transient"/><md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-Redirect" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SSOService.php"
  <md:SingleSignOnService Binding="urn:oasis:names:to:SAML:2.0:bindings:HTTP-POST" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SSOService.php"/>
  <md:IDPSSODescriptor>
  <md:Organization>
  <md:OrganizationName xml:lang="en">KREONET</md:OrganizationName>
  <md:OrganizationDisplay xml:lang="en">KREONET</md:OrganizationDisplay>
  <md:OrganizationURL xml:lang="en">http://www.kreonet.net/</md:OrganizationURL>
  </md:Organization>
  <md:ContactPerson contactType="technical">
  <md:GivenName>coreen</md:GivenName>
  <md:SurName>support</md:SurName>
  <md:EmailAddress>coreen@kreonet.net</md:EmailAddress>
  </md:ContactPerson>
  </md:EntityDescriptor>

```

메타데이터의 교환

- FIM Operator가 개체 메타데이터를 수집 후 연합 메타데이터를 배포
 - 연합 메타데이터



SAML 인증요청 메시지

- 서비스제공자가 인증요청 메시지를 생성

- ✓ IdP의 SSO URL
- ✓ ACS(Assertion Consumer Service) 주소
- ✓ 서비스제공자 식별자

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_bc6335d0970e40d7d40c161ca9e1adcfdd2d47c3d4"
  Version="2.0"
  IssueInstant="2022-11-14T08:17:21Z"
  Destination="https://saml.kafe.or.kr/simplesaml/saml2/idp/SSOService.php"
  AssertionConsumerServiceURL="https://webinar.kafe.or.kr/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  <saml:Issuer>https://webinar.kafe.or.kr/sp/simplesamlphp</saml:Issuer>
  <samlp:NameIDPolicy
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    AllowCreate="true"/>
  <samlp:Scoping>
    <samlp:RequesterID>https://webinar.kafe.or.kr/sp/python</samlp:RequesterID>
  </samlp:Scoping>
</samlp:AuthnRequest>
```

SAML 인증응답 메시지

- IdP가 인증응답 메시지를 생성
- Assertion: 인증에 성공한 사용자의 신원정보와 인증정보를 담고 있는 XML statement

- ✓ 메시지 발행자(Issuer)
- ✓ Signature
- ✓ Digest를 개인키로 암호화
- ✓ X.509 인증서
- ✓ 인증정보: 누가, 언제, 어떤 서비스제공자를 위해;
어떤 인증방식(예, 비밀번호)으로 로그인 했고;
메시지가 언제까지 유효한가?
- ✓ 사용자 속성값

```
<saml:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2d9926a42ce0f17629c6af30a6dd8a15fa7409415" InResponseTo="RkN2YnlEM"
  Version="2.0" IssueInstant="2007-01-02T20:48:35Z">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    idp.ssocircle.com
  </saml:Issuer>
  <saml:Status xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml:StatusCode xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
      Value="urn:oasis:names:tc:SAML:2.0:status:Success">
    </saml:StatusCode>
  </saml:Status>
  <saml:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
    ID="s276a3300f0e2b3d7f67a800d332156f0fdb99c5d0"
    InResponseTo="NKRDzVK7e" Version="2.0" IssueInstant="2007-01-02T20:48:35Z">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      idp.ssocircle.com
    </saml:Issuer>
    <saml:Status xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol">
      <saml:StatusCode xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
        Value="urn:oasis:names:tc:SAML:2.0:status:Success">
      </saml:StatusCode>
    </saml:Status>
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
      ID="s25d1bbb23ed13c6da325a6f7637c6dc5d9e7f13a9" IssueInstant="2007-01-02T20:48:35Z">
      <saml:Issuer>
        idp.ssocircle.com
      </saml:Issuer>
      <saml:Subject>
        <saml:NameID NameQualifier="idp.ssocircle.com" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
          amv90yvHQzEW2rmaRViMpWX4qyDA
        </saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml:SubjectConfirmationData NotOnOrAfter="2007-01-02T20:58:35Z" InResponseTo="NKRDzVK7e"
            Recipient="http://cgi.cohos.de:80/cgi-bin/zxid" ></saml:SubjectConfirmationData>
        </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2007-01-02T20:48:35Z" NotOnOrAfter="2007-01-02T20:58:35Z">
        <saml:AudienceRestriction>
          <saml:Audience>
            http://cgi.cohos.de:80/cgi-bin/zxid?o=B
          </saml:Audience>
        </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2007-01-02T20:48:35Z" SessionIndex="s24bfc21323ee9c117bf5769a074belff177262701">
        <saml:AuthnContext>
          <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
          </saml:AuthnContextClassRef>
        </saml:AuthnContext>
      </saml:AuthnStatement>
    </saml:Assertion>
  </saml:Response>
</saml:ArtifactResponse>
```


속성(Attributes)

Assertion에 속성(Attributes) 포함

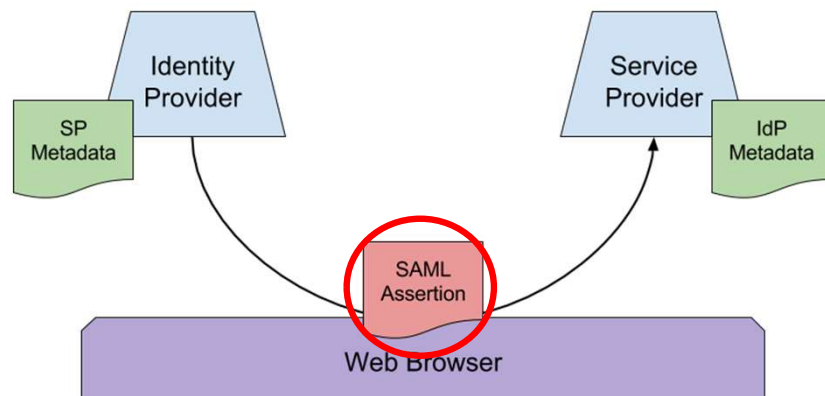
Friendly name/OID 형식 표기

¶ Friendly name

(예): cn/commonName, sn/surName,

¶ OID(Object Identifier)

(예): URN:OID:2.5.4.3



displayName

- SAML Name: urn:oid:2.16.840.1.113730.3.1.241
- LDAP source attribute: suDisplayName
- Example: Prof. John Doe

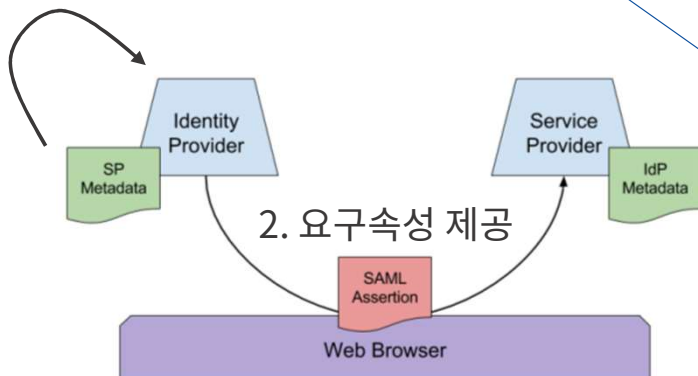
```

<saml:AttributeStatement>
  <saml:Attribute
    Name="urn:oid:2.16.840.1.113730.3.1.241"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">Jinyong JO
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:0.9.2342.19200300.100.1.3"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">jinyong.jo@gmail.com
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">staff
    </saml:AttributeValue>
    <saml:AttributeValue
      xsi:type="xs:string">member
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:2.5.4.10"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">KISTI
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">jiny92@coreen.or.kr
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:1.3.6.1.4.1.25178.1.2.9"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">coreen.or.kr
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:NameID
      NameQualifier="https://coreen-idp.kreonet.net/ldap/simplesamlphp"
      SPNameQualifier="https://filesender.kreonet.net/sp/simplesamlphp"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">d74f17c949df30493dc8cf7171959c01716f1d03
    </saml:NameID>
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
  
```

전달되는 속성값

- 서비스제공자는 SP 메타데이터에 요구속성을 명시
- IdP는 SP 메타데이터를 확인하고 요구속성 중 전달 가능한 속성을 전달

1. 서비스제공자의 요구속성 확인



2. 요구속성 제공

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:initialization"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xi="http://www.w3.org/2001/XInclude"
entityID="https://snu.bookcube.biz/sp/shibboleth">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://kafe.kreonet.net" registrationID="1" />
  </md:Extensions>
```

...

```
<md:AttributeConsumingService index="0">
  <md:ServiceName xml:lang="en">Bookcube for Seoul National University</md:ServiceName>
  <md:ServiceDescription xml:lang="en">It is a service that allows you to use e-books online. Users can use it to search for books and borrow them online.</md:ServiceDescription>
  <md:RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attr-format-urn" />
  <md:RequestedAttribute FriendlyName="eduPersonAffiliation" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attr-format-urn" />
  <md:RequestedAttribute FriendlyName="email" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attr-format-urn" />
  <md:RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat="urn:oasis:names:tc:SAML:2.0:attr-format-urn" />
</md:AttributeConsumingService>
```

SAML SP Metadata

주요 속성

- <https://www.kafe.or.kr/attributeMap> 참조 (KAFE 표기법)
 - 속성은 OID 표기법을 따름
 - 예, mail == urn:oid:0.9.2342.19200300.100.1.3

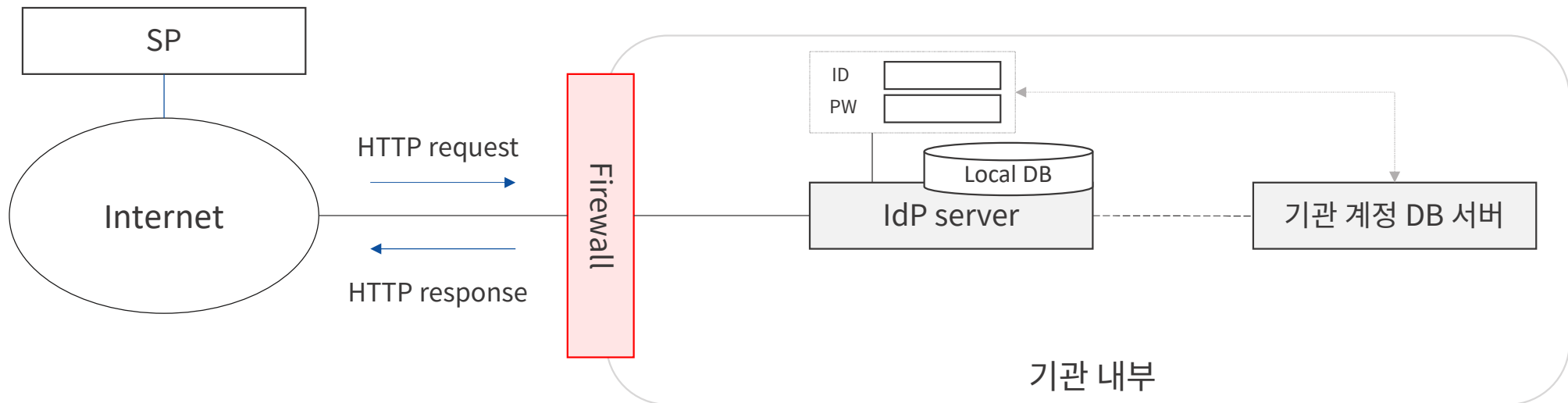
속성명	예시	설명
eduPersonTargetedID	Fdeef0012abcf22af	특정 서비스 한정 (사용자) 고유식별자
eduPersonPrincipalName	fedff0323aa@kafe.or.kr	글로벌 (사용자) 고유식별자 • 전자우편 주소와 다름
eduPersonScopedAffiliation	faculty@kafe.or.kr	기관 내 직무정보 • 전자우편 주소와 다름
eduPersonEntitlement	storage.read	리소스 접근 자격
displayName	John Doe	성명
cn (commonName)	John Doe	성명
Mail	john@kafe.or.kr	전자우편 • 'email' 속성은 사용하지 않음

2교시: 아이디어제공자의 구축



IdP의 역할 및 구동 환경

- 인증 요청의 수신
- ID/PW의 입력 (사용자)
- ID/PW의 유효성 검증 (with 사용자 계정 DB)
- 사용자 정보의 획득 (from 사용자 계정 DB)
- 사용자 정보의 가공 (속성화)
- 접근 제어 및 접근 기록 관리, etc.
- 사용자 동의
- 인증 응답의 송신



IdP 서버의 설치 환경

- Rocky 리눅스 8.8 (권장) 서버
 - 서버 설치 후 **Clean slate 유지**
- 서버 시스템 요구 사양 (최소)
 - 2 vCPU
 - 16 GB Memory
 - 100Mbps 네트워크 카드
 - 32 GB HDD
- 도메인 이름 및 공인 IP 할당
- 소프트웨어 방화벽 비활성화 (필요 시 KAFE 소프트웨어 설치 후 활성화)
 - iptables, selinux, firewalld 등

IdP 서버의 운영 환경

- Apache 2.4 이상
 - HTTPS용 TLS 인증서 필요 (기관보유 wildcard 인증서)
- PHP 8.2
- DBMS 클라이언트 드라이버 또는 RESTful API (사용자 계정 DB 연동 목적)
 - AD, LDAP, MSSQL, Tiberio, MySQL, Oracle, etc.
- NTP 시간 동기화
 - 기관 NTP 서버 연동 또는 time.kriss.re.kr (default) 이용
- 방화벽
 - 인터넷 ~ IdP 서버 구간: TCP 80/443 **입출력** 개방
 - IdP 서버 ~ 계정 DB 서버 구간: DBMS 포트 개방

데이터베이스 테이블 또는 API 구성

- 필수 항목 (최소)
 - User ID, user password, 이름, 이메일, 직무정보
- User ID/password
 - (권장) email ID와 다른 ID 사용
 - (권장) email PW와 다른 PW 사용
- 이름
 - (권장) 영문으로 성과 이름을 구분
- 직무정보
 - (필수) faculty, student, staff, alum 으로만 구분
 - (권장) alum은 서비스 이용 불가

기타

- 기관 로고 파일
 - 탐색 서비스 화면 용: 60x20 ~ 70x25 pixel
 - 로그인 화면 용: 240x80 pixel 내외

LOGIN to KAFE Web Portal Why am I here? ?

Search for an institution

☐ Remember selection ?

Previously chosen

K KAFE COREEN set.ID by KAFE | 비회원기관 로그인 ×

탐색 서비스 화면

Please select your organization below

K KAFE	COREEN set.ID by KAFE 비회원기관 로그인
NTS	National Science and Technology Information Service
CNU	Chungnam National University
EDISON	Everything for Computational Science and Engineering
KISTI	Korea Institute of Science and Technology Information
KFE	Korea Institute of Fusion Energy
KAIST	Korea Advanced Institute of Science and Technology

LOGIN to KAFE Web Portal

로그인 화면



KOREA UNIVERSITY
Identity Provider

Username

Password

Login

Please note

By accessing or using this service, you represent that you have read, understood, and agree to be bound by this [User Agreement](#) including any future modifications. Before entering your username and password, verify that the URL for this page begins with: <https://share-ss0.korea.ac.kr>

Trouble in login? or forgot your password? Contact your [IT Administration staffs](#)

설치

- Rocky linux 8.8 설치 후 IdP 서버로 SSH 접속
 - 현재 시간과 리눅스 서버 시간이 일치하는지 확인

- root 권한으로 변경

```
$ su
```

- KAFE IdP 설치 소프트웨어 다운로드
 - <https://git.kafe.or.kr/kafe-software/simplesamlphp-rocky-8-9-installer.git>
 - 권한 확보 필요
 - 권한 부재 시 support@kafe.or.kr에 zip 파일 제공 요청

```
$ cd ~
```

```
$ git clone https://git.kafe.or.kr/kafe-software/simplesamlphp-rocky-8-9-installer.git
```

- ‘SSL certificate problem’ 오류 발생 시

```
$ git config --global http.sslVerify false
```

```
$ git clone https://git.kafe.or.kr/kafe-software/simplesamlphp-rocky-8-9-installer.git
```

- 다운로드 성공 시 아래와 같음

```
$ ls
```

```
simplesamlphp-rocky-8.9-installer
```


환경 설정 - IdP 설치 소프트웨어

- Simpleamlphp-rocky-8-9-installer 디렉토리 이동 후 .env 수정

```
$ ls
simpleamlphp-rocky-8.9-installer

$ cd simpleamlphp-rocky-8.9-installer
$ nano .env
```

- .env 환경 변수 설정

```
# Local DB configuration (IdP 서버에서 관리하는 local DB, 설치 후 환경 변경 불가)
DB_USER           # KAFE_DB_NAME DB에 접근하기 위한 사용자 ID
DB_PASSWORD       # KAFE_DB_NAME DB에 접근하기 위한 사용자 PW
KAFE_DB_NAME      # 테스트용 사용자 DB 명 (기관 계정 DB 연동 전 사용)
USER_TEST_DB

INSTALLER_PATH    # 기본값 유지

# SAML SW 설치 경로
INSTALL_PATH      # 기본값 유지
SSP_VERSION       # 2.1.4

PHP_VERSION       # 기본값 유지

MODULES_REPO      # 기본값 유지
```

환경 설정 - IdP 설치 소프트웨어 (계속)

- .env 환경 변수 설정 (계속)

# SAML SW 환경 설정	
POSTFIX	# 기본값 유지
ADMIN_PASSWORD	# SAML SW 관리자 비밀번호
ADMIN_NAME	# SAML 소프트웨어/서버 관리자 이름, 기본값 유지
ADMIN_EMAIL	# 서버 관리자 이메일
OTP_DB_NAME	# 기본값 이용
# TLS 인증서 생성	
DOMAIN	# IdP 서버의 도메인 주소
SSL_CITYNAME	# 기관이 위치한 도시 이름(영문)
SSL_COMPANYNAME	# 기관이름(영문)
SSL_DEPTNAME	# 서버 관리 부서(영문)
MEMBER_ORG_KR	# 기관명(한글)
MEMBER_ORG	# 기관명(영문, fullname)
MEMBER_ORGDISPLAY	# 기관명(영문, fullname)
MEMBER_ORGURL	# 기관 대표 홈페이지 주소
MEMBER_ORGIMG	# 기관 로고(큰 그림) 파일 명
MEMBER_ORGIMG_DS	# 기관 로고(작은 그림) 파일 명

환경 설정 - IdP 설치 소프트웨어 (계속)

- .env 환경 변수 설정 (계속)

메타데이터 환경 변수 (중요)

META_SCOPE

기관 대표 도메인 명 예, kisti.re.kr, snu.ac.kr, korea.ac.kr 등

ATTRIBUTE_SCHACHOMEORG

META_SCOPE 값과 동일하게 설정

이하 기본 값으로 유지

- 설치 스크립트 실행

\$ pwd

/root/simplesamlphp-rocky-8-9-installer

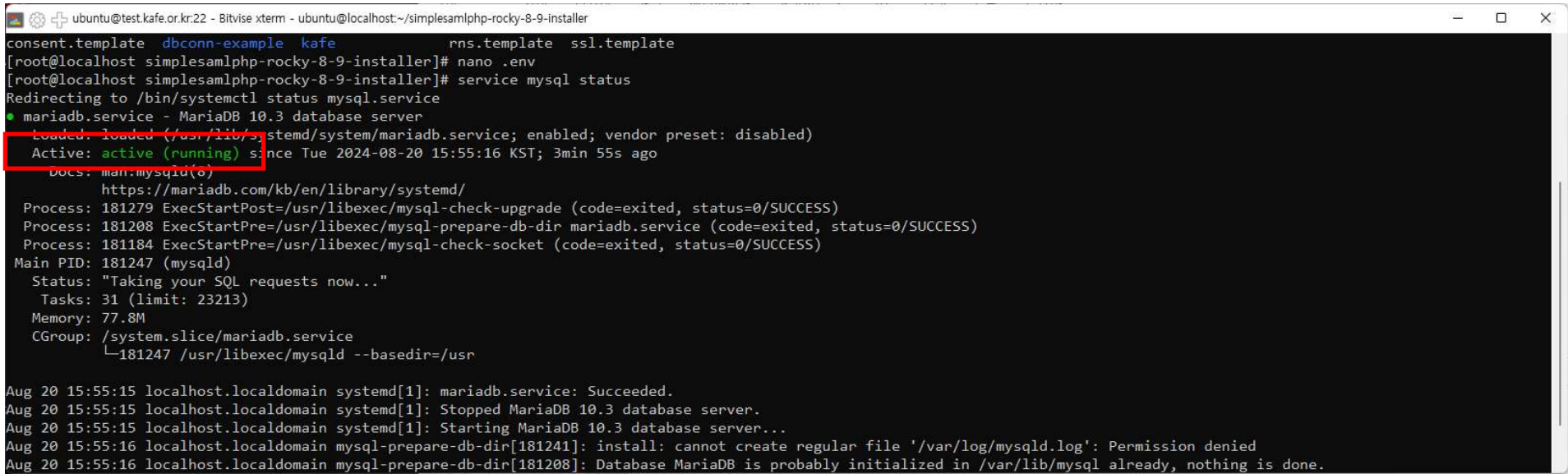
MEMBER_ORGIMG와 MEMBER_ORGIMG_DS에 설정한 로고파일 2개를 simplesamlphp-rocky-8-9-installer/kafe/theme/images 디렉토리에 복사한 후 아래 명령을 실행

\$ bash install.sh

설치 검증

- MariaDB, HTTPD, PHP

```
$ service mysqld status
$ service php-fpm status
$ service httpd status
$ service chronyd status
```

A terminal window titled 'ubuntu@test.kafe.or.kr:22 - Bitvise xterm - ubuntu@localhost:~/simplesamlphp-rocky-8-9-installer'. The terminal shows the command 'service mysql status' being executed, which redirects to 'systemctl status mysql.service'. The output shows 'mariadb.service - MariaDB 10.3 database server' is 'loaded' and 'Active: active (running)'. A red box highlights the 'Active: active (running)' line. Below this, the terminal shows the service's process details, including the main PID (181247) and the status 'Taking your SQL requests now...'. At the bottom, system logs show the service starting successfully at 15:55:15, but then failing at 15:55:16 due to a 'Permission denied' error when trying to create the log file '/var/log/mysqld.log'.

```
consent.template dbconn-example kafe rns.template ssl.template
[root@localhost simplesamlphp-rocky-8-9-installer]# nano .env
[root@localhost simplesamlphp-rocky-8-9-installer]# service mysql status
Redirecting to /bin/systemctl status mysql.service
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-08-20 15:55:16 KST; 3min 55s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 181279 ExecStartPost=/usr/libexec/mysql-check-upgrade (code=exited, status=0/SUCCESS)
   Process: 181208 ExecStartPre=/usr/libexec/mysql-prepare-db-dir mariadb.service (code=exited, status=0/SUCCESS)
   Process: 181184 ExecStartPre=/usr/libexec/mysql-check-socket (code=exited, status=0/SUCCESS)
  Main PID: 181247 (mysqld)
    Status: "Taking your SQL requests now..."
     Tasks: 31 (limit: 23213)
    Memory: 77.8M
   CGroup: /system.slice/mariadb.service
           └─181247 /usr/libexec/mysqld --basedir=/usr

Aug 20 15:55:15 localhost.localdomain systemd[1]: mariadb.service: Succeeded.
Aug 20 15:55:15 localhost.localdomain systemd[1]: Stopped MariaDB 10.3 database server.
Aug 20 15:55:15 localhost.localdomain systemd[1]: Starting MariaDB 10.3 database server...
Aug 20 15:55:16 localhost.localdomain mysql-prepare-db-dir[181241]: install: cannot create regular file '/var/log/mysqld.log': Permission denied
Aug 20 15:55:16 localhost.localdomain mysql-prepare-db-dir[181208]: Database MariaDB is probably initialized in /var/lib/mysql already, nothing is done.
```

DB table 확인

- DB 로그인

```
# .env 파일에 설정한 DB_USER 값과 DB_PASSWORD 값을 입력
$ mysql -u kafe -p
Password:
```

```
$ show databases;
$ use user_test_db;
$ show tables;
$ desc ex_users;
```

```
ubuntu@test.kafe.or.kr:22 - Bitvise xterm - ubuntu@localhost:~/simplesamlphp-rocky-8-9-installer
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'ls' at line 1
MariaDB [user_test_db]> show tables;
+-----+
| Tables_in_user_test_db |
+-----+
| ex_users                |
+-----+
1 row in set (0.001 sec)

MariaDB [user_test_db]> desc ex_users;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| pid   | int(10) | NO | PRI | NULL | auto_increment |
| username | varchar(30) | YES | | NULL | |
| password | varchar(20) | YES | | NULL | |
| name  | varchar(30) | YES | | NULL | |
| email | varchar(30) | YES | | NULL | |
| affi  | varchar(30) | YES | | NULL | |
+-----+-----+-----+-----+-----+-----+
6 rows in set (0.004 sec)

MariaDB [user_test_db]>
```

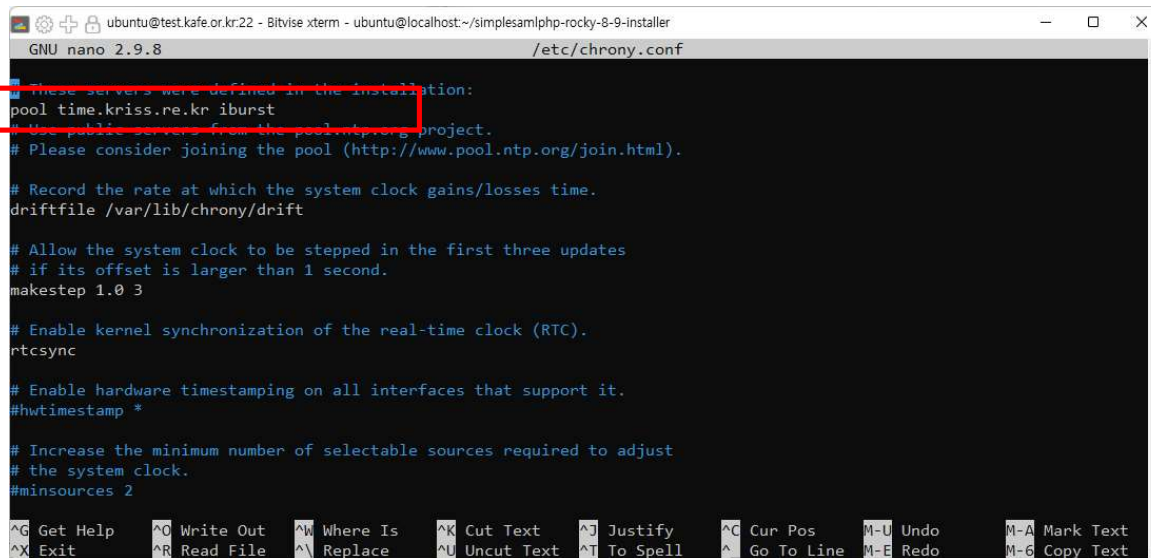
NTP 서버 변경

- Chronyd 사용 함

```
$ nano /etc/chrony.conf
```

```
# 아래 라인을 찾아 NTP 서버를 변경  
pool time.kriss.re.kr iburst
```

```
$ systemctl restart chronyd
```



```
ubuntu@test.kafe.or.kr:22 - Bitvise xterm - ubuntu@localhost:~/simplesamlphp-rocky-8-9-installer
GNU nano 2.9.8 /etc/chrony.conf
# These servers were defined in the installation:
pool time.kriss.re.kr iburst
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

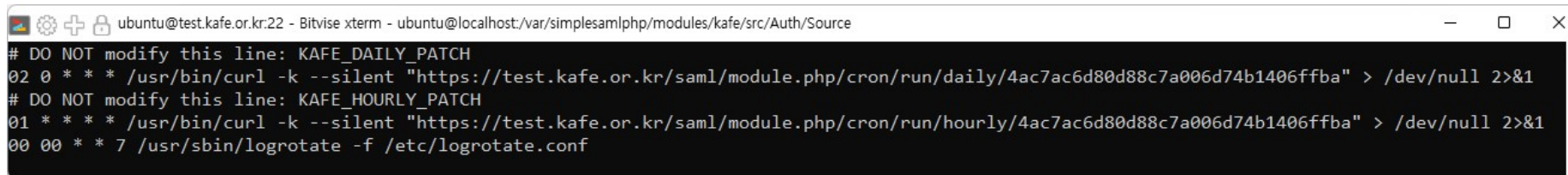
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos   M-U Undo     M-A Mark Text
^X Exit      ^R Read File  ^_ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line M-E Redo     M-G Copy Text
```

Cron 확인

- Cron을 이용해 연합 메타데이터를 주기적으로 다운로드 함

```
$ crontab -e
```

- IdP의 도메인이 test.kafe.or.kr인 경우



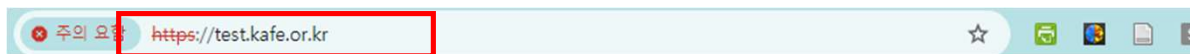
```
ubuntu@test.kafe.or.kr:22 - Bitvise xterm - ubuntu@localhost:/var/simplesamlphp/modules/kafe/src/Auth/Source
# DO NOT modify this line: KAFE_DAILY_PATCH
02 0 * * * /usr/bin/curl -k --silent "https://test.kafe.or.kr/saml/module.php/cron/run/daily/4ac7ac6d80d88c7a006d74b1406ffba" > /dev/null 2>&1
# DO NOT modify this line: KAFE_HOURLY_PATCH
01 * * * * /usr/bin/curl -k --silent "https://test.kafe.or.kr/saml/module.php/cron/run/hourly/4ac7ac6d80d88c7a006d74b1406ffba" > /dev/null 2>&1
00 00 * * 7 /usr/sbin/logrotate -f /etc/logrotate.conf
```

- 연합 메타데이터의 다운로드 주소 확인

```
$ nano /var/simplesamlphp/config/module_metarefresh.php
```

HTTP 서비스 확인

- .env 파일에 DOMAIN 변수 값으로 설정한 주소로 접근



연결이 비공개로 설정되어 있지 않습니다.

공격자가 **test.kafe.or.kr**에서 정보(예: 비밀번호, 메시지, 신용카드 등)를 도용하려고 시도
중일 수 있습니다. [자세히 알아보기](#)

NET::ERR_CERT_AUTHORITY_INVALID

고급

새로고침

공인 TLS 인증서 설치

- 환경 설정

```
$ nano /etc/httpd/conf.d/ssl.conf
```

```
SSLCertificateFile /etc/pki/tls/test.kafe.or.kr/ca.crt  
SSLCertificateKeyFile /etc/pki/tls/test.kafe.or.kr/ca.key  
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt  
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

```
# 기관 wildcard 인증서로 cert로 변경  
# 기관 wildcard 인증서의 key로 변경  
# 필요 시 변경  
# 필요 시 변경
```

```
# 설정 후
```

```
$ systemctl restart httpd
```



- 설치된 초기 IdP 소프트웨어는 IdP 서버 내 Local DB에 연동된 상태 → 기관 계정 DB로 연동 변경 필요
- IdP 서버에 기관 계정 DB의 DBMS Client driver 설치(예, Oracle OCI client)

아래 예시는 기관 계정 DB의 DBMS가 Oracle일 경우에 한 함 → 기관 DBMS에 맞는 driver 설치

```
$ dnf install systemtap-sdt-devel -y
```

```
$ rpm -ivh oracle-instantclient19.9-devel-19.9.0.0.0-1.x86_64.rpm
```

```
$ php -r "oci_connect();"
```

```

ubuntu@test:~$ cd /root/.ssh/ && cp -r ~/.ssh/oci8 ~/.ssh/oci8
interface:lo oci8 failover.lo -Wl,-rpath,/usr/lib/oracle/19.9/client64/lib -L/usr/lib/oracle/19.9/client64/lib -lcintsh
libtool: link: cc -shared -fPIC -DPIC ./libs/oci8_dtrace.d.o ./libs/oci8.o ./libs/oci8_lob.o ./libs/oci8_statement.o ./libs/oci8_collection.o ./libs/oci8_interface.o ./libs/oci8_failover.o -L/usr/lib/oracle/19.9/client64/lib -lcintsh -g -O2 -Wl,-rpath -Wl,/usr/lib/oracle/19.9/client64/lib -Wl,-soname -Wl,oci8.so -o ./libs/oci8.so
libtool: link: ( cd './libs' && rm -f 'oci8.la' && ln -s '../oci8.la' 'oci8.la' )
/bin/sh /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/libtool --tag=CC --mode=install cp ./oci8.la /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/modules
libtool: install: cp ./libs/oci8.so /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/modules/oci8.so
libtool: install: cp ./libs/oci8.lai /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/modules/oci8.la
libtool: finish: PATH="/home/ubuntu/.local/bin:/home/ubuntu/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin" ldconfig -n /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/modules
-----
Libraries have been installed in:
  /root/simplesamphp-rocky-8-9-installer/oracle/oci8_php8.2/oci8-3.3.0/modules

If you ever have to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the 'LLIBDIR'
flag during linking and do at least one of the following:

- add LIBDIR to the 'LD_LIBRARY_PATH' environment variable
during execution
- add LIBDIR to the 'LD_RUN_PATH' environment variable
during linking
- use the '-Wl,-rpath -Wl,LIBDIR' linker flag
- have your system administrator add LIBDIR to '/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as ld(1) and ld.so(8) manual pages.
-----

Build complete.
Don't forget to run 'make test'.

root@localhost:~# cd /root/.ssh/ && cp -r ~/.ssh/oci8 ~/.ssh/oci8
PHP Fatal error: Uncaught ArgumentCountError: oci_connect() expects at least 2 arguments, 0 given in Command line code:1
Stack trace:
#0 Command line code(1): oci_connect()
#1 (main)
thrown in Command line code on line 1
## finished##

[root@localhost:~# cd /root/.ssh/ && cp -r ~/.ssh/oci8 ~/.ssh/oci8]# php -r "oci_connect();"
PHP Fatal error: Uncaught ArgumentCountError: oci_connect() expects at least 2 arguments, 0 given

```

기관 계정 DB 연동 검증 – 검증용 Script 작성

- 테스트용 php script를 작성

[simplsam|php-rocky-8-9-installer/dbconn-example/oci_connect.php](#)를 참조

```
$ nano oci_connect.php
```

```
<?php
```

```
$db_username='DB_USER_NAME';
```

```
$db_userpass='DB_USER_PASS';
```

```
$username='USER_NAME';
```

```
$password='USER_PASS';
```

```
# tns(Transparent Network Substrate) string
```

```
$db = "(DESCRIPTION=(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = DB_IP_ADDR)(PORT = DB_PORT)))(CONNECT_DATA=(SID=SID_NAME)))";
```

```
$conn = oci_connect($db_username, $db_userpass, $db);
```

```
if(!$conn){ $e = oci_error(); var_dump($e); }
```

```
# 비밀번호 암호화 알고리즘을 고려해 질의해야 함
```

```
$stid = oci_parse($conn, "SELECT * FROM TABLENAME_ORG WHERE USERNAME_ORG='$username' and PASSWORD_ORG='$password'");
```

```
oci_execute($stid);
```

```
if(!$row = oci_fetch_assoc($stid)){ echo "error"; exit; }
```

```
var_dump($row);
```

```
oci_free_statement($stid);
```

```
oci_close($conn);
```

```
?>
```

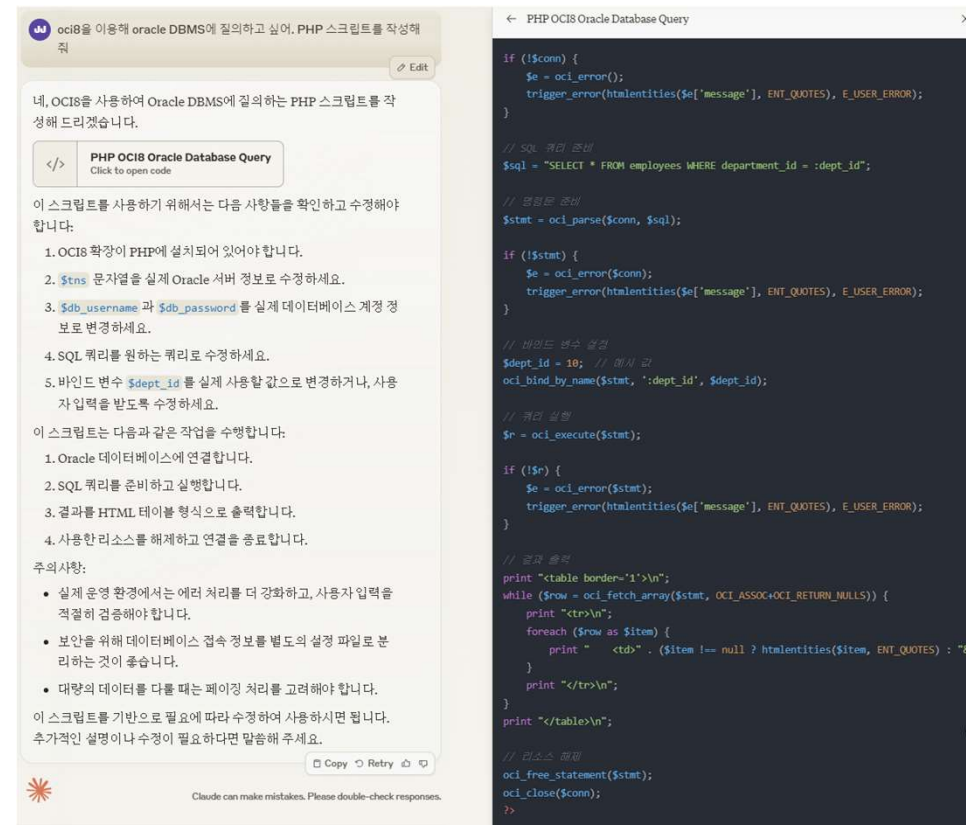
기관 계정 DB 연동 검증 -Script 동작 검증

- IdP 서버와 기관 계정 DB 간 연동 검증

\$ php oci_connect.php

사용자 정보가 정상적으로 출력되면 OK

<참고> claude.ai 또는 chat.openai.com를 이용해 원시 script 작성 가능
예, 'oci8을 이용해 oracle DBMS에 질의하고 싶어. PHP 스크립트를 작성해줘'
예, 'API 호출 경로가
<https://kafe.or.kr/authencation/users?id=username&pw=123> 임.
PHP 8.2에서 동작하는 스크립트를 작성해줘'



IdP와 기관 계정 DB 연동 (계속)

- 기관 계정 DB 연동 및 로그인 시도 횟수 제한

```
$ nano /var/simplesamlphp/modules/kafe/src/Auth/Source/CoreAuth.php
```

```
# 데이터 베이스 연결설정과 질의 등(반환 값을 얻어오는 부분까지)은 oci_connect.php를 참조해 설정
# DB 연결 설정과 관련된 오류는 'throw new Exception()'을 이용해 예외 처리 함
```

```
...;
$row = oci_fetch_assoc($stmt);
```

```
if(!$row) $tmp_userinfo = false;
else {
```

```
    $tmp_userinfo = [
        'name' => $row['name'],
        'email' => $row['email']
    ];
}
```

```
# 사용자 잠금 확인(blockCheck()) 및 로그인 시도횟수 초과 사용자 잠금(wrongUserpass())
```

```
$kafeUtil = new kafe\Util();
```

```
$this->blockCheck($kafeUtil, $username, $tmp_userinfo);
```

```
If (!$row) {
```

```
    /* User not found */
```

```
    Logger::warning( ' MyAuth: Could not find user ' . Var_export($username, TRUE) . ' . ' );
```

```
    $this->wrongUserpass($kafeUtil, $username, []);
```

```
}
```

```
/* 생략 If (!$this->checkPassword($row['password'], $password)) { ..., } */
```

```
// Login success
```

```
$kafeUtil->resetWrongCount($username);
```

\$username: 사용자 ID (사용자 이름 아님)

계정 DB에서 반환되는 배열을 \$row로 가정
\$row에 사용자 속성값이 저장됨

\$row['affi']: 사용자의 직무정보

\$row['name']: 사용자의 성명

\$row['email']: 사용자의 전자우편 주소

IdP와 기관 계정 DB 연동 (계속)

- 사용자 속성값 확보 및 생성

직무 정보가 affiliationMap에 존재하면, 반환 받은 값에 member를 추가해 eAffiliation에 저장
예, 'faculty'를 반환 받으면 ['faculty', 'member']로 변경

eduPersonAffiliation 생성

```
if (array_key_exists($row[ ' affi ' ], $this->affiliationMap)) {
    $this->eAffiliation = $this->affiliationMap[$row[ ' affi ' ]];
} else {
    $this->eAffiliation = [ ' affiliate ' ];
}
```

직무정보가 alum인 사용자 차단

```
if (in_array('alum', $this->eAffiliation)) {
    Logger::warning('KafeAuth: the user ' . var_export($username, TRUE) . ' has no privilege. ');
    throw new Error('NOPRIVILEGE');
}
```

\$config = Configuration::getOptionalConfig('module_kafe.php')->toArray();

sn과 givenName 생성: 성명을 '성 ' 과 '이름 ' 으로 분리

```
$name = $this->separateName($row['name']);
$sn = [$name['sn']]; # 성
$givenname = [$name['gn']]; #이름
```

eduPersonScopedAffiliation 생성: scope 내 직무정보를 표기 예, faculty@kafe.or.kr

구축한 IdP의 scope이 "kafe.or.kr"인 경우

```
$sepsAffiliation = [$this->eAffiliation[0] . "@kafe.or.kr"];
```

\$username: 사용자 ID (사용자 이름 아님)

계정 DB에서 반환되는 배열을 \$row로 가정
\$row에 사용자 속성값이 저장됨

\$row['affi']: 사용자의 직무정보

\$row['name']: 사용자의 성명

\$row['email']: 사용자의 전자우편 주소

```
$this->affiliationMap = array(
    ...,
    'student' => array('student', 'member'),
    'staff' => array('staff', 'member'),
    'faculty' => array('faculty', 'member'),
    'alum' => array('alum'),
);
```

IdP와 기관 계정 DB 연동 (계속)

- 사용자 속성값 확보 및 생성

```
# eduPersonPrincipalName 생성
# 구축한 IdP의 scope이 "kafe.or.kr"이고
# sha1으로 $username을 encryption 한 경우
$seppName = [sha1($username) . "@kafe.or.kr"];

# 모든 속성값은 배열([]) 형태로 저장
$attributes = [
    'uid' => [$username],
    'displayName' => [$row["name"]], #성명과 동일
    'email' => $row["email"],
    'sn' => $sn,
    'givenName' => $givenname,
    'eduPersonAffiliation' => $this->eAffiliation,
    'eduPersonPrincipalName' => $seppName,
    'eduPersonScopedAffiliation' => $sepsAffiliation,
    'mail' => $row["email"],
    'organizationName' => ["Korean Access Federation"],
    'schacHomeOrganization' => ["kafe.or.kr"],
```

...

\$username: 사용자 ID (사용자 이름 아님)

계정 DB에서 반환되는 배열을 \$row로 가정
\$row에 사용자 속성값이 저장됨

\$row['affi']: 사용자의 직무정보

\$row['name']: 사용자의 성명

\$row['email']: 사용자의 전자우편 주소

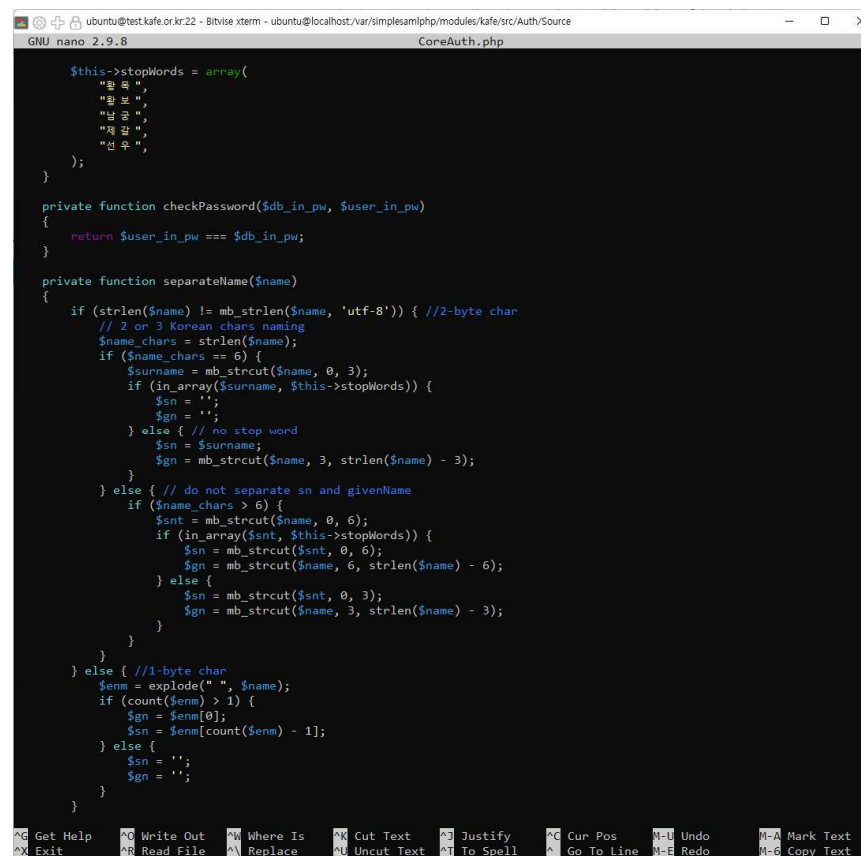
#email과 mail의 값은 동일

기관 이름이 "Korean Access Federation"인 경우

IdP의 scope이 "kafe.or.kr"인 경우

성명의 분리

- 기관 계정 DB에서 사용자의 ‘성’과 ‘이름’을 구분하지 않을 경우
 - IdP 소프트웨어가 자동 구분 → **성과 이름의 구분이 실제와 다를 수 있음**



```
GNU nano 2.9.8 CoreAuth.php

$this->stopWords = array(
    "왕",
    "왕",
    "남",
    "재",
    "선"
);

}

private function checkPassword($db_in_pw, $user_in_pw)
{
    return $user_in_pw === $db_in_pw;
}

private function separateName($name)
{
    if (strlen($name) != mb_strlen($name, 'utf-8')) { //2-byte char
        // 2 or 3 Korean chars naming
        $name_chars = strlen($name);
        if ($name_chars == 6) {
            $surname = mb_substr($name, 0, 3);
            if (in_array($surname, $this->stopWords)) {
                $sn = '';
                $gn = '';
            } else { // no stop word
                $sn = $surname;
                $gn = mb_substr($name, 3, strlen($name) - 3);
            }
        } else { // do not separate sn and givenName
            if ($name_chars > 6) {
                $snt = mb_substr($name, 0, 6);
                if (in_array($snt, $this->stopWords)) {
                    $sn = mb_substr($snt, 0, 6);
                    $gn = mb_substr($name, 6, strlen($name) - 6);
                } else {
                    $sn = mb_substr($snt, 0, 3);
                    $gn = mb_substr($name, 3, strlen($name) - 3);
                }
            }
        }
    } else { //1-byte char
        $nm = explode(" ", $name);
        if (count($nm) > 1) {
            $gn = $nm[0];
            $sn = $nm[count($nm) - 1];
        } else {
            $sn = '';
            $gn = '';
        }
    }
}
```


디버깅 정보

- Linux log files

```
# /var/log/php-fpm/www-error.log  
# /var/log/messages  
# /var/log/httpd/ssl_access_log  
# /var/log/httpd/ssl_error_log
```

```
ubuntu@test.kafe.or.kr:22 - Bitvise xterm - ubuntu@localhost:/var/simplesamlphp/modules/kafe/src/Auth/Source  
^C  
[root@localhost Source]# tail -f /var/log/php-fpm/www-error.log  
[20-Aug-2024 17:35:29 Asia/Seoul] PHP Warning: Trying to access array offset on value of type null in /var/simplesamlphp/modules/kafe/src/Auth/UserPassBase.php on line 373  
[20-Aug-2024 17:46:17 Asia/Seoul] PHP Warning: Undefined array key 0 in /var/simplesamlphp/modules/affiliationfilter/src/Auth/Process/AffiliationFilter.php on line 157  
[20-Aug-2024 17:46:17 Asia/Seoul] PHP Warning: Undefined array key 0 in /var/simplesamlphp/modules/attributerule/src/Auth/Process/AttributeRelease.php on line 101  
[20-Aug-2024 17:46:17 Asia/Seoul] PHP Warning: session_cache_limiter(): Session cache limiter cannot be changed when a session is active in /var/simplesamlphp/modules/consent/src/Controller/ConsentController.php on line 134  
[20-Aug-2024 17:46:17 Asia/Seoul] PHP Warning: Undefined array key "consent:useLogo" in /var/simplesamlphp/modules/consent/src/Controller/ConsentController.php on line 262  
[20-Aug-2024 17:46:22 Asia/Seoul] PHP Warning: session_cache_limiter(): Session cache limiter cannot be changed when a session is active in /var/simplesamlphp/modules/consent/src/Controller/ConsentController.php on line 134  
[20-Aug-2024 18:12:11 Asia/Seoul] PHP Warning: Undefined array key "uid" in /var/simplesamlphp/modules/kafe/src/Auth/UserPassBase.php on line 373  
[20-Aug-2024 18:12:11 Asia/Seoul] PHP Warning: Trying to access array offset on value of type null in /var/simplesamlphp/modules/kafe/src/Auth/UserPassBase.php on line 373  
[21-Aug-2024 10:34:06 Asia/Seoul] PHP Warning: Undefined array key "uid" in /var/simplesamlphp/modules/kafe/src/Auth/UserPassBase.php on line 373  
[21-Aug-2024 10:34:06 Asia/Seoul] PHP Warning: Trying to access array offset on value of type null in /var/simplesamlphp/modules/kafe/src/Auth/UserPassBase.php on line 373
```

<참고> 탐색 서비스용 로고 파일의 위치

- 서버 도메인이 test.kafe.or.kr이고 로고 파일(작은 그림)이 my_inst_logo.png 이면
- 로그파일의 위치 URL은 https://test.kafe.or.kr/my_inst_logo.png 임
→ 탐색서비스 로고 표시에 활용되므로 KAFE에 위치 URL을 알려야 함

3교시: IdP의 검증/관리와 KAFE 가입



구축된 IdP의 검증

- IdP의 메타데이터 확보
 - [https://\[test.kafe.or.kr\]/saml/module.php/admin](https://[test.kafe.or.kr]/saml/module.php/admin)
 - 암호는 .env 파일의 ADMIN_PASSWORD 값
 - Federation 탭 클릭
 - SAML 2.0 IdP metadata 클릭
 - In SAML 2.0 Metadata XML format의 메타데이터를 복사

The screenshot shows the KAFE Identity Provider admin interface. The 'Federation' tab is selected. A message indicates that the user is running an outdated version of SimpleSAMLphp and should update to the latest version. Below this, a dropdown menu is open, showing 'KREONET KAFE' as the selected entity. The 'SAML 2.0 IdP metadata' option is highlighted. A red arrow points from this option to the 'SAML Metadata' section below. In the 'SAML Metadata' section, the URL for the metadata is provided: <https://test.kafe.or.kr/saml/module.php/saml/idp/metadata>. A red box highlights the 'Download' icon next to the URL. Below the URL, the SAML 2.0 Metadata XML format is displayed, and a red box highlights the 'Signature' element in the XML.

KAFE Identity Provider

Configuration Test **Federation** Log out

You are running an outdated version of SimpleSAMLphp. Please update to [the latest version](#) as soon as possible.

SimpleSAMLphp is installed in [/usr/local/saml](#)
You are running version 2.11.0

KREONET KAFE
EntityID: <https://test.kafe.or.kr/idp/simpleasamlphp> (hostname: default)
Type: **SAML 2.0 IdP metadata**

Modules

You have the following modules installed (ⓘ means the module is not enabled):

- ✓ SAML 2.0 IdP
- ✓ admin
- ✓ affiliationfilter
- ✓ attributerule
- ✓ consent

SAML Metadata

You can get the metadata XML on a dedicated URL:
<https://test.kafe.or.kr/saml/module.php/saml/idp/metadata>

In SAML 2.0 Metadata XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:shibmd="urn:shibboleth:metadata:1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://test.kafe.or.kr/idp/simpleasamlphp" ID="_E1a81630c4a22a182738a7b152c4379d4e5159b45172184117971b7036170">
  <md:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xmldsig-core14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:Signature Value="MIGY..."/>
  </md:SignedInfo>
  <md:BaseID URI="#_E1a81630c4a22a182738a7b152c4379d4e5159b45172184117971b7036170">
    <ds:Transform URI="http://www.w3.org/2001/10/xmldsig-core14n#"/>
    <ds:Transform URI="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:DigestValue>...</ds:DigestValue>
  </md:BaseID>
  <md:NameID URI="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:Transform URI="http://www.w3.org/2001/10/xmldsig-core14n#"/>
    <ds:Transform URI="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:DigestValue>...</ds:DigestValue>
  </md:NameID>
  <md:Signature URI="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:Transform URI="http://www.w3.org/2001/10/xmldsig-core14n#"/>
    <ds:Transform URI="http://www.w3.org/2001/04/xmldsig-core14n#"/>
    <ds:DigestValue>...</ds:DigestValue>
  </md:Signature>
</md:EntityDescriptor>
```

Details

[Diagnostics on hostname, port and protocol](#)
[Information on your PHP installation](#)
[Consent administration](#)
[Cron module information page](#)
[KAFE Admin Panel](#)
[KAFE OTP Config](#)
[Metarefresh](#)

구축된 IdP의 검증 (계속)

- KAFE debugger에 IdP 메타데이터 등록
 - <https://debug.kafe.or.kr>
 - SAML 선택
 - Input raw xml에 IdP 메타데이터를 붙여넣기

<참고> debug.kafe.or.kr은 IdP를 검증하기 위한 검증용 서비스제공자 임

The screenshot displays the KAFE Debugger interface. At the top, it says "KAFE Debugger for KAFE members" and provides instructions for SAML service providers and clients. Below this, there are two large buttons: "SAML" (highlighted with a red box) and "OIDC". A red arrow points from the "SAML" button to the "SAML" tab in the navigation bar. The main content area shows a progress bar with three steps: 1. 메타데이터 등록 (Metadata Registration), 2. 메타데이터 확인 (Metadata Confirmation), and 3. 로그인 검증 (Login Verification). Below the progress bar, the "SAML Debugger for KAFE members" section is visible. It includes instructions for SAML service providers and a note about the 7-day expiration of uploaded metadata. On the right, there is a form with two options: "File upload" and "Input raw xml" (highlighted with a red box). A red arrow points from the "Input raw xml" option to a text area labeled "Copy and paste XL-formatted metadata here". At the bottom right of the form is an "Enroll" button.

구축된 IdP의 검증 (계속)

- 로그인 검증으로 이동
 - 구축된 IdP를 선택하고 로그인
 - 사용자 정보가 전달되는지 확인

AuthnContextClassRef

Requested	Returned
urn:oasis:names:tc:SAML:2.0:ac:classes:Password	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

NameID

Value	Format
_048f1f12545ed132836baa8bc85816449b44d404e1	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SAML Attributes

Attribute	Value
displayName	홍길동
eduPersonAffiliation	student
eduPersonEntitlement	urn:mace:dir:entitlement:common-lib-terms
eduPersonPrincipalName	2439e0457579ab4fd962cbd80b9206aca794cc38@kafe.or.kr
eduPersonScopedAffiliation	student@kafe.or.kr
eduPersonTargetedID	c3bbfc19e9cf98ff6548bc498a6e1f5e37f69a07
mail	coreen@example.org
o	KREONET KAFE
schacHomeOrganization	kafe.or.kr
uid	student1

1 메타데이터 등록 2 메타데이터 확인 3 로그인 검증

Select your identity provider

Please select the identity provider where you want to authenticate.

Select your identity provider

Select a ACR type

urn:oasis:names:tc:SAML:2.0:ac:classes:Password

LOGIN

2명 이상의 사용자를 대상으로 검증: eduPersonTargetedID 값이 서로 달라야 함

KAFE 가입 등 회원기관 등록 절차

1. (가입 기관) IdP 가입신청서 작성 및 제출
 - 가입 신청서는 <https://www.kafe.or.kr/join>에서 'ID 제공자용 프로덕션 페더레이션 참가 신청서'를 다운로드
 - IdP 가입신청서는 **기관장(원장, 총장 등) 직인 필수**
 - 공문(수신처: 한국과학기술정보연구원) 또는 support@kafe.or.kr로 제출
 - 구축된 IdP의 메타데이터와 탐색서비스용 로고 파일의 위치를 함께 제출
2. (KISTI) KAFE Metadata Registry 시스템에 메타데이터 등록
 - 등록 후 연합 메타데이터가 배포되는데 **하루 이상 소요**
3. (가입 기관) 프로덕션 중인 서비스제공자를 대상으로 로그인 검증 실시
<참고> 상용 서비스 이용 시 기관 구독 및 별도 연결 설정 필요

IdP의 관리

- KAFE Admin Panel과 KAFE OTP Config를 이용해 IdP 관리
 - [https://\[test.kafe.or.kr\]/saml/module.php/admin](https://[test.kafe.or.kr]/saml/module.php/admin)

Details

[Diagnostics on hostname, port and protocol](#)

[Information on your PHP installation](#)

[Consent administration](#)

[Cron module information page](#)

[KAFE Admin Panel](#)

[KAFE OTP Config](#)

[Metarefresh](#)

KAFE Admin Panel

- 메뉴 설명
 - System config
 - 로그인 시도 횟수 및 로그 정보 설정
 - Lock/unlock user
 - 사용자 ID를 기준으로 차단 및 차단해제
 - Affiliation filter
 - 특정 서비스에 대한 접근을 직무정보를 기반으로 제어
 - Attribute release
 - 특정 서비스에 제공할 사용자 속성을 정의
 - Login records
 - 로그인 기록 확인
 - Consent records
 - 사용자 동의 기록을 확인

The screenshot displays the KAFE Admin Panel interface. On the left is a dark sidebar with a menu. The main content area is white and shows three configuration sections:

- Limit Verification Attempts:** A form with two input fields. The first is labeled "If attempts fail more than" and contains the value "5". The second is labeled "times, lock the user for" and contains the value "30", followed by "minutes". A green "Save" button is at the bottom.
- Login Log Configuration:** A section for configuring login logs. It has a "Logging Attributes when Login" label and a list of attributes with checkboxes: "SP Entity ID", "User Access IP", "Timestamp", "uid", "appn", "email", and "displayName". The "uid", "appn", "email", and "displayName" checkboxes are checked. A green "Save" button is at the bottom.
- Consent Log Configuration:** A section for configuring consent logs. It has a "Logging Attributes when Consent" label and a list of attributes with checkboxes: "SP Entity ID", "User Access IP", and "Timestamp". The "User Access IP" and "Timestamp" checkboxes are checked. A green "Save" button is at the bottom.

KAFE Admin Panel - Affiliation filter

- 특정 서비스제공자에 접속 허용할 사용자의 직무정보를 설정하는데 이용
- 이용 방법
 - 메타데이터에서 서비스제공자의 고유식별자 확인
 - /var/simplesamlphp/config/module_metarefresh.php에서 구축된 IdP가 사용 중인 연합 메타데이터를 확인 가능

```
# 예
'src' => 'https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-testfed/metadata.xml',
'src' => 'https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-eduGAIN/eduGAIN-SP.xml'
```

- 웹 브라우저에서 URL을 입력한 후, 설정하고자 하는 서비스제공자를 검색(예, thomson)
- 해당 서비스제공자의 개체식별자(entityID)를 확인

```
<!--
https://onepass.thomsonreuters.com/entity
-->
<md:EntityDescriptor entityID="https://onepass.thomsonreuters.com/entity">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://kafe.kreonet.net" registrationInstant="2022-03-08T05:05:00Z" />
    <mdattr:EntityAttributes>
      <saml:Attribute Name="http://kafe.kreonet.net/jurisdiction" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue>US</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
```

- 서비스제공자의 entityID를 선택하고, 해당 서비스에 접근할 수 있는 사용자의 직무정보를 입력

KAFE Admin Panel - Attribute release

- SP 메타데이터에 포함된 요구 속성과 다른 속성을 IdP가 제공하고자 하는 경우 이용
 - 예, mathworks는 eduPersonPrincipalName 또는 eduPersonTargetedID 중 하나의 속성을 필수 요구 하지만, metadata에는 위 속성이 필수 속성으로 지정되어 있지 않음 → IdP는 필수 속성 (Required attributes)만 제공 함

SUPPORTED PROTOCOLS:	• SAML 1.1 • SAML 2.0
REQUIRED ATTRIBUTES:	• urn:oid:1.3.6.1.4.1.5923.1.1.1.9 (eduPersonScopedAffiliation) • urn:oid:0.9.2342.19200300.100.1.3 (mail)
OPTIONAL ATTRIBUTES:	• urn:oid:1.3.6.1.4.1.5923.1.1.1.6 (eduPersonPrincipalName) • urn:oid:1.3.6.1.4.1.5923.1.1.1.10 (eduPersonTargetedID) • urn:oid:2.5.4.42 (givenName) • urn:oid:2.5.4.4 (sn)

SYSTEM
SSP
System config
Lock/unlock user
Affiliation filter
Attribute release

Attribute Release Policy

SP entityId
https://www.mathworks.com/edu-sp

Attributes to be released

eduPersonPrincipalName x
eduPersonScopedAffiliation x
mail x
Press enter to add attribute

KAFE OTP config

- 내장 TOTP 또는 외장(상용) MFA 이용 가능
 - 상용 MFA 이용 권장
 - RESTful API를 지원해야 함
 - 내장 TOTP는 Google OTP와 호환

• 내장 TOTP 이용 설정

```
$ nano /var/simplesamlphp/config/config.php
```

```
# 'authproc.idp'를 검색
# 아랫 라인의 주석(//)을 해제
//89 => 'kafeotp:OTP',
```

- OTP Config 환경 설정
 - OTP Processing flow: 기본값 유지
 - Force reacting to MFA profile: 기본값 유지
 - OTP invoke condition
 - 리스트에 명시된 SP를 제외하고 모든 SP에 대해서 활성화
 - 리스트에 명시된 SP만 활성화
 - 모든 SP에 대해서 비활성화

오류 관리

- 데몬 서비스 상태
 - httpd, php-fpm, mysqld, chronyd가 **항상 active (running) 상태로 유지**되어야 함

```
$ systemctl status httpd
$ systemctl status php-fpm
$ systemctl status mysqld
$ systemctl status chronyd
```

- ‘Metadata for the entity expired’ 오류
 - NTP 동기화 또는 metadata 업데이트 불량
 - Admin 화면에서 Metarefresh 클릭

Details

[Diagnostics on hostname, port and protocol](#)
[Information on your PHP installation](#)
[Consent administration](#)
[Cron module information page](#)
[KAFE Admin Panel](#)
[KAFE OTP Config](#)
[Metarefresh](#)

Debug information

The debug information below may be of interest to the administrator / help desk:

SimpleSAML_Error_Error: UNHANDLEDEXCEPTION

Backtrace:

1 www/_include.php:17 (SimpleSAML_exception_handler)
0 [builtin] (N/A)

Caused by: Exception: Metadata for the entity [https://ieeexplore.ieee.org/shibboleth-sp] expired 5709262 seconds ago.

Backtrace:

3 lib/SimpleSAML/Metadata/MetaDataStorageHandler.php:285 (SimpleSAML_Metadata_MetaDataStorageHandler::getMetadata)
2 lib/SimpleSAML/Metadata/MetaDataStorageHandler.php:319
(SimpleSAML_Metadata_MetaDataStorageHandler::getMetadataConfig)
1 modules/saml/lib/IdP/SAML2.php:334 (sspmod_saml_IdP_SAML2::receiveAuthnRequest)
0 www/saml2/idp/SSOService.php:19 (N/A)

- ‘Metadata not found’ 오류 (무시)
 - KAFE에 가입되어 있지 않은 서비스제공자 접근 시 발생
 - KAFE에서 다운로드를 거부한 국외 서비스제공자 접근 시 발생

정보 제공

- 상용서비스 연계 시 서비스제공자에 전달해야 하는 필수 정보
 - entityID, scope, affiliation 정보
 - entityID: 개체식별자
 - Scope: 기관 대표 도메인 (.env 파일 참조)
 - Affiliation: 서비스에 접근을 허용하고자 하는 사용자의 직무정보
 - IdP admin 화면의 Federation 메뉴 → SAML metadata 탭 → XML format에서 검색 가능
 - 'entityid', 'scope'으로 검색
 - Affiliation
 - 학생: student@scope
 - e.g., student@kafe.or.kr
 - 교수: faculty@scope
 - e.g., faculty@kafe.or.kr
 - 직원: staff@scope
 - e.g., staff@kafe.or.kr

Configuration Test **Federation** Log out

Hosted entities

KREONET KAFE

EntityID: <https://test.kafe.or.kr/idp/simplesamlphp> (hostname: default)

Type: SAML 2.0 IdP metadata

SAML Metadata

You can get the metadata XML on a dedicated URL:

<https://test.kafe.or.kr/saml/module.php/saml/idp/metadata>

In SAML 2.0 Metadata XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://test.kafe.or.kr/idp/simplesamlphp" ID="_6fa8162064be22af26736a7b152c4979d4ea51598a95172184f1797fb786bf70"><ds:Signature>
<ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
```

Korean Access Federation

<https://www.kafe.or.kr/>
support@kafe.or.kr