

신뢰기반 디지털 ID 관리기술

한국과학기술정보연구원 조진용
jiny92@kisti.re.kr

Audience

대상

- ¶ 통합인증과 인증연합에 관심 있는 누구나
- ¶ 인증연합에 참여 중인 학연 기관 및 서비스제공자

수준

- ¶ 초급+α
- ¶ IT 관련 기초지식 필요

참고

- ¶ CentOS 7 기준

Agenda

1교시 (13:30PM - 14:45PM)

- ¶ 실습환경 구성
- ¶ SAML 표준 소개
- ¶ 실습

2교시 (15:00PM - 16:30PM)

- ¶ 아이디제공자의 관리운영 등
- ¶ 실습

실습환경 구성

목적

- ¶ SAML의 개념과 동작원리 이해
- ¶ 아이디제공자(Identity provider)의 관리운영

할일

- ① 계정 생성
- ② Chrome용 SAML 플러그인 설치
- ③ notepad++ 설치

실습자료

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

실습환경 구성 - 계정 생성

계정 생성이 필요하지 않음 (Home 계정)

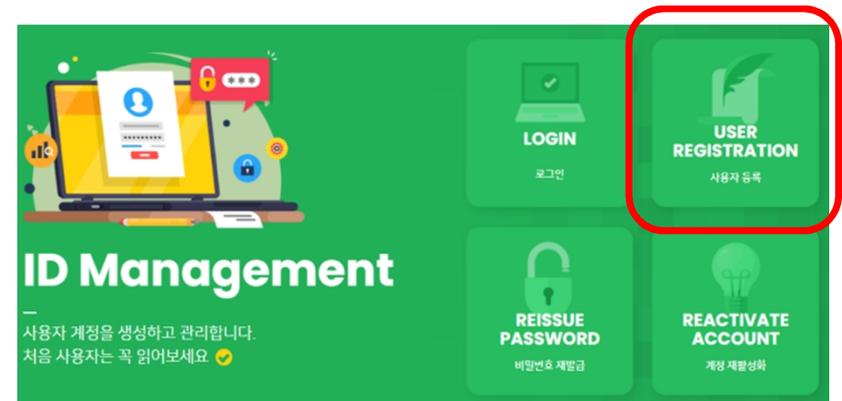
¶ KAFE 참여기관(https://www.kafe.or.kr/participants_idp)

계정 생성이 필요 (Guest 계정)

- ① <https://coreen-idp.kreonet.net> 방문
- ② 사용자 등록 메뉴에서 계정 생성
 - * 본명 사용
 - * 연구기관이나 교육기관 구성원은 기관 이메일 주소 입력

기억하세요!

¶ Guest 계정의 이름은 'COREEN Set.ID by KAFE'



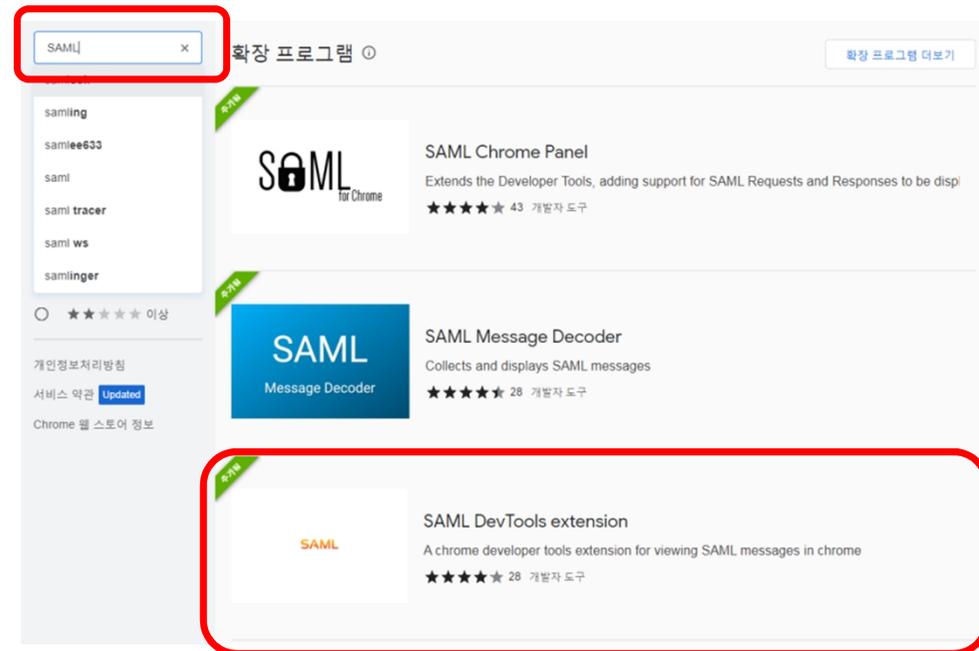
실습환경 구성 - Chrome용 SAML Plugin

설치 방법 (Chrome 브라우저)

- ① <https://chrome.google.com/webstore/category/extensions> 또는 Google에서 'Chrome 확장프로그램 설치'로 검색
- ② 'SAML' 로 검색
- ③ 'SAML DevTools extension' 로 설치

설치 확인

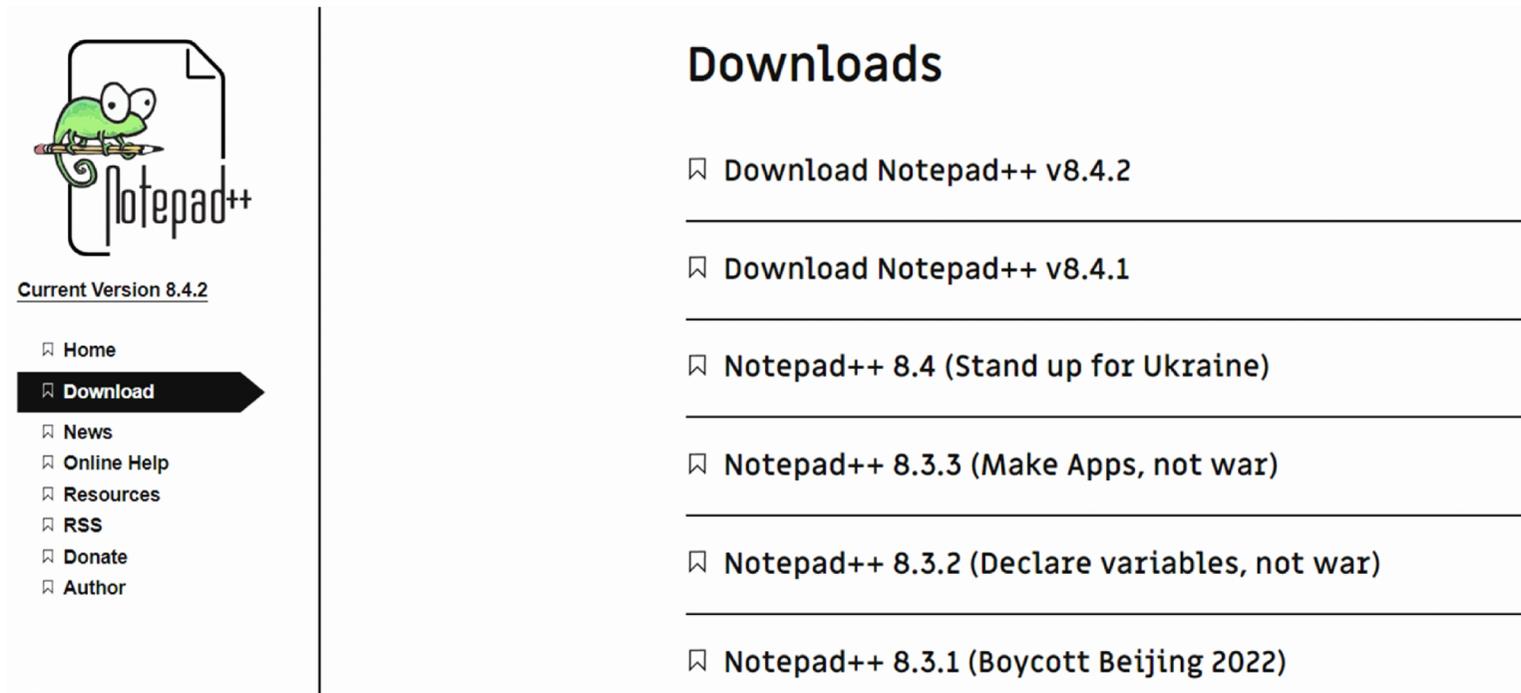
¶ Chrome 브라우저에서 F12 키 입력



실습환경 구성 - Notepad++

설치 방법

- ① Google에서 'notepad++'로 검색
- ② 최신버전을 다운로드 받아 설치



The image shows a screenshot of the Notepad++ website. On the left, there is a navigation menu with the following items: Home, Download (highlighted with a black arrow), News, Online Help, Resources, RSS, Donate, and Author. Above the menu is the Notepad++ logo, which features a green chameleon holding a pencil, with the text 'Notepad++' and 'Current Version 8.4.2' below it.

On the right, there is a 'Downloads' section with a list of download links, each preceded by a bookmark icon:

- Download Notepad++ v8.4.2
- Download Notepad++ v8.4.1
- Notepad++ 8.4 (Stand up for Ukraine)
- Notepad++ 8.3.3 (Make Apps, not war)
- Notepad++ 8.3.2 (Declare variables, not war)
- Notepad++ 8.3.1 (Boycott Beijing 2022)

Part I . SAML



SAML이란?

SAML [샘엘]

Security Assertion Markup Language
웹 통합인증(Single sign-on)을 위한 국제표준

보안 주장 표시 언어?



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

주요 용어

주체(Subject)

¶ 인증의 대상이 되는 사람이나 사물

인증(Authentication)

¶ 디지털 식별자(예, 사용자 ID와 비밀번호)를 이용한 주체의 검증

“Verifying that the subject seeking access to a resource is the one previously identified and approved”

인가/권한부여(Authorization)

¶ 주체가 서비스/리소스에 접근 가능 여부를 결정

속성(Attribute)

¶ 사용자의 신원정보(예, 이메일, 전화번호 등)

단언(Assertion)

¶ 인증의 주체, 인증상태, 속성정보 등을 주장

SAML

웹 통합인증(싱글사인온)을 위한 XML 규약

SAML 1.1(`03), SAML2.0(`05, Errata(정오표)/`19)

¶ OASIS 보안서비스 기술위원회 제정

연구교육분야 활용(`05~)

¶ SWITCH(스위스 연구망)

강화된 보안 vs 적용 어려움

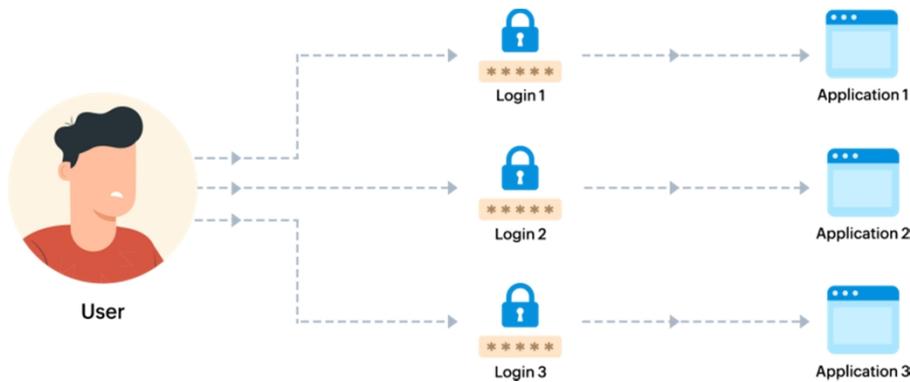
웹 환경 지원(모바일 미지원)

¶ OpenID Connect(OIDC) 출현

통합인증(싱글사인온, SSO)

하나의 아이디와 한번의 로그인으로 다수 응용서비스 이용

- ㉮ 보안성 ↑
- ㉮ 편의성 ↑
- ㉮ 관리비용 ↓



통합인증이 없는 경우



통합인증이 있는 경우

SAML 통합인증 시스템의 구성

아이디(신원정보) 제공자/Identity provider(IdP)

¶ 신원정보 관리

¶ 사용자 인증(로그인)

¶ SAML 메시지 처리(서명 등)

서비스 제공자/Service provider(SP)

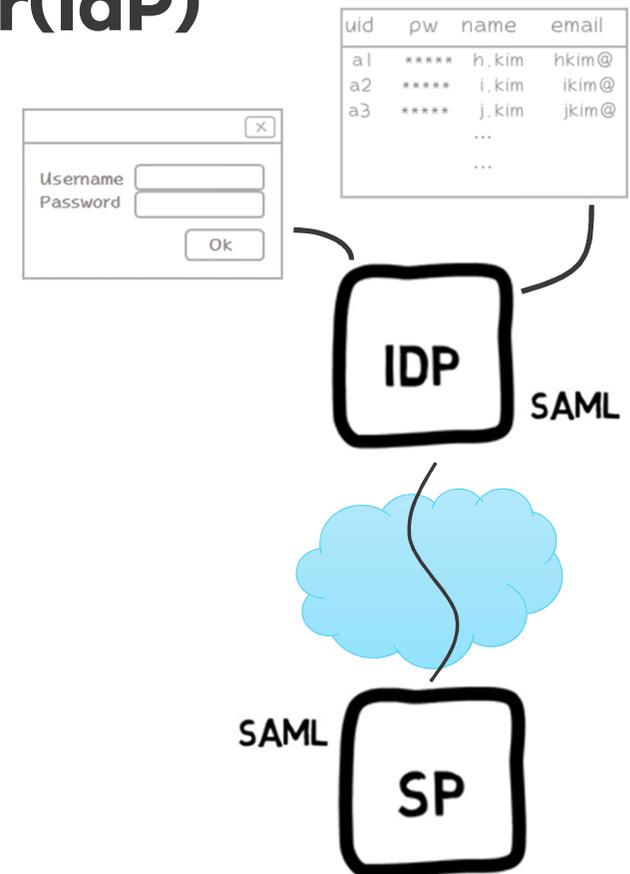
¶ 사용자 인가(권한부여)

¶ SAML 메시지 처리(서명검증 등)

특징

¶ IdP와 SP가 분리되어 있음

¶ 일반적으로 HTTP를 전송규약으로 이용



SAML 통합인증 절차

- ① 메타데이터 교환
- ② 인증요청(로그인요청)
- ③ 인증응답

SAML Web Browser SSO With Static Metadata

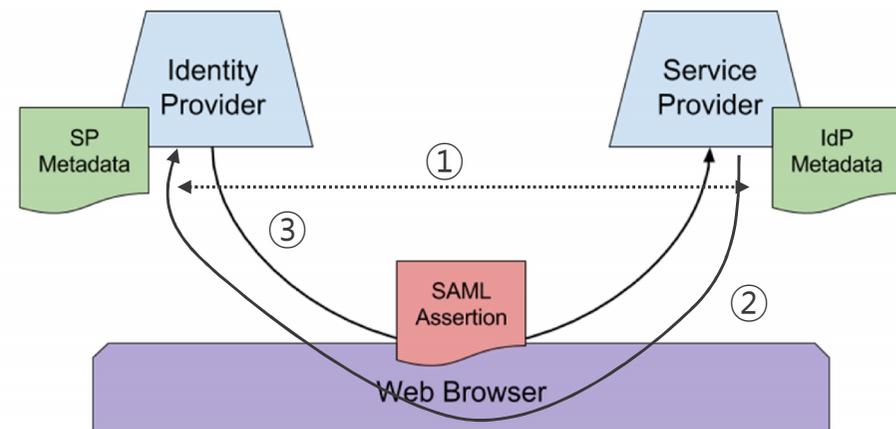


Image Source: https://en.wikipedia.org/wiki/SAML_metadata

SAML Metadata

아이디제공자/서비스제공자의 시스템 정보를 저장한 XML 파일

내용

¶ 개체식별자(EntityID)

¶ 기관도메인(Scope)

¶ 암호키(서명/암호화)

¶ 서비스 주소

* Protocol endpoints

¶ 부가정보

```

<?xml version="1.0"?>
<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://coreen-idp.kreonet.net/idp/simplesamlphp" ID="pfx7e712720-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="#pfx7e712720-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>MIIDuTCCAqGgAwIBAgIJAOCu0jK2GcAMA0GCSqGS1b3DQEBCwUAMHkxCzAJBgNVBAYTaktSMRwDgYDVQQLHAdEYVWVqZW9uMQ4wDAYDVQQKDAVLSVNUST
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
  <shibmd:Scope xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" regexep="false">coreen.or.kr</shibmd:Scope>
  </md:Extensions>
  <md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
  <ds:X509Certificate>MIIDuTCCAqGgAwIBAgIJAOCu0jK2GcAMA0GCSqGS1b3DQEBCwUAMHkxCzAJBgNVBAYTaktSMRwDgYDVQQLHAdEYVWVqZW9uMQ4wDAYDVQQKDAVLSVNUSTEEMB0GA1UEAwWY
  </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>MIIDuTCCAqGgAwIBAgIJAOCu0jK2GcAMA0GCSqGS1b3DQEBCwUAMHkxCzAJBgNVBAYTaktSMRwDgYDVQQLHAdEYVWVqZW9uMQ4wDAYDVQQKDAVLSVNUSTEEMB0GA1UEAwWY
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SingleLogout
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SingleLogoutServ
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://coreen-idp.kreonet.net/simplesaml/saml2/idp/SSOService.p
  <md:SingleSignOnService Binding="urn:oasis:names:tc: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:OrganizationDisplayName xml:lang="en">KREONET</md:OrganizationDisplayName>
  <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>
  
```

SAML Request

서비스제공자가 전송하는 인증요청 메시지

메시지 내용

¶ SSO 서비스 주소

¶ ACS 서비스 주소

* Assertion Consumer Service

¶ 서비스제공자 식별자

¶ 서명

¶ 인증방법(ID/PW, OTP 등)

등등

```
<saml:AuthnRequest
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_bc6335d0970e40d7d40c161ca9e1adcfcd2d47c3d4"
  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-acs.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>
  <saml:NameIDPolicy
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
    AllowCreate="true"/>
  <saml:Scoping>
    <saml:RequesterID>https://webinar.kafe.or.kr/sp/python</saml:RequesterID>
  </saml:Scoping>
</saml:AuthnRequest>
```

SAML Response with Assertion

인증요청에 대한 응답으로 아이디제공자가 전송

메시지 내용

¶ 발행자(Issuer)

¶ 서명(Signature)

- * digest(간추림)를 개인키로 암호화

¶ X.509 인증서

- * 서명검증 및 복호화

¶ 인증정보

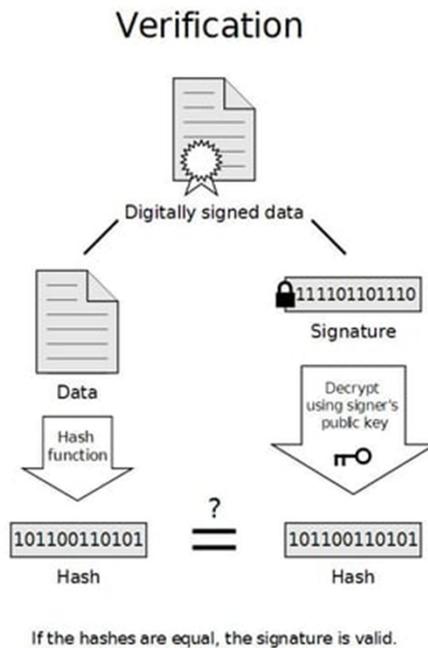
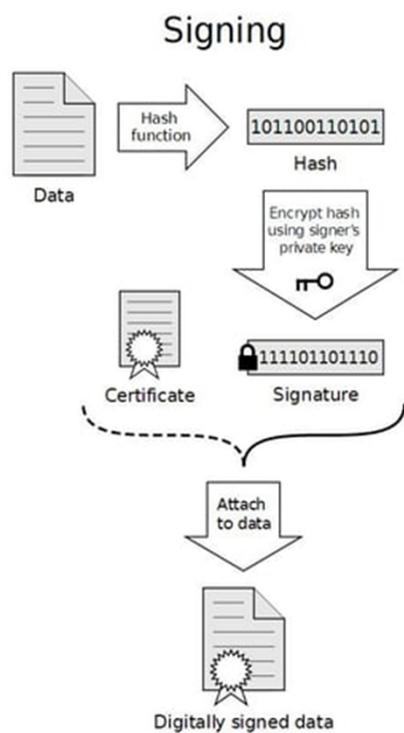
- * 누가, 언제, 어떤 서비스제공자를 위해
어떤 인증방식(예, 비밀번호)으로 로그인했고
- * 메시지가 언제까지 유효한지를 기록

¶ 속성값

<참고> SAML에서 서명과 검증은 **매우** 중요한 보안요소입니다.

```
<saml:ArtifactResponse xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2d9926a42ce0f17629c6af30a6dd8a15fa7409415" InResponseTo="RkN2YnEM"
  Version="2.0" IssueInstant="2007-01-02T20:48:36Z">
  <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="2007-01-02T20:48:36Z">
    <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="s25d1bbb23ed13c6da325a627637c6d5d9e7f13a9" IssueInstant="2007-01-02T20:48:36Z">
      <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">
          amv90ywHqzEW2rmaRViMpWX4qyDA
        </saml:NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml:SubjectConfirmationData NotOnOrAfter="2007-01-02T20:58:36Z" InResponseTo="NKRDzVK7e"
            Recipient="http://cgi.cohos.de:80/cgi-bin/zxid" ></saml:SubjectConfirmationData>
        </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2007-01-02T20:48:36Z" NotOnOrAfter="2007-01-02T20:58:36Z">
        <saml:AudienceRestriction>
          <saml:Audience>
            http://cgi.cohos.de:80/cgi-bin/zxid?c=B
          </saml:Audience>
        </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2007-01-02T20:48:36Z" SessionIndex="s24bfc21323ee9c117bf5769a074be1ff177262701">
        <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>
```

Digital Signature



```

<saml:Assertion
  xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns: xs="http://www.w3.org/2001/XMLSchema"
  ID="_4ee1121c24771a9cf31ef208923f12f5d9e24d8722"
  Version="2.0"
  IssueInstant="2022-11-14T08:17:35Z">
  <saml:Issuer>https://saml.kafe.or.kr/idp/simpleSamlPhp</saml:Issuer>
  <ds:Signature
    xmlns: ds="http://www.w3.org/2000/09/xmldsig#"
    <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" />
      <ds:Reference
        URI="#_4ee1121c24771a9cf31ef208923f12f5d9e24d8722">
        <ds:Transforms>
          <ds:Transform
            Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod
          Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
        <ds:DigestValue>
          whUztIpkU4o9p3k:Jbm3aVWyIx1biAyZLfWzYyJ6vK8=
        </ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>M3Hj+Vzab43p3JWlUuuIH1aVZNI DF1bZn+U32CmbAUAJCCVh4yJnMkwvsz6681GiOrUA+N1L08N24oa1VJnpTsBUBckhRW69UgdCf/VOS
        ZpOAYuR1USWlQw=
      </ds:SignatureValue>
    </ds:Signature>
  </ds:Signature>
  <saml:Subject>
    <saml:NameID
      SPNameQualifier="https://webinar.kafe.or.kr/sp/simpleSamlPhp"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">_9c25d611ebb697df5b96798d37f029a347b7586685
    </saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
  
```

Image Source: <https://www.identityfusion.com/>

Attributes in SAML Assertion

Assertion에 속성(Attributes) 포함

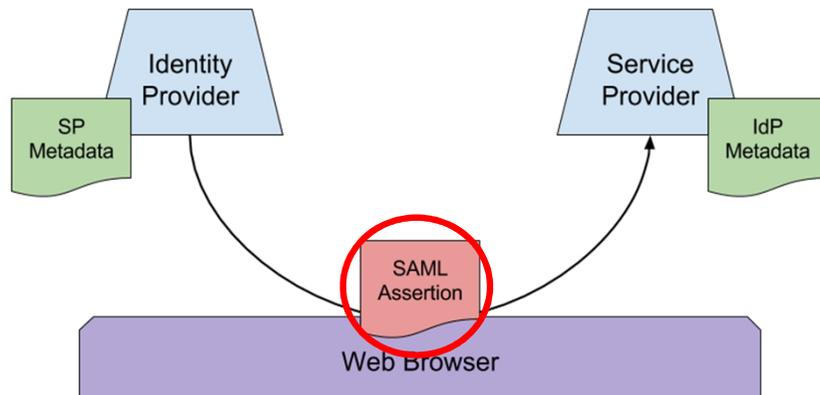
Friendly name/OID 형식 표기

¶ Friendly name

(예): cn/commonName, sn/surName,

¶ OID(Object Identifier)

(예): URN:OID:2.5.4.3



```

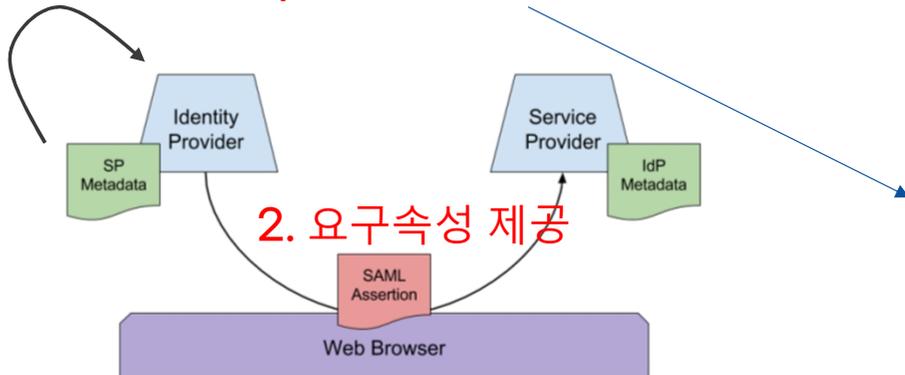
<saml:AttributeStatement>
  <saml:Attribute
    Name="urn:oid:2.16.840.1.113730.3.1.241"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue
      xsi:type="xs:string">Jinyong JO
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute
    Name="urn:oid:0.9.2342.19200300.100.1.3"
    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:1.3.6.1.4.1.5923.1.1.1.1"
    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-ldap.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>
  
```

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

Attributes provided

서비스제공자는 요구속성을 SP 메타데이터에 기록

1. 개체식별자(entityID) 및 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:n
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:a
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:mdui="urn:oasis:names:tc:SAML:met
xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:
xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" xmlns:init=
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xi="http://www.w3.org/2001/
entityID="https://snu.bookcube.biz/sp/shibboleth">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://kafe.kreonet.net" registrationI
  </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
  <md:RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" Name
  <md:RequestedAttribute FriendlyName="eduPersonAffiliation" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" Name
  <md:RequestedAttribute FriendlyName="email" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:o
  <md:RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat="
</md:AttributeConsumingService>
```

SAML SP Metadata

Attributes 활용

응용서비스가 사용자 권한부여에 사용

예시

¶ kisti.re.kr에 소속된 학생만 서비스 이용을 허용하라!

<참고>

urn:oid:1.3.6.1.4.1.5923.1.1.1.9 == eduPersonScopedAffiliation

```
<saml:Attribute
  Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
  <saml:AttributeValue
    xsi:type="xs:string">student@kisti.re.kr
  </saml:AttributeValue>
</saml:Attribute>
```

SAML Assertion 일부

서비스제공자 != 응용서비스

실습 #1

SP 메타데이터의 내용 확인

↓ 다운로드 받은 파일을 notepad++로 읽어오기

<https://testssp.kreonet.net/simplesaml/module.php/saml/sp/metadata.php/default-sp>

URL은 edu.kafe.or.kr를 참조

실습 #2

Chrome Plugin으로 SAML 메시지 내용 확인하기 ¶ AuthnRequest/AuthnResponse 메시지

① [검증용 아이디제공자] <https://testidp.kreonet.net>로 이동

② 사용자 등록 메뉴에서 계정 생성

* 개인정보는 입력하지 마세요! 계정은 24시간 이후에 자동삭제 됩니다.



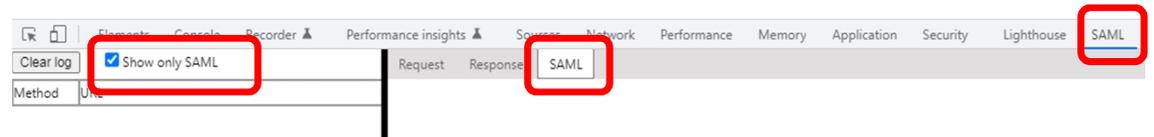
③ [검증용 서비스제공자] <https://testssp.kreonet.net>으로 이동

④ 로그인 검증 메뉴로 이동



⑤ Chrome 브라우저에서 F12 키 입력

* 우측 그림 참조



URL은 edu.kafe.or.kr를 참조

실습 #2 (계속)

⑥ [검증용 서비스제공자] 로그인버튼 클릭

⑦ KAFE test-idp를 선택

⑧ SAML Request 메시지 확인

⑨ 검증용 아이디제공자에서 만든 사용자 계정으로 로그인

⑩ SAML Response 메시지 확인

The screenshot shows a two-step login process. The first step, titled "Select an AuthnContextRef type", features a dropdown menu with the selected value "urn:oasis:names:tc:SAML:2.0:ac:classes:Password" and a blue "LOGIN" button. The second step features a dropdown menu with the selected value "KAFE Test-IdP", a blue "Select" button, and a checkbox labeled "Remember my choice" which is currently unchecked.

URL은 edu.kafe.or.kr를 참조

[참고] Identity federation



Identity federation(신원연합)

동일한 정책프레임워크 공유
협약에 의한 참여
연합운영자에 의해 관리

※ 우리나라의 신원연합은 KAFE
(Korean Access Federation),
국가과학기술연구망에서 운영

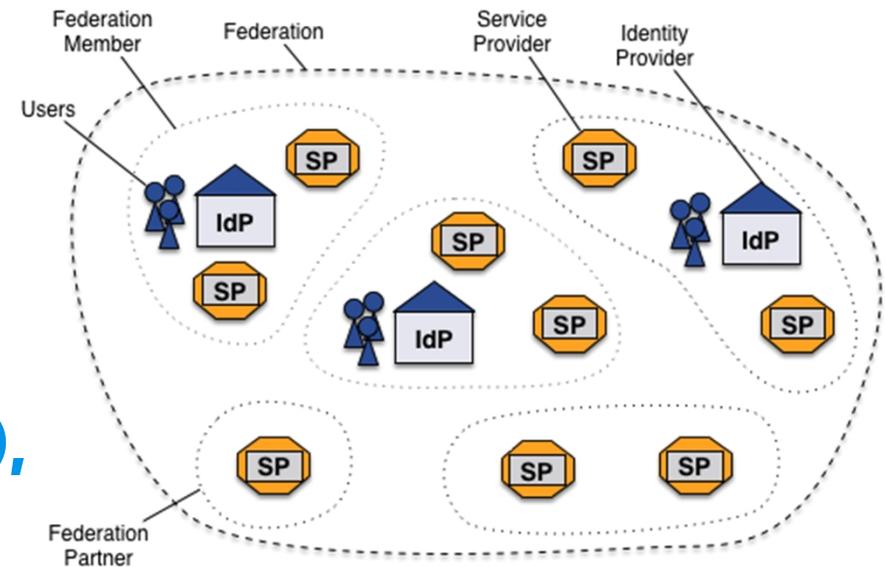


Image Source: Geant

Federation operation

정책프레임워크 제공
메타데이터 관리
공통도구 제공
메시지중계(Optional)

※ 메시지중계가 아닐 경우,
아이디제공자와 서비스제공자가
브라우저를 통해 직접 SAML
메시지를 교환

SAML Web Browser SSO With Automated Metadata Exchange

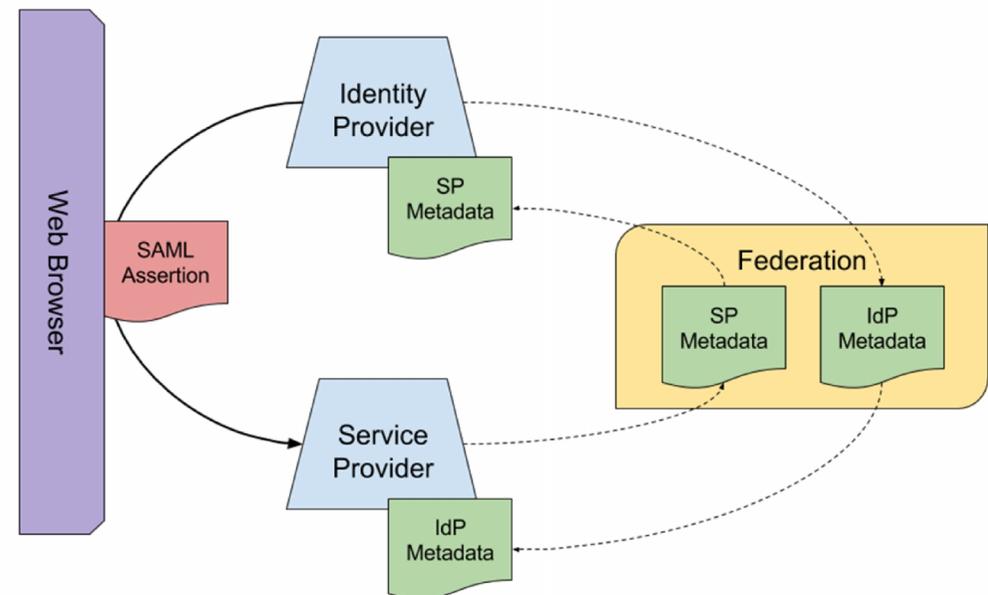


Image Source: https://en.wikipedia.org/wiki/SAML_metadata

Part II . 아이디어제공자의 구축



공개소스 SAML 소프트웨어

분류	Shibboleth	simpleSAMLphp
인증 플로우	비밀번호, X.509, SPNEGO/Kerberos, IP Address, etc	비밀번호(SQL/LDAP/Radius), X.509, Social media
표준지원	SAML 1.1/2.0, X.509, Kerberos, LDAP, SQL	SAML 1.1/2.0, OpenID, Oauth 2.0, Kerberos, VOOT, SQL, LDAP, RADIUS
구현 언어	Java(Spring) for IdP, Apache daemon for SP	PHP for IdP and SP
고가용성(HA) 지원	Yes	Yes (다수의 memcached를 통해 가능)
License	GNU GPL v2.0	GNU LGPL v2.1
지원	Shibboleth 컨소시엄	사용자 커뮤니티

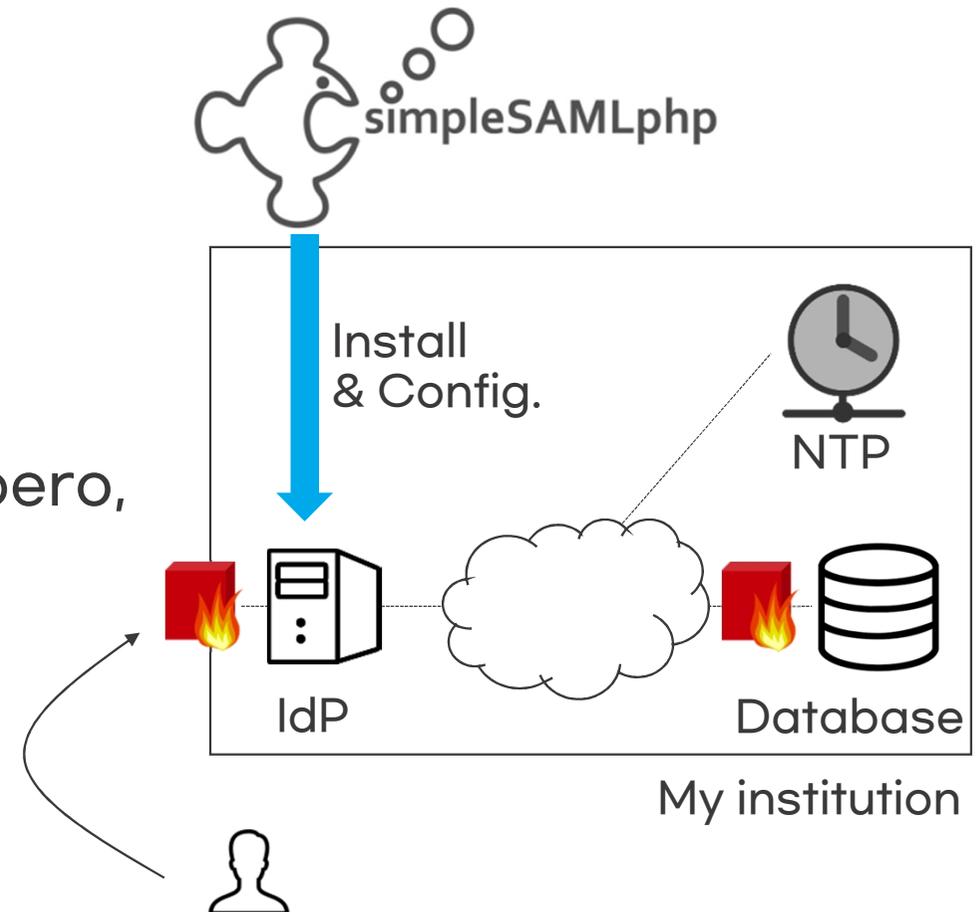
아이디제공자의 구축

1 아이디제공자(IdP)

- * KAFE installer 이용
- * NTP 시간동기화 및 TLS 통신 필수
- * Apache 웹 서버에서 동작

2 데이터베이스

- * MySQL, Oracle, LDAP, AD, Tiberio, MSSQL, RESTful API, 등등



Why NTP?

¶ SAML response message

```

<saml:Conditions
  NotBefore="2022-11-21T02:14:44Z"
  NotOnOrAfter="2022-11-21T02:20:14Z">
  <saml:AudienceRestriction>
    <saml:Audience>...</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement
  AuthnInstant="2022-11-21T02:02:26Z"
  SessionNotOnOrAfter="2022-11-21T10:15:14Z"
  SessionIndex="_f70c5e79d90cb0bbc119920844a38311940f280580">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>

```

¶ SAML Metadata

```

<md:EntitiesDescriptor ID="kafe-20221128022233" Name="urn:mace:kisti.re.kr:kafe:testfed" validUntil="2022-11-28T02:22:33Z"
  <md:Extensions>
    <mdrpi:PublicationInfo creationInstant="2022-11-21T02:22:33Z" publisher="http://kafe.kreonet.net"/>
  </md:Extensions>
  <!--
https://proxy.kreonet.net/sp/simplesamlphp
-->
  <md:EntityDescriptor entityID="https://proxy.kreonet.net/sp/simplesamlphp">
    <md:Extensions>
      <mdrpi:RegistrationInfo registrationAuthority="http://kafe.kreonet.net" registrationInstant="2015-11-10T08:32:00Z"/>
    </md:Extensions>

```

데이터베이스 연동

① 아이디제공자 서버에 데이터베이스(예, Oracle) 라이브러리 설치

- I. <http://www.oracle.com>에서 Oracle instant client 다운로드: oracle instantclient basic, oracle instant client devel
- II. Instant client 설치 rpm -ivh xxxx.rpm
- III. <http://pecl.php.net/package/oci8> 에서 oci8 다운로드
※ oci8 버전은 php 버전에 의존성 있으므로 php 버전에 맞는 oci8버전을 다운로드
- IV. oci8 설치

```
$ tar xvzf oci8-1.4.9.tgz
$ cd oci8-1.4.9
$ phpize
$ ./configure --with-oci8=shared,instantclient,/usr/lib/oracle/11.2/client64/lib
$ ln -s /usr/include/oracle/11.2/client64/ /usr/lib/oracle/11.2/client64/lib/include
$ make all install
```

- V. php 연동: echo 'extension=oci8.so' > /etc/php.d/oci8.ini; service httpd restart

데이터베이스 연동(계속)

② 검증용 PHP 코드 작성

```
<?php
$user_id = "USER_ID";
$user_pw = "USER_PW";
$tns =
"(DESCRIPTION=(ADDRESS_LIST=(LOAD_BALANCE=ON)(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.10.10)(PORT=5055))(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.10.11)(PORT=5505)))(CONNECT_DATA=(SERVICE_NAME=HELLO_WORLD)))";
$conn = oci_connect("DB_ID", "DB_PW", $tns, 'AL32UTF8 ');
if(!$conn){
    $e = oci_error();
    var_dump($e);
} else echo "success";

$query = "SELECT NAME, EMAIL, AFFLI FROM TABLE(ORACLE_FUNC('$user_id', '$user_pw' ))";
$stmt = oci_parse($conn, $query);
oci_execute($stmt);
if(!$row = oci_fetch_assoc($stmt)){
    $e = oci_error();
    var_dump($e);
}
var_dump($row);
oci_free_statement($stmt);
oci_close($conn);
?>
```

데이터베이스 연동(계속)

③ simpleSAMLphp 소스코드 수정

* /var에 simplesamlphp가 설치된 경우

```
[root@localhost ~]# nano /var/simplesamlphp/modules/kafe/lib/Auth/Source/CoreAuth.php
```

* protected function login(\$username, \$password) 함수 수정

☞ 아래 그림의 예시 임

```
protected function login($username, $password) {
    $db = new PDO($this->dsn, $this->username, $this->password);
    $db->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $db->exec("SET NAMES 'utf8'");

    $st = $db->prepare("SELECT username, password, name, email, affi from ex_users where username = '$username'");
    if(!$st->execute()){
        throw new Exception('Failed to Query database for the user');
    }
}
```

데이터베이스 연결부

데이터베이스 질의부

데이터베이스 연동(계속)

② simpleSAMLphp 소스코드 수정(contd.)

* 질의(Query) 결과를 SAML attributes로 변환

```
$attributes = array(
    'uid' => array($username),
    'displayName' => array($row['name']),
    'cn' => array($row['name']),
    'sn' => $sn,
    'givenName' => $givenname,
    'mail' => array($row['email']),
    'eduPersonAffiliation' => $this->eAffiliation,
    'eduPersonPrincipalName' => $eppName,
    'eduPersonScopedAffiliation' => $epsAffiliation,
    'organizationName' => array('YOUR ORG FULL NAME'),
    'schacHomeOrganization' => array('yourorg.ac.kr'),
    // for future use
    'eduPersonEntitlement' => array('urn:mace:dir:entitlement:common-lib-terms'),
);
```

* 이용 가능한 속성명 확인

```
[root@localhost ~]# nano /var/simplesamlphp/attributemap/name2oid.php
```

```
$attributemap = [
    'aRecord' => 'urn:oid:0.9.2342.19200300.100.1.26',
    'aliasedEntryName' => 'urn:oid:2.5.4.1',
    'aliasedObjectName' => 'urn:oid:2.5.4.1',
    'associatedDomain' => 'urn:oid:0.9.2342.19200300.100.1.37',
    'associatedName' => 'urn:oid:0.9.2342.19200300.100.1.38',
    'audio' => 'urn:oid:0.9.2342.19200300.100.1.55',
    'authorityRevocationList' => 'urn:oid:2.5.4.38',
```

[참고] 국제 신원연합 참여기관 숙지사항



국외 응용서비스 이용

1 국제 신원연합 eduGAIN을 통해 연합 메타데이터 교환

- * 개인정보처리방침을 제공하는 아이디제공자와 서비스제공자만 수용
- * 여과된 eduGAIN 메타데이터 배포 주소(서비스제공자 확인 가능)

<https://fedinfo.kreonet.net/signedmetadata/federation/KAFE-eduGAIN/eduGAIN-SP.xml>

Federations in eduGAIN ?		Entities in eduGAIN ?	
Participants	80	All entities	8801
Voting-only Members	1	IdPs	5185
Candidates	5	SPs	3631
		Standalone AAs	2

1 이용 조건

- * eduGAIN 가입(KAFE 가입 시 선택)
- * 아이디제공자의 경우, SIRTFI(보안사고 대응프레임워크) 및 Research & scholarship category(개인정보최소사용) 준수

```

<mdattr:EntityAttributes>
  <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>

```

SIRTFI 중 TLP 규정

¶ TLP(Traffic Light Protocol)

- * 민감정보의 공유범위를 지정
- * 참조: <https://www.cisa.gov/tlp>

181.1.253.234, IPV4ADDR, ,IP_WATCHLIST, C2, 12/28/2017 00:10:25Z, TLP:WHITE, According to DHS and FBI analysis, this IP address is compromised infrastructure. This IP is geolocated in Argentina.

 <p>TLP: RED</p> <p>Not For Disclosure</p> <p>This information cannot be disseminated to third parties unless the sender permits it</p> <p>Only participating groups can have access to it.</p>	 <p>TLP: AMBER</p> <p>Limited Disclosure</p> <p>This information can be shared with participants of an organization or some members of a community</p> <p>Additional restrictions can be made.</p>
 <p>TLP: GREEN</p> <p>Community-Wide Disclosure</p> <p>This information can be shared with everyone in a particular community</p> <p>However, it cannot be published publicly on the Internet.</p>	 <p>TLP: WHITE</p> <p>Unlimited Disclosure</p> <p>This information can be shared publicly with everyone</p> <p>However, the laws of Copyright still need to be applied</p>

Image Source: <https://cyberhoot.com/cybrary/traffic-light-protocol/>

Part III. 관리운영



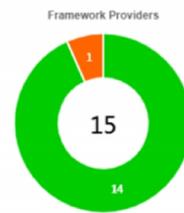
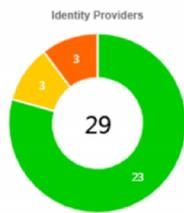
회원기관 모니터링 시스템

📌 <https://www.kafe.or.kr/status> (edu.kafe.or.kr 참조)

KAFE Entity Monitoring Dashboard Meta Service

- Metadata validUntil (7)
- SP - mds: 6 Days 9 hours left
- edugain up IdP: 6 Days 9 hours left
- KAFE Test federation: 6 Days 9 hours left
- KAFE Production fed: 6 Days 9 hours left
- eduGAIN Down: 4 Days 3 h

메타데이터 모니터링



SSL 인증서 교체필요

Report all entities (66)

NAME	HTTP STATUS	SSL STATUS	META STATUS	TIME STATUS	SINCE	ACT
Daegu Gyeongbuk Institute of Science and Technology	Fault	Insecure	Valid	Fault	2022-11-16 18:03:03	🔍
EDISON - Computational Science Platform	Fault	Secure	Careful	Fault	2022-11-21 00:02:45	🔍
KAFE OIDC Broker	Fault	Secure	Valid	Sync	2022-11-21 06:02:13	🔍
KOREA RESEARCH INSTITUTE OF SHIPS & OCEAN ENGINEERING	Fault	Insecure	Valid	Fault	2022-11-20 12:02:20	🔍
Institute for Basic Science	Fault	Secure	Valid	Sync	2022-11-21 11:52:06	🔍
Pusan National University	Available	Warning	Valid	Sync	2022-11-21 06:02:30	🔍

서버 다운

HW/SW 방화벽

메타데이터 수정필요

아이디제공자의 정상동작 여부 확인

¶ 웹 브라우저에서 아이디제공자의 도메인에 직접 접근 시

* 정상동작 여부를 확인할 수 없음(예, iam.knou.ac.kr)

Notice

- 본 서버는 KAFE 연합인증 서비스의 제공을 목적으로 한국방송통신대학교에서 운영합니다.
- 지금 보고계신 페이지는 어떤 서비스도 제공하지 않습니다. 본 서버가 제공하는 기능은 서비스제공자에 로그인하는 과정에서만 확인하실 수 있습니다.

서버 운영상태나 로그인과정과 관련된 문의는 기관자산담당부서로 하십시오. 연합인증 서비스는 support@kafe.or.kr로 문의하시기 바랍니다.

¶ 서비스제공자를 통해 로그인 가능 여부를 확인해야 함

* 예) www.kafe.or.kr에 접속 → 소속기관 선택 → ID/PW 입력 → 사용자 동의 → www.kafe.or.kr에 로그인 된 상태로 이동

서비스 데몬 확인

¶ Apache

\$ systemctl status httpd

* active 상태가 아니면,
\$ systemctl restart httpd

¶ NTP

\$ systemctl status ntpd

* active 상태가 아니면,
\$ systemctl restart ntpd

```
[root@localhost ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-06-02 10:19:41 KST; 5 months 14 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Process: 23124 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Main PID: 23166 (httpd)
   Status: "Total requests: 43891; Current requests/sec: 0; Current traffic:  0 B/sec"
   CGroup: /system.slice/httpd.service
           └─14225 /usr/sbin/httpd -DFOREGROUND
             └─14586 /usr/sbin/httpd -DFOREGROUND
               └─17378 /usr/sbin/httpd -DFOREGROUND
                 └─17521 /usr/sbin/httpd -DFOREGROUND
                   └─23166 /usr/sbin/httpd -DFOREGROUND
                     └─30803 /usr/sbin/httpd -DFOREGROUND
                       └─31280 /usr/sbin/httpd -DFOREGROUND
                         └─31333 /usr/sbin/httpd -DFOREGROUND
                           └─31465 /usr/sbin/httpd -DFOREGROUND
                             └─31623 /usr/sbin/httpd -DFOREGROUND
                               └─31632 /usr/sbin/httpd -DFOREGROUND
```

```
[root@localhost ~]# systemctl status ntpd
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-05-11 17:21:12 KST; 6 months 5 days ago
     Main PID: 12087 (ntpd)
   CGroup: /system.slice/ntpd.service
           └─12087 /usr/sbin/ntpd -u ntp:ntp -g
```

방화벽 및 데이터베이스 확인

¶ SW/HW 방화벽 확인(80/443 포트개방 확인)

- * HTTP(80)/HTTPS(443) 개방 여부
- * 데이터베이스 서버포트 개방 여부

¶ 데이터베이스 연결여부 확인

- * 아이디제공자 서버에서 데이터베이스 접속 가능 여부 확인

```
# telnet <ip> <port>  
$ telnet 127.0.0.1 10002
```

```
# echo > /dev/tcp/<ip>/<port>, 포트가 열려있으면 반환메시지가 없음(echo $?는 0)  
$ echo > /dve/tcp/127.0.0.1/22  
$ echo $?
```

자주 발생하는 오류 I

¶ Metadata not found

* 원인

1. 이용 불가능한 서비스제공자
2. 연합 메타데이터의 새로 고침이 안됨

SimpleSAMLphp Error Report

Message from user:

Explain what you did when this error occurred...

Exception: SimpleSAML_Error_MetadataNotFound: METADATANOTFOUND('%ENTITYID%' => 'Wt')

Backtrace:

```
3 /var/simplesamlphp/lib/SimpleSAML/Metadata/MetaDataStorageHandler.php:301 (SimpleSAML_Metadata_MetaDataStorageHandler->getMetadataEntry)
2 /var/simplesamlphp/lib/SimpleSAML/Metadata/MetaDataStorageHandler.php:318 (SimpleSAML_Metadata_MetaDataStorageHandler->getMetadataEntry)
1 /var/simplesamlphp/modules/saml/lib/IdP/SAML2.php:303 (sspmod_saml_IdP_SAML2::receiveAuthnRequest)
0 /var/simplesamlphp/www/saml2/IdP/SSOService.php:18 (N/A)
```

URL:

SimpleSAMLphp Error Report

Message from user:

Explain what you did when this error occurred...

Exception: SimpleSAML_Error_Error: UNHANDLED EXCEPTION

Backtrace:

```
1 www/_include.php:45 (SimpleSAML_exception_handler)
0 [builtin] (N/A)
```

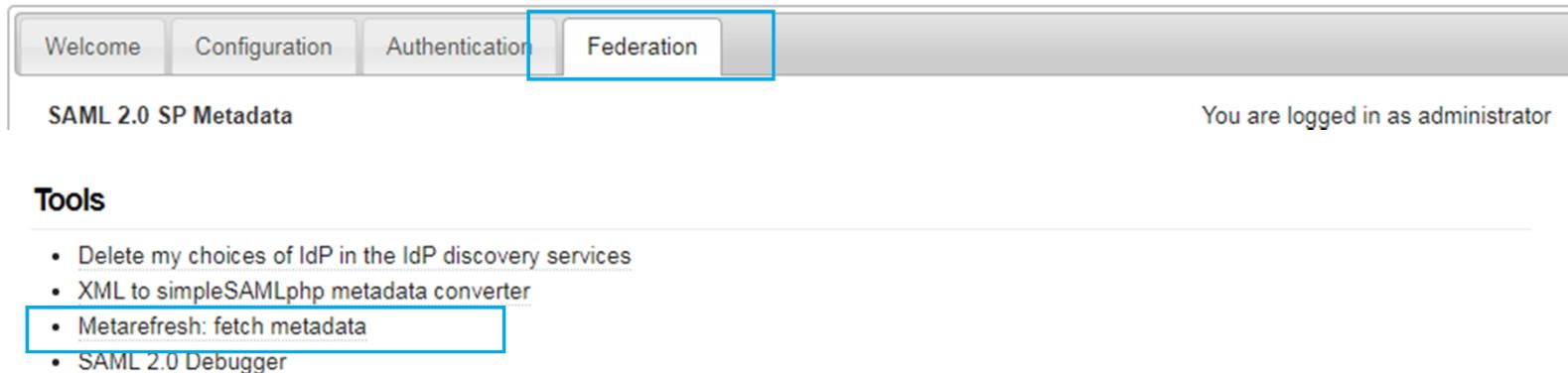
Caused by: SimpleSAML_Error_Exception: Could not find the metadata of an IdP with entity ID 'ht'

Backtrace:

오류 1-2의 해결

1 연합 메타데이터의 새로 고침이 안됨

- * 웹 브라우저에서 <https://도메인이름/simplesaml>로 접근
- * Federation 탭의 Metafresh를 클릭



자주 발생하는 오류 II

¶ Clock synchronization

* NTP 시간 동기화 실패로 발생(clock skew < 60s 이어야 함)

* 원인

1. NTP 데몬 정지: NTP 데몬 재실행
2. 연합 메타데이터의 새로 고침이 안됨(오류 1-2 해결방법 참조)

```
SimpleSAML_Error_Error: UNHANDLEDEXCEPTION
```

```
Backtrace:
```

```
1 www/_include.php:17 (SimpleSAML_exception_handler)
```

```
0 [builtin] (N/A)
```

```
Caused by: SimpleSAML_Error_Exception: Received an assertion that is valid in the future. Check clock synchronization on IdP and SP.
```

```
Backtrace:
```

```
3 modules/saml/lib/Message.php:660 (sspmod_saml_Message::processAssertion)
```

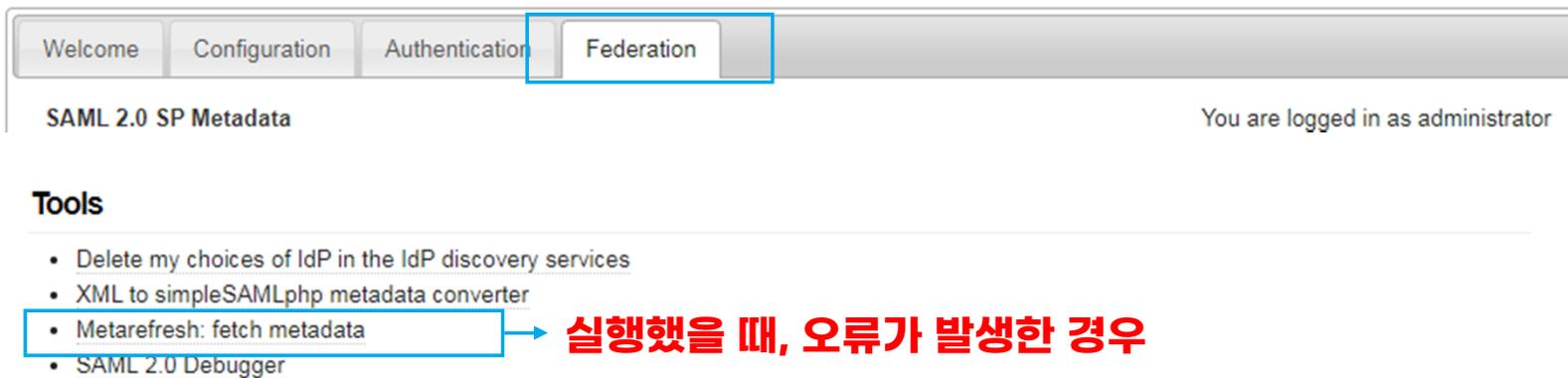
```
2 modules/saml/lib/Message.php:613 (sspmod_saml_Message::processResponse)
```

```
1 modules/saml/www/sp/saml2-acis.php:129 (require)
```

```
0 www/module.php:135 (N/A)
```

자주 발생하는 오류 III

¶ metarefresh failure



Welcome Configuration Authentication **Federation**

SAML 2.0 SP Metadata You are logged in as administrator

Tools

- [Delete my choices of IdP in the IdP discovery services](#)
- [XML to simpleSAMLphp metadata converter](#)
- **Metarefresh: fetch metadata** → 실행했을 때, 오류가 발생한 경우
- [SAML 2.0 Debugger](#)

* php.ini 파일 수정

```
memory_limit=600M  
max_execution_time=120
```

기타 오류 발생 대처

📁 로그파일

* /var/log/messages 및 /var/log/httpd/ssl_error_log

```
[341fcdbfaf] SimpleSAML_Error_Exception: Error 8 - Undefined offset: 0
[341fcdbfaf] Backtrace:
[341fcdbfaf] 10 /var/www/simplesamlphp/www/_include.php:70 (SimpleSAML_error_handler)
[341fcdbfaf] 9 /var/www/simplesamlphp/modules/outsideRnE/lib/Auth/Process/UserAcl.php:203 (sspmod_outsideRnE_Auth_Process_UserAcl::process)
[341fcdbfaf] 8 /var/www/simplesamlphp/lib/SimpleSAML/Auth/ProcessingChain.php:194 (SimpleSAML_Auth_ProcessingChain::processState)
[341fcdbfaf] 7 /var/www/simplesamlphp/lib/SimpleSAML/IdP.php:309 (SimpleSAML_IdP::postAuth)
[341fcdbfaf] 6 [builtin] (call_user_func)
[341fcdbfaf] 5 /var/www/simplesamlphp/lib/SimpleSAML/Auth/Default.php:133 (SimpleSAML_Auth_Default::loginCompleted)
[341fcdbfaf] 4 [builtin] (call_user_func)
[341fcdbfaf] 3 /var/www/simplesamlphp/lib/SimpleSAML/Auth/Source.php:139 (SimpleSAML_Auth_Source::completeAuth)
[341fcdbfaf] 2 /var/www/simplesamlphp/modules/core/lib/Auth/UserPassBase.php:272 (sspmod_core_Auth_UserPassBase::handleLogin)
[341fcdbfaf] 1 /var/www/simplesamlphp/modules/core/www/loginuserpass.php:75 (require)
[341fcdbfaf] 0 /var/www/simplesamlphp/www/module.php:134 (N/A)
```

※ Error 표시가 서비스 중단을 의미하지는 않습니다.

오류파악이 어려울 경우, 로그파일을 support@kafe.or.kr에 전달

Apache 보안설정

¶ httpd.conf

```
<IfModule mod_headers.c>
Header set Content-Security-Policy "default-src https;; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline';"
Header set X-Content-Type-Options nosniff
Header set X-XSS-Protection "1;mode=block"
Header set Cache-Control "no-cache, no-store, must-revalidate"
Header set Pragma "no-cache"
Header set Expires 0
Header always set Referrer-Policy "no-referrer"
Header always set Strict-Transport-Security "max-age=31536000; preload; includeSubDomains"
Header unset X-Forwarded-Host
</IfModule>
```

느슨하게 설정된 보안정책(적합 함)

콘텐츠 보안 정책

- 패킷분석 금지
- XSS 탐지 시, 공격차단 및 웹 페이지 출력 금지
- 기존 캐시 검사 후, 재 검증 및 저장 금지 (HTTP/1.1)
- 상동(HTTP/1.0)
- 캐시 만료시간 0
- 이동정보 추적 금지
- HTTPS 접속 강제
- 호스트 헤더 조작 금지

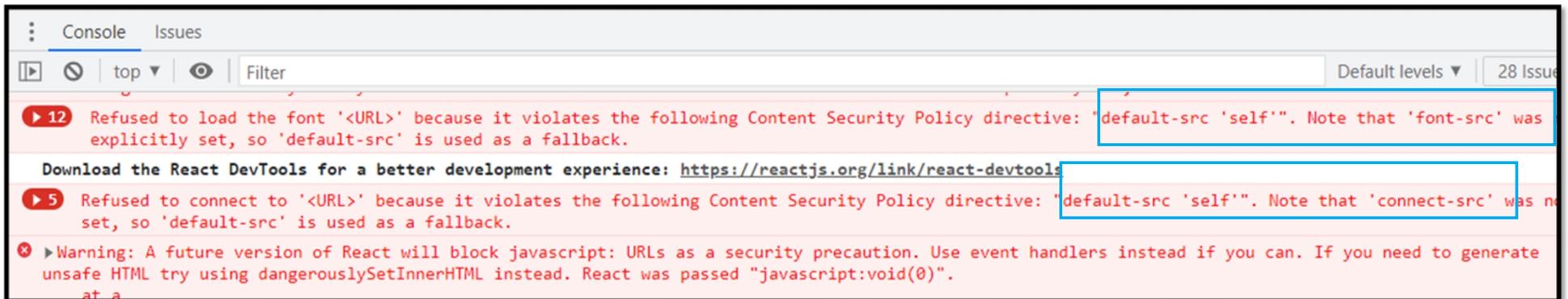
¶ ssl.conf

SSLProtocol +TLSv1.1 +TLSv1.2

Apache 보안설정 검증

¶ Chrome browser, F12 개발자모드에서 오류 점검 필수

- * 오류 확인 시, httpd.conf의 mod_headers 수정
→ 수정 후 service httpd restart



소프트웨어 방화벽

¶ **iptables와 selinux는 disabled로 기본 설정 됨**

* 필요할 경우, firewalld(CentOS), ufw(Ubuntu),
selinux(CentOS/Ubuntu)를 이용해 방화벽 설정

→ 80/http(tcp), 443/https(tcp), 123/ntp(udp), DB 접속주소와 포트는 양방향 개방

도서관 응용 지원

¶ 전자저널의 경우, 속성정보를 이용해 이용권한을 관리

* Web of Science 예시

등록양식 작성
<ul style="list-style-type: none"> Product: Web of Science Core Collection <참조> Clarivate 사의 타 플랫폼(예, JCR) 등은 플랫폼 종류에 맞게 설정 Institution Name Federation: Korean Access Federation (KAFE) Identity Provider URL (IDP): 아래 내용을 기입 entityID: entityID를 기입(2장 참조) Institution URL: 기관 홈페이지 주소 Assertion statements: 아래 내용을 기입 scope: 2장 참조 attributes: eduPersonScopedAffiliation (student@SCOPE, faculty@SCOPE, staff@SCOPE) <중요> SCOPE은 위 'scope'의 값으로 설정 (예, scope이 kisti.re.kr일 경우, student@kisti.re.kr) How can we help you? Please enable offsite access (Shibboleth access) to [플랫폼 이름]

도서관 응용 지원(계속)

¶ 전자저널의 경우, 속성정보를 이용해 이용권한을 관리

- * entityID
- * SCOPE

- * entitlement (자격정보)

- student
- faculty
- staff
- alum
- affiliate

→ student@SCOPE

(예, student@kaist.ac.kr)

```
<?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:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:mattr="urn:oasis:names:tc:SAML:metadata:attrib" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSC" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init" xmlns:xsi="http://www.w3.org/2001/XMLSchema" xmlns:xi="http://www.w3.org/2001/XInclude" entityID="https://kafe.kaist.ac.kr/idp/simplesamlphp">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="http://kafe.kreonet.net" registrationInstant="2021-02"
    <mdrpi:RegistrationPolicy xml:lang="en">https://www.kafe.or.kr/kafe-mrps-v1.1.1.pdf</mdrpi:Registrati
    </mdrpi:RegistrationInfo>
    <mdattr:EntityAttributes>
      <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:names:tc:SA
      <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:oa
      <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <shibmd:Scope regexp="false">kaist.ac.kr</shibmd:Scope>
    </md:Extensions>
    <mdui:UIInfo>
      <mdui:DisplayName xml:lang="en">Korea Advanced Institute of Science and Technology</mdui:DisplayName>
      <mdui:Description xml:lang="en">Korea Advanced Institute of Science and Technology</mdui:Description>
      <mdui:InformationURL xml:lang="en">https://kafe.kaist.ac.kr</mdui:InformationURL>
      <mdui:PrivacyStatementURL xml:lang="en">https://www.kaist.ac.kr/kr/html/footer/0812.html</mdui:Privac
      <mdui:Logo width="53" height="17">https://kafe.kaist.ac.kr/kaist_small_logo.png</mdui:Logo>
    </mdui:UIInfo>
    <mdui:DiscoHints>
      <mdui:GeolocationHint>geo:36.372300,127.360149</mdui:GeolocationHint>
    </mdui:DiscoHints>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Federation metadata

실습 #3

연합메타데이터의 내용 확인

<https://fedinfo.kreonet.net/signed-metadata/federation/KAFE-profed/metadata.xml>

URL은 edu.kafe.or.kr를 참조

Korean Access Federation

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