통합로그인 기술의 이해와 활용

한국과학기술정보연구원 조진용
jiny92@kisti.re.kr

2025년 6월 19일(목)

Audience

대상

- 통합로그인 시스템을 구축하고자 하는 학연 기관 관계자

수준

- 초급+α
- IT 관련 기초지식 필요

참고

- 강의자료: https://edu.kafe.or.kr
- 자세한 기술 상세는 https://edu.kafe.or.kr/lec-2024-3q.pdf를 참조

Agenda

1차시

¶ 통합 로그인의 개념

2차시

¶ SAML을 이용하는 연합 로그인의 이해

3차시

¶ 연합 로그인과 KAFE의 역할

4차시

¶ SAML IdP 구축

5차시

¶ IdP 운영 및 KAFE 가입

1차시: 통합 로그인의 개념

통합로그인(SSO, Single-Sign On)?

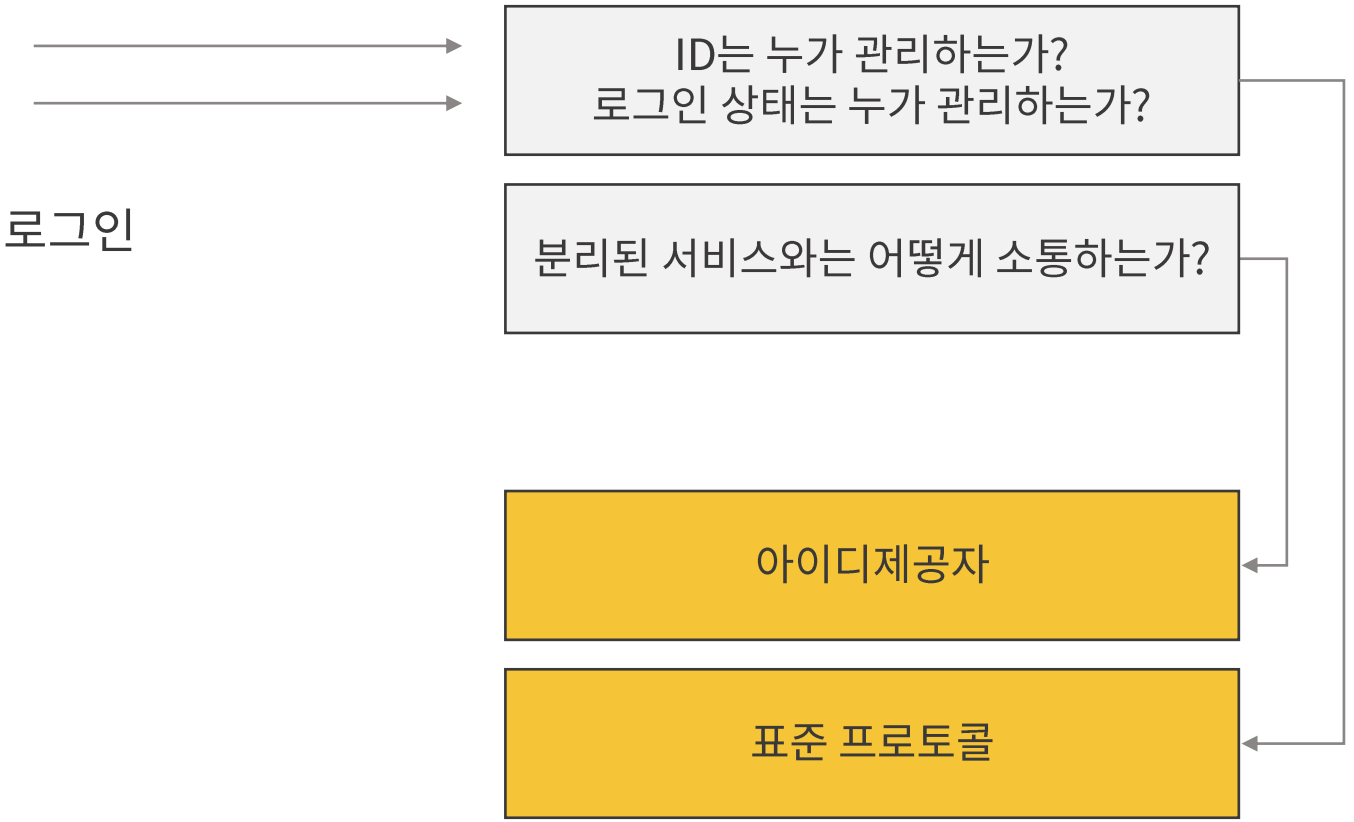
- 정의
  - 하나의 디지털 ID와;
    한번의 로그인으로;
    연동된 모든 온라인 서비스에 로그인

- 예시
  - (오프라인) 대학교 학생증 하나로
    - 도서관 출입
    - 수강신청
    - 기숙사 출입
    - 학식 결재

  - (온라인)
    - 구글 계정으로 로그인
    - 네이버 아이디로 로그인
    - 카카오톡으로 로그인

통합로그인 시스템 구성과 표준 프로토콜

- 정의
  - 하나의 디지털 ID와;
    한번의 로그인으로;
    +
    연동된 모든 온라인 서비스에 로그인



주요 표준 프로토콜

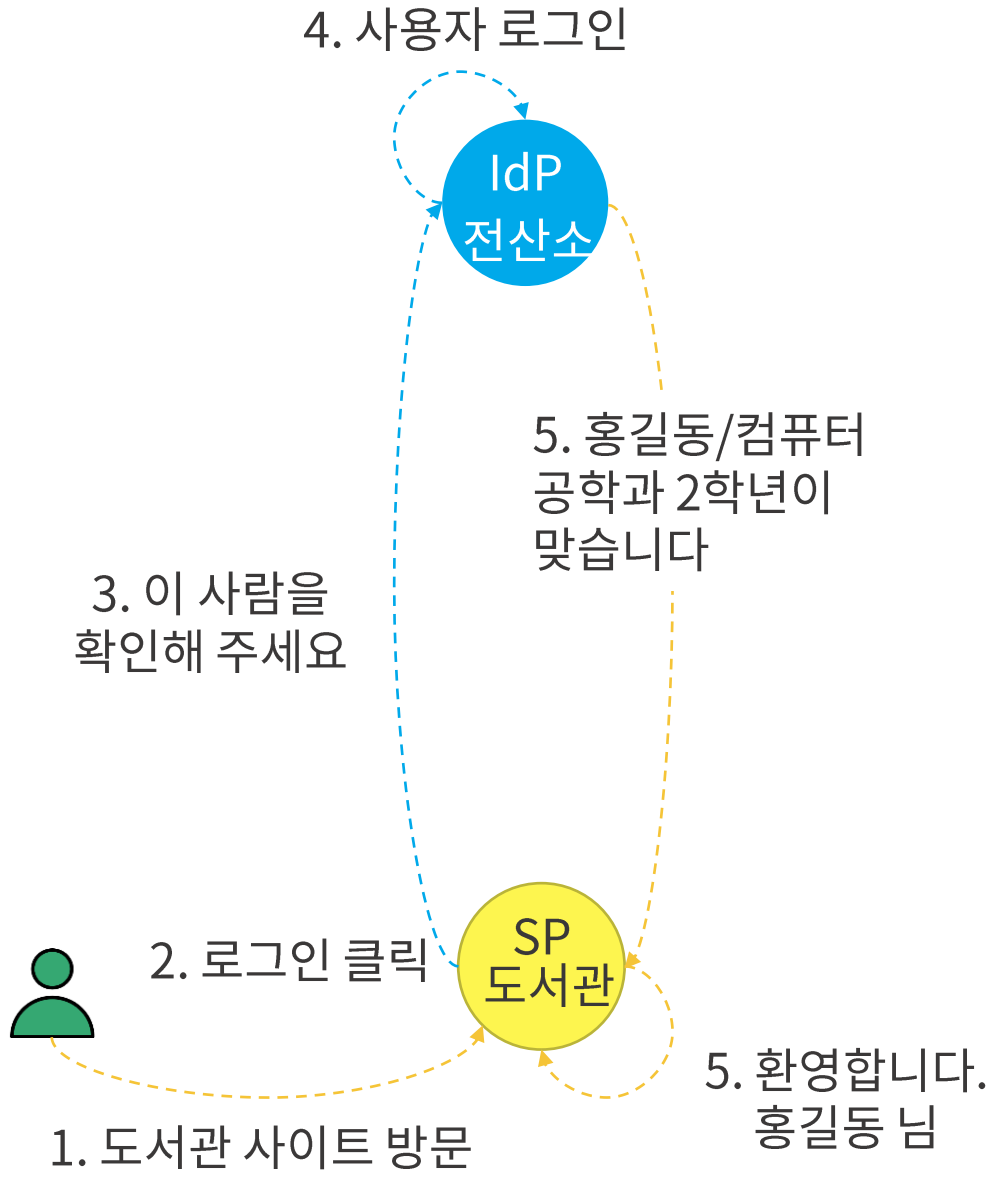
- SAML(Security Assertion Markup Language)
  - 특징: 정부기관, 대학교, 기업에서 주로 활용
  - 장점: 안전, 많은 정보 전달 가능
  - 단점: 설정이 복잡, 모바일에 부적합

- OAuth 2.0/OIDC(OpenID Connect)
  - 특징: SNS, 모바일 앱에서 주로 사용
  - 장점: 간단한 설정, 모바일 친화적
  - 단점: 단순한 정보만 전달
  - 사용 예: 구글 로그인

기관 유형	권장 프로토콜	이유
대학	SAML	학적정보, 소속정보 등 상세한 정보 필요
연구기관	SAML	보안성, 국제 연구 기관 간 호환성
기업	OAuth2/OIDC	빠른 구축 및 모바일 지원
정부기관	SAML	높은 보안요구 사항

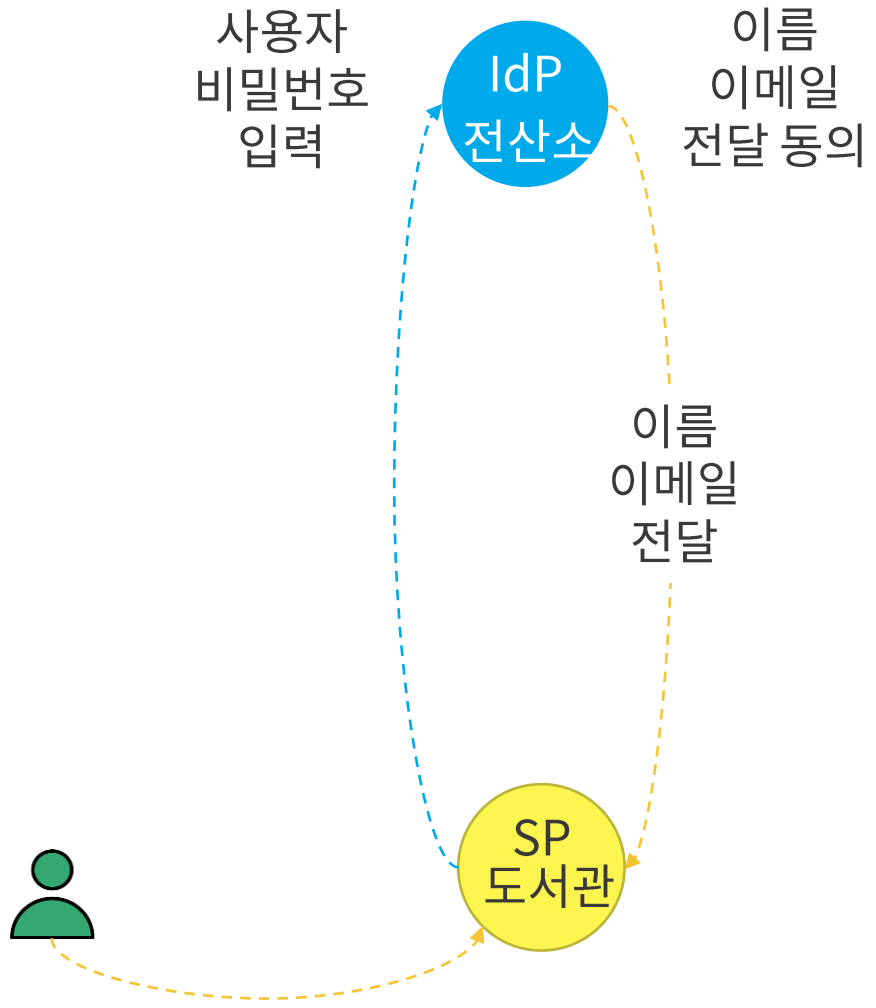
통합 로그인의 3대 요소

- 아이디 제공자(IdP, Identity Provider) = 신분증 발급 기관
  - 사용자 신원을 확인하고 증명서를 발급
  - 사용자 신원 정보와 사용자 상태(로그인 상태 등)를 관리
- 서비스 제공자(SP, Service Provider) = 서비스 제공 업체
  - 신분증을 확인하고 서비스 제공
- 사용자
  - 신분증을 가지고 다니며 서비스를 이용



보안과 개인정보보호

- 비밀번호 보호
  - 각 서비스 제공자마다 다른 비밀번호 불필요
    (비밀번호 도난 위험 감소)
- 사용자 동의
  - 어떤 정보가 전달되는지 사용자에게 명시적으로 알림
- 개인정보 오남용 방지
  - 사용자가 동의한 정보만 전달



기관에서 얻는 이득

- 사용자 편의성
  - 하나의 계정으로 모든 서비스 이용
- 보안 강화
  - 중앙집중식 보안 관리
- 비용 절감
  - 각 서비스별 계정 관리 불필요
- 국제 호환성
  - 해외 서비스(전자저널 등)와 연동 가능

2차시: SAML을 이용하는 연합 로그인의 이해

연합 로그인?

- 정의
  - 서로 다른 기관들이 사용자 인증 정보를 공유
  - 한 번의 로그인으로 여러 기관의 서비스를 이용 가능

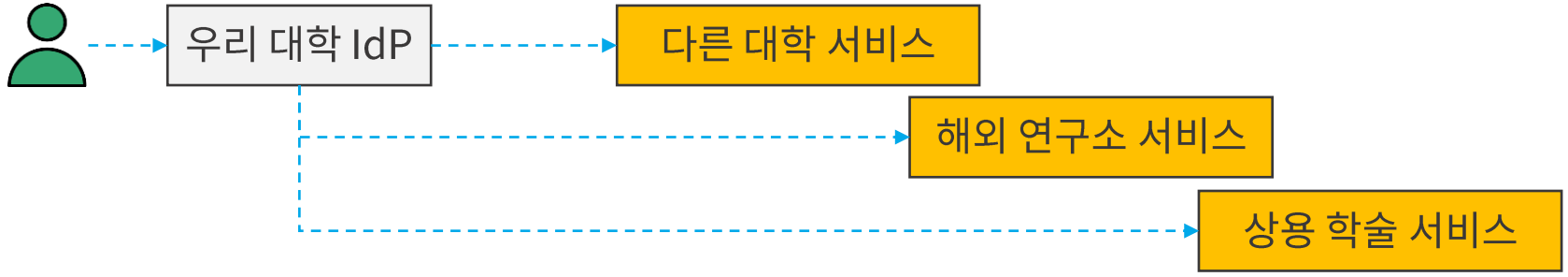
기관 간 연합한 통합 로그인

- 대학교 간 학점 교환 프로그램과 유사한 개념
  - 우리 대학 신분증으로 협정 대학의 도서관도 이용 가능
  - 각 대학과 도서관이 사전에 협정을 맺어 '신뢰'하기 때문에 가능
  - 협정식에 협정서(메타데이터)를 서로 교환해야 함

연합 vs 단일 기관 SSO 비교

- 단일 기관 SSO
  - 한 회사/학교/연구소 내에서만 사용

- 연합 SSO
  - 여러 기관이 협력할 때 사용



연합 로그인의 장점

- 사용자
  - 편의성: 하나의 계정으로 여러 기관 서비스 이용
  - 보안성: 각 서비스마다 계정 생성 불필요
  - 일관성: 동일한 로그인 절차
- 기관
  - (서비스제공자)비용: 개별 서비스 마다 계정 관리 불필요
  - 보안강화: 표준 프로토콜 사용 및 중앙 집중 관리
  - 국제협력: 해외 기관과 서비스 및 자원 공유
  - 사용자 만족도: 편리한 서비스 이용

SAML 연합 로그인의 특징

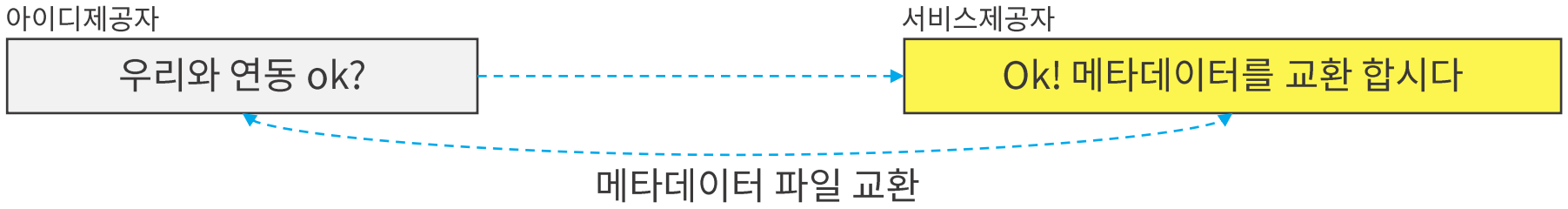
- 왜 SAML을 사용하는가?
  - 다양한 사용자 정보(소속, 학과, 직급, 학번 등)를 전달 가능
  - 디지털 서명으로 정보 위변조 방지(높은 보안 수준)
  - 메타데이터를 통한 자동화된 신뢰 관계 구축
  - 국제 표준(전 세계 대학/연구소들과 호환 가능)
- (동향) SAML에서 OAuth2/OIDC 연합 로그인으로 진화 중
  - 스마트폰 대중화
  - 관리 편의성

메타데이터의 역할

- 메타데이터란? IdP와 SP 간의 연동을 위한 설정 정보
  - ‘명함’과 유사
    - 소유자 정보를 담고 있음 vs 아이디제공자/서비스제공자의 정보를 담고 있음
    - 사람 간 서로 교환 vs 아이디제공자와 서비스제공자가 서로 교환

- 메타데이터에 포함된 정보
  - 기관 이름과 연락처
  - 보안 Key(디지털 서명용)
  - 서비스 주소
  - 필요한 사용자 정보

- 메타데이터의 교환 과정



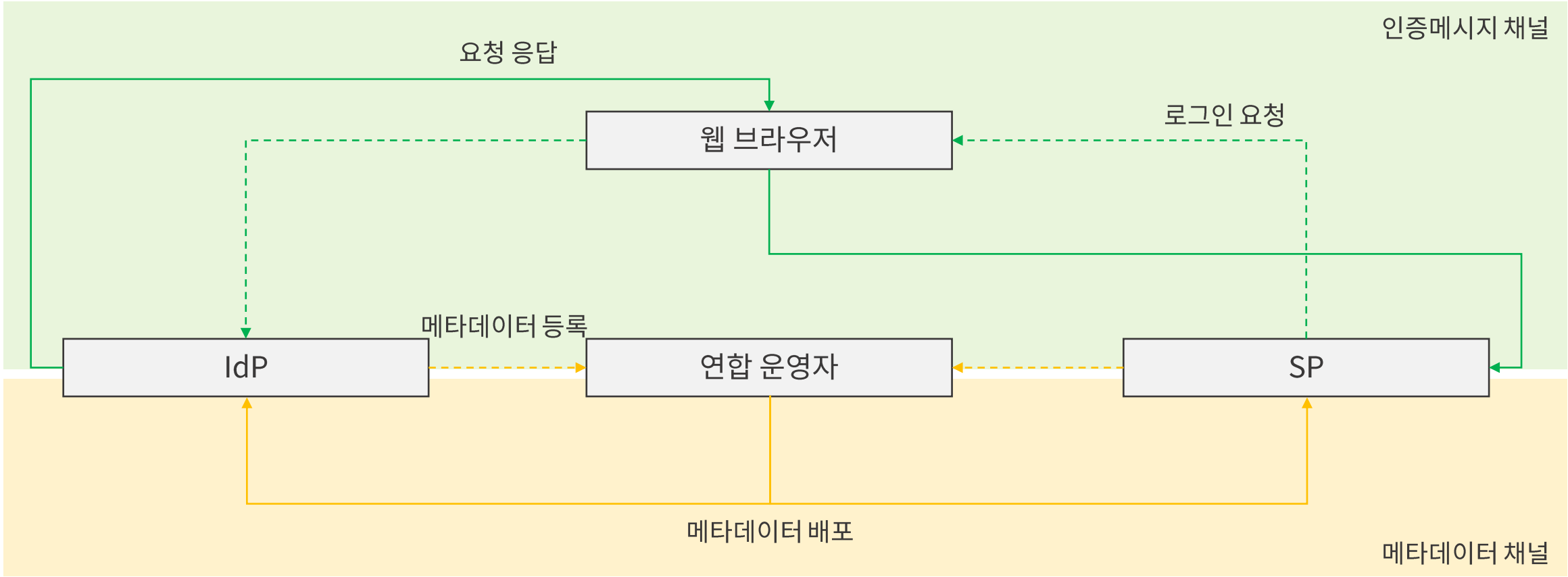
<참고> 메타데이터

- Exchange public keys for encryption and signature
- Exchange endpoint URLs

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

SAML 채널 분리

- 메타데이터 채널 vs 인증메시지 채널

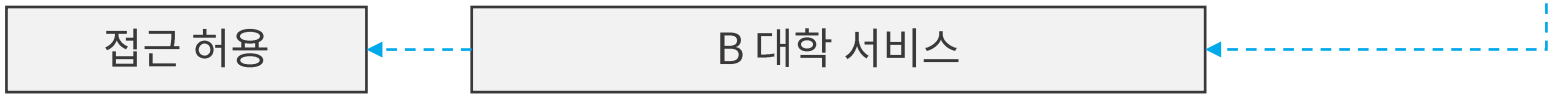


SAML 연합 로그인의 동작 과정

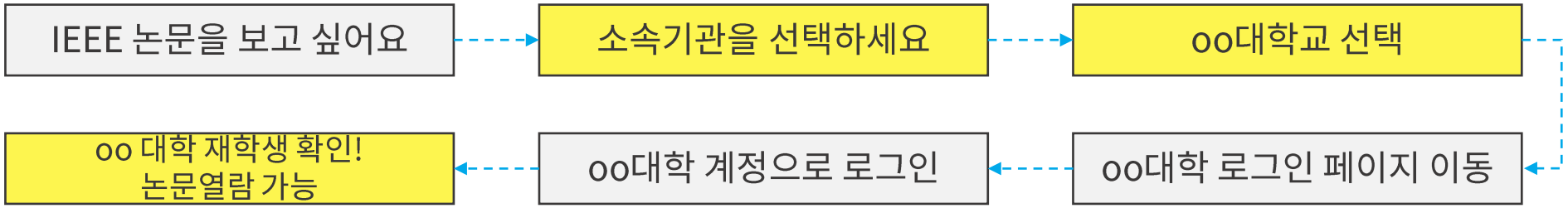
- 1단계: 사전 준비(메타데이터 교환)

- 2단계: 사용자 인증

- 3단계: 서비스 이용

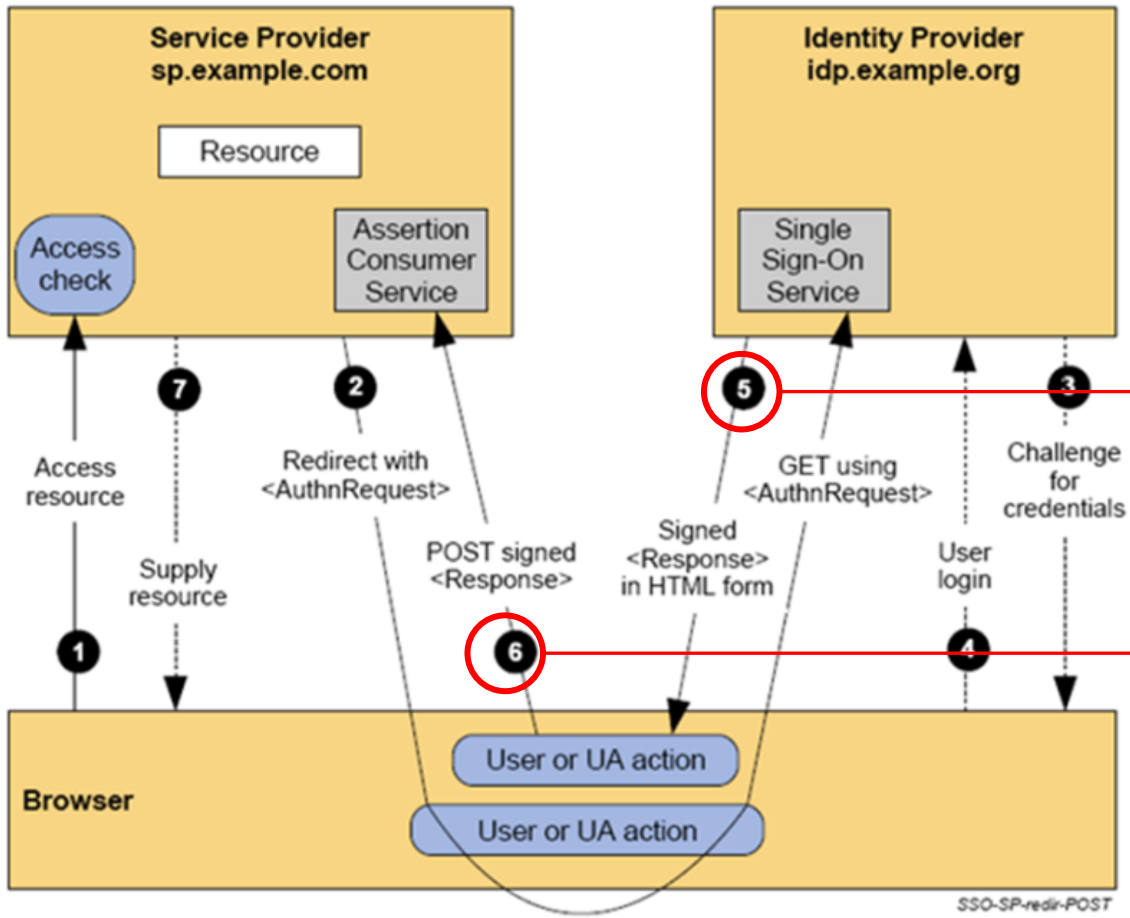


- 실 사용 예시



SAML에서 정보 전달 방식

- 웹 브라우저를 중개자로 활용하는 방식을 주로 사용



- 사용자 속성 정보를 전달
- 패스워드는 속성에 포함되지 않음

Img. Source: Wikipedia, ECLIPSE Foundation

데모 I

- Inter-federation (국제 서비스제공자)

https://ieeexplore.ieee.org/Xplore/home.jsp
https://www.home.cern/

- Identity provider: KISTI (KR)
- Service provider: IEEExplore (US), CERN (SWISS)
- Standard: SAML

데모 II

Local-federation (국내 서비스제공자)

https://webinar.kafe.or.kr

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

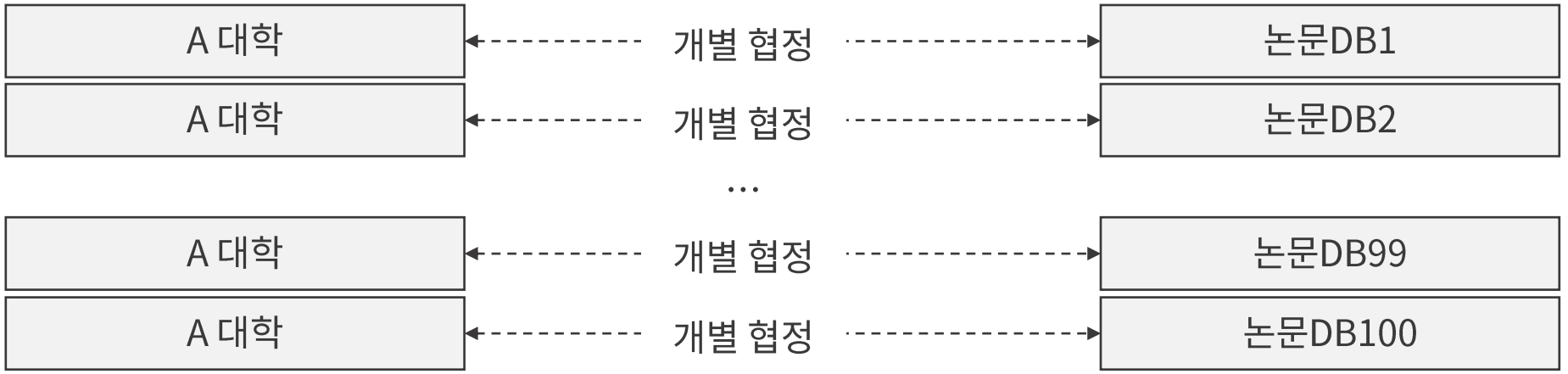
3차시: 연합 로그인과 KAFE의 역할

연합(federation)의 개념

- 신뢰 네트워크

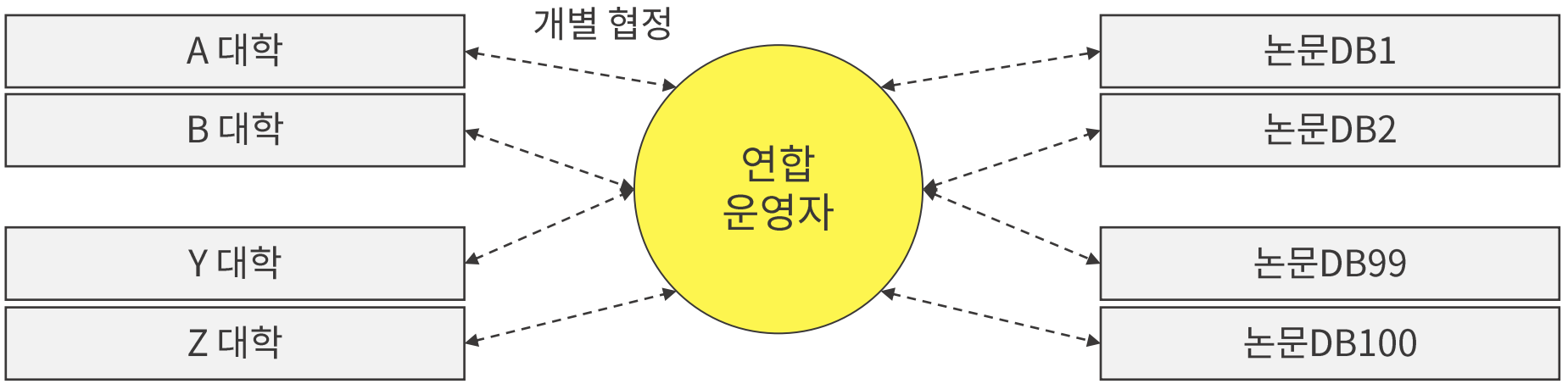
- Federation = 여행사
- IdP 기관 = 여권 발급국가
- SP 서비스 = 여행 목적지
- 사용자 = 여행자

연합이 없다면?



- 각 기관마다 수백 개 서비스와 개별 협정 필요
- 메타데이터 교환과 관리 복잡
- 보안 정책의 일관성 부족
- 새로운 서비스 추가 시 모든 기관이 개별 작업

연합이 있다면?



- 한 번의 협정(가입)으로 모든 연동 서비스 이용
- (관리 정책 표준화 및 일원화)통일된 보안 정책과 관리
- 새로운 서비스 추가 시 자동 연동
- 기술 지원과 문제 해결 도움

KAFE(Korean Access Federation) 현황

- KAFE는?

  1. 한국과학기술정보연구원 국가과학기술연구망에서 운영 중인 국내 연합체

- 34개 국내 학연기관 및 83개 서비스제공자로 구성

NAME	COUNTRY	ENTITIES	IDP	SP	AA
RCTSaai Federation	Portugal	139	108	31	0
KAFE	South Korea	117	34	83	0
PIONIER.Id	Poland	109	92	17	0

- 국가 간 연합(eduGAIN)을 통해 6,058 학연기관 및 3,790 서비스제공자와 연동(약 27,000,000 사용자)

KAFE 연동 서비스

- 상용 서비스는 (기관) 구독 라이선스 필요

IEEE xplore, Nature, MathWorks 등 학술 서비스

AIDA, National Bio-Big Data, Chembank 등 과학기술 서비스

Webinar, Webmeet, ZOOM 등 협업응용 서비스

주체 별 역할과 책임

Identity Provider(학연)	KAFE(연합 운영자)	Service Provider
소속 구성원의 신원 확인 사용자 인증 및 속성 정보 제공 IdP 시스템 구축 운영	메타데이터 중앙집중식 관리 참여기관 간 신뢰관계 중개 연합정책 수립 및 관리 기술지원 및 교육	콘텐츠 및 자원 제공 연합 로그인에 대한 접근제어 사용자별 서비스 개인화
사용자 계정 관리 연합정책 및 기술표준 준수 개인정보보호 준수 IdP 시스템 보안 유지	서비스 안정성 보장 보안사요 예방 및 대응 품질 기준 유지	사용자 데이터 보호 연합정책 및 기술표준 준수 사용자 데이터 보호

신뢰 체계

- 기술적 신뢰

  디지털 서명: 메타데이터 및 인증 메시지의 위변조 방지
  암호화 통신: HTTPS/TLS 필수
  표준 준수: SAML 2.0 국제 표준 적용

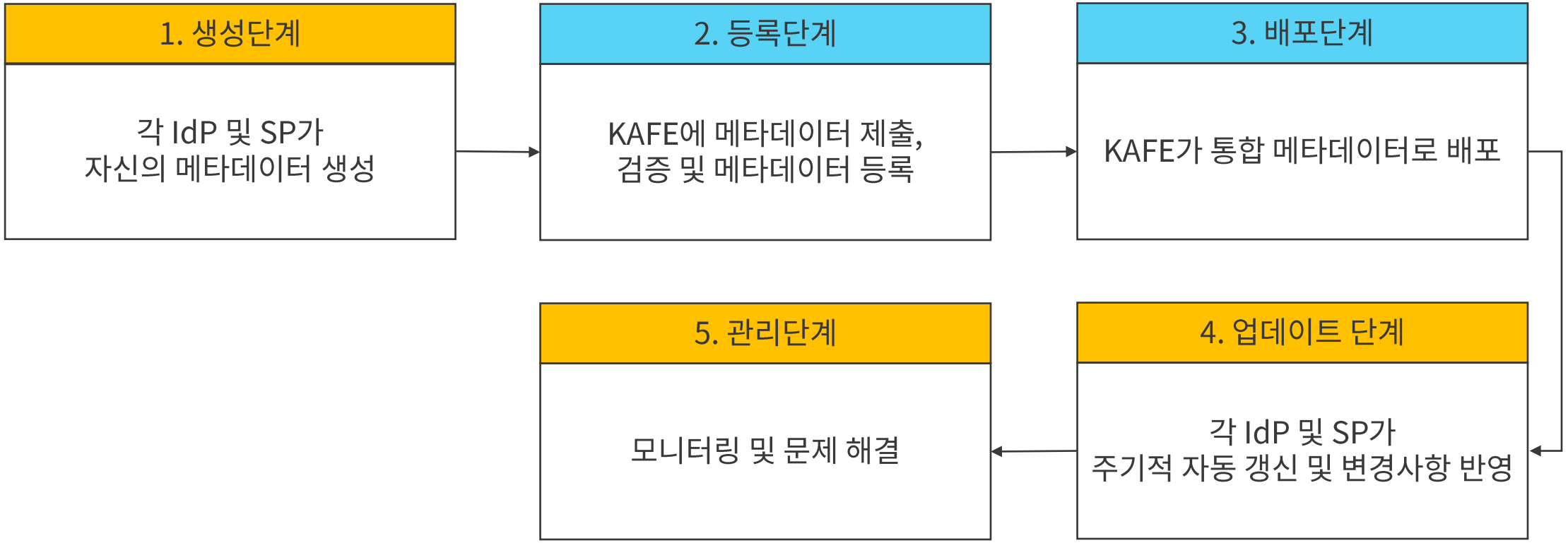
- 정책적 신뢰

  가입 심사: 기관 자격과 기술 요건 검증
  연합 정책: 모든 참여자가 동의하는 규칙
  신원 관리: 신원 정보의 등록, 유지, 삭제 등 정책 준수

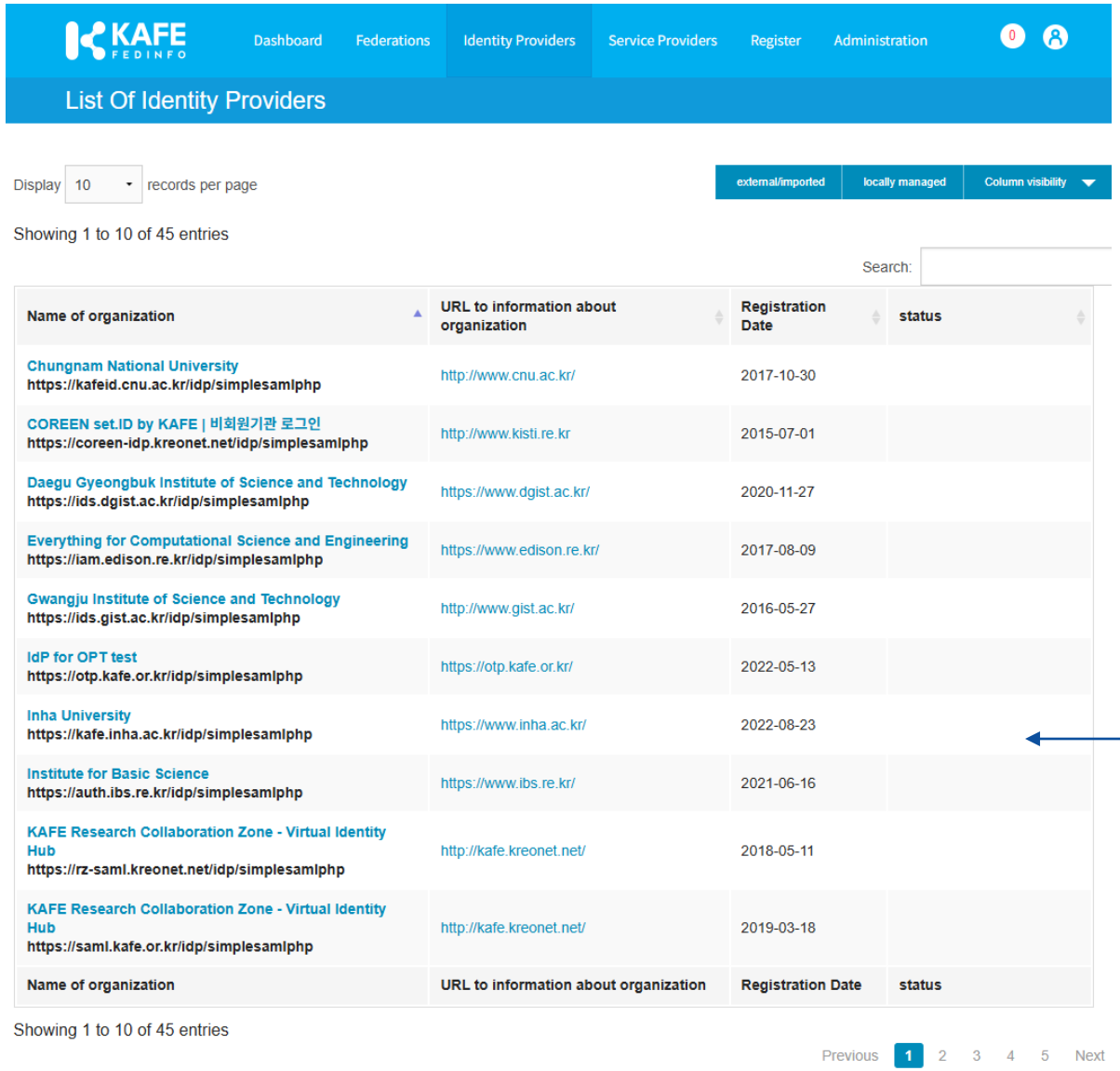
- 운영적 신뢰

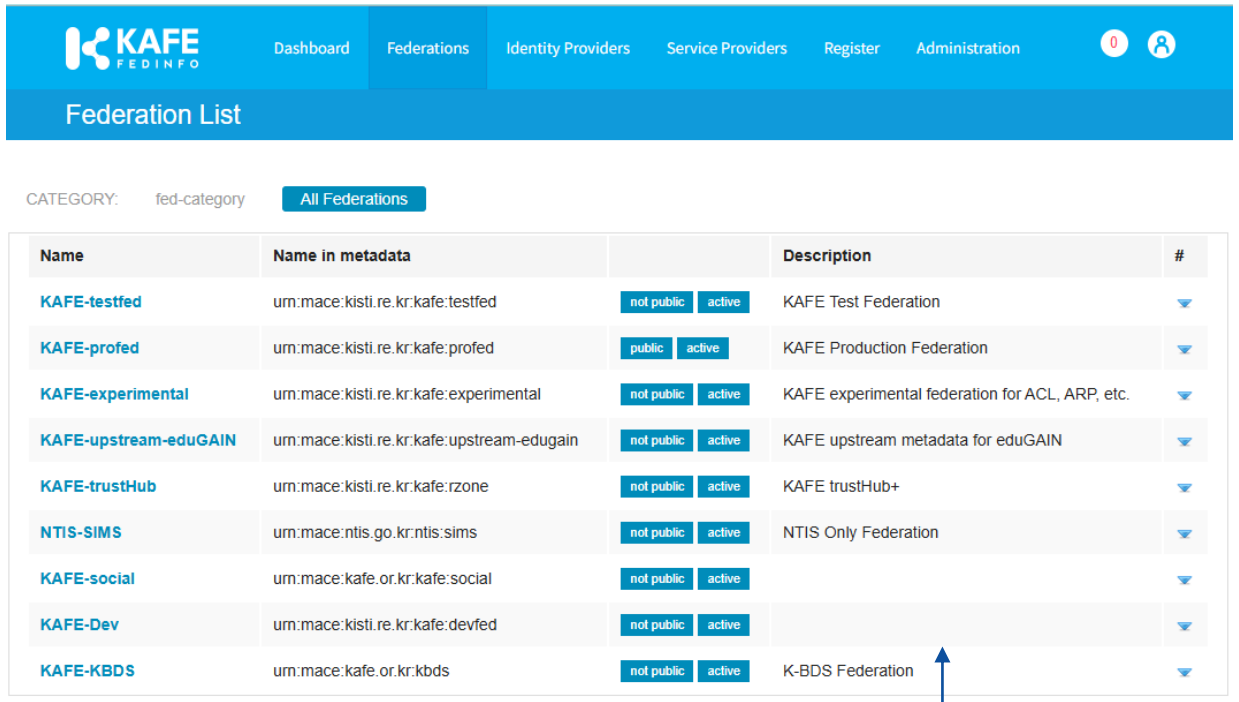
  24/7 모니터링: 시스템 안정성 감시
  사고 대응: 국제 표준 보안 사고 대응 체계
  연합 도구: 편의성 및 연속성 보장

메타데이터의 생명주기(Lifecycle)



메타데이터의 등록 및 배포





2. 개별 메타데이터 등록

3. 통합 메타데이터 배포

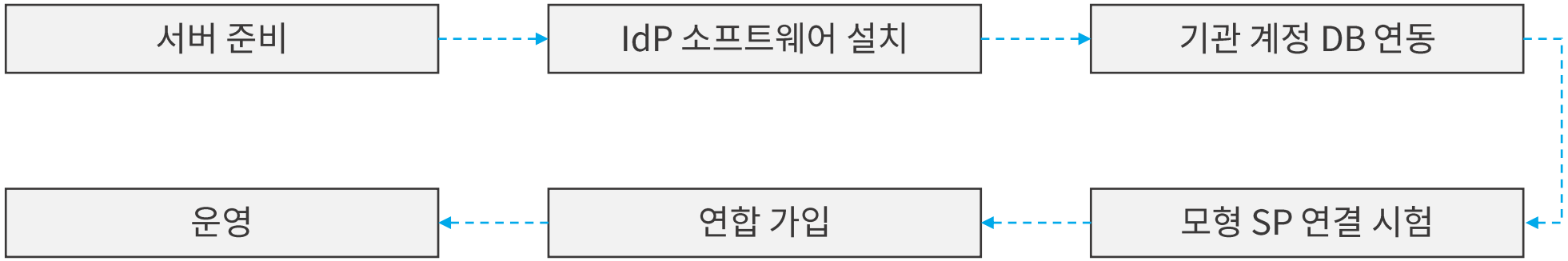
4차시: SAML IdP 구축

실습 환경

- IdP = 디지털 신분증 발급 및 상태 정비소

  - 사용자 신원 확인(ID/PW 검증)
  - 디지털 신분증 발급(SAML 토큰 생성)
  - 사용자 정보 관리 및 제공(이름, 소속, 직급 등)
  - 보안 관리(로그인 시도제한, 기록 관리, OTP 등)

- 구축 절차



IdP 구축 개요

- 테스트용 IdP 서버
  - https://ssptest.seasonsoft.net/saml/
    - 비밀번호: kafe123!@
  - 샘플 사용자 계정
    - student[1~5]/student1234

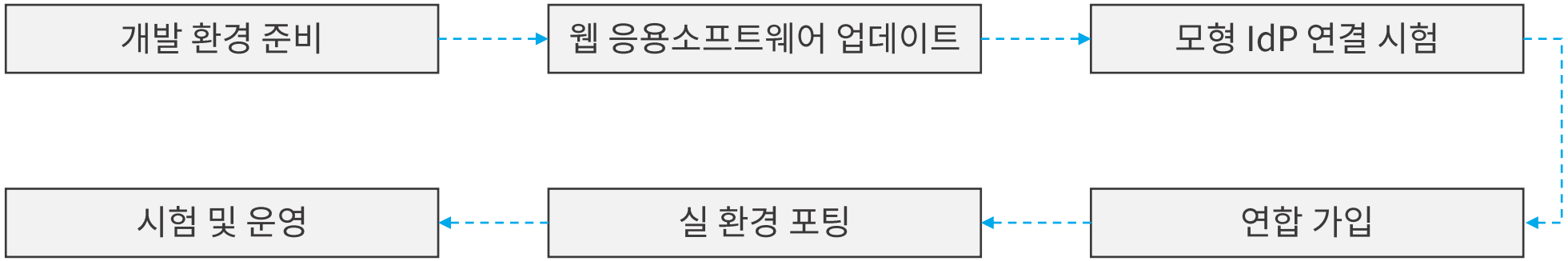
<참고> SP는?

- SP = 디지털 신분증 이용 및 접근 허용

  - 디지털 신분증 확인(SAML 토큰 소비)
  - 사용자 정보(이름, 소속, 직급 등)를 이용한 서비스 이용 권한 부여

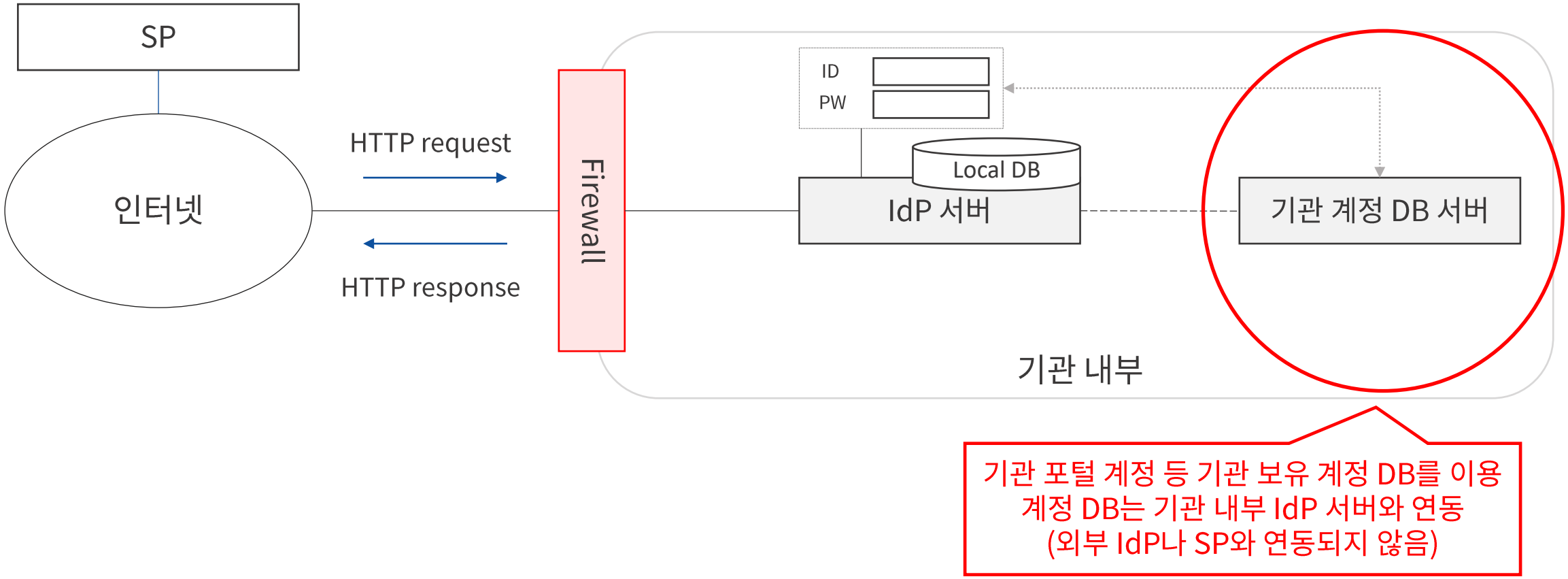
- **웹 응용 업데이트 개발 필요: Why? IdP와 호환되어야 함**

- 구현 절차



IdP 서버 구축 환경

- 기관 내부 DMZ 환경에 구축



IdP 소프트웨어 설치 환경

- 운영체제
  - Rocky Linux 8.8 이상 (8.x)
- 웹 서버
  - Apache 2.4+
- 데이터베이스
  - MariaDB 10.x
- 스크립트 언어
  - PHP 8.2+
- 보안
  - TLS 인증서(기관 와일드카드 인증서)

IdP 설치

- 체크리스트
  - 권장 서버 사양: CPU 4코어, RAM 8GB, 디스크 100GB
  - 서버 Clean slate 상태 유지
  - 소프트웨어 방화벽 비활성화
  - 시간 동기화
  - 기관 로고 파일 (240x80 픽셀/로그인 화면용, 60x20 픽셀/탐색 서비스용)
  - 인터넷 연결 필수(소프트웨어 패키지 설치): 고정 IP 및 도메인 이름
- 설치 과정 간소화

기관 사용자 계정 DB 연동

- 로컬 및 원격 데이터베이스

  - 로컬(IdP): 서버 설정 상태 및 로그 정보 저장
    - 로컬 서버는 사용자 계정 정보를 저장하지 않음
  - 원격(기관): 사용자 계정 저장

- 원격 DB 연동 방법
  1. RESTful API (권장)
  2. 직접 DB 연결: Oracle, LDAP/AD, MySQL, MSSql, PostgreSQL 등

- 원격 DB 저장 필수 사용자 정보
  - 사용자 ID
  - 비밀번호
  - **성명(성과 이름 분리 권장, 영문 권장)**
  - 이메일 주소
  - **직무 정보(faculty/staff/student)**

<참고> 원격 계정 DB의 직무 정보

- 직무정보는 아래 값 중 하나를 반환해야 함

상용 서비스에서 접근 권한 관리에 사용하는 속성
<중요> 상용서비스 이용 권한은 기관에서 결정(서비스마다 별도 설정 가능)

속성 값	설명	상용서비스 이용 권한
student	재학 중인 모든 학생	있음
faculty	교원 및 연구원	있음
staff	행정 직원	있음
alum	졸업생	없음
affiliate	협력 기관 소속 인력 등 기타 구성원	불가

원격 DB 연동 과정 예시

1. DB 드라이버 설치
   - Oracle: OCI driver 설치
2. 연결 테스트 스크립트 작성: 원격 DB 연결 및 사용자 정보 획득(실 사용자 ID/PW 필요)
   - test_connection.php
3. IdP 연동 모듈 수정: 위 2번의 스크립트를 기반으로 모듈 수정
   - /var/simplesamlphp/modules/kafe/src/Auth/Source/CoreAuth.php 의 login() 함수
     - DB 필드 이름을 사용자 속성 이름으로 변환
     - 시도 회수 제한 등 기능 설정

사용자 속성 생성 및 매핑

1. SAML 표준 속성 이해
   - 기본 속성
     - displayName: 별칭(however, 성명과 동일하게 사용)
     - mail: 전자우편 주소
     - sn: 성(surname, family name)
     - givenName: 이름
   - 학연 기관 전용 속성
     - eduPersonPrincipalName: **글로벌 고유 식별자**
     - eduPersonTargetedID: **서비스별 고유 식별자**
     - eduPersonScopedAffiliation: 소속 정보(예, faculty@korea.ac.kr)

2. 속성 변환 예시(기관 DB → SAML 속성)
   - KOR_NM: 김철수 → displayName: 김철수
   - TITLE: 교수 → eduPersonAffiliation: [‘faculty’, ‘member’]
   - UID: prof1234 → eduPersonPrincipalName: prof123@korea.ac.kr
   - COLL: 코리아대학교 → schacHomeOrganization: korea.ac.kr

보안설정

1. 로그인 보안 강화

- 로그인 시도 횟수 제한(설정 가능): 예, 5회 실패 시 계정 차단
- 계정 잠금/해제 기능
- 로그인 기록 관리
- 사용자 동의 관리

2. 인증서 및 암호화

- 기관 Wildcard 인증서
- HTTPS 통신 강제
- 메타데이터 디지털 서명

3. 방화벽 설정 가이드: 아래 포트 개방 필요

- HTTPS: TCP 80/443
- NTP(Network Time Protocol): UDP 123

문제 해결

1. 자주 발생하는 문제
   - 시간 동기화

     - 반드시 NTP 동기화되어야 함(기본 설정: time.kriss.re.kr)
     - Replay attack 방지 목적

     → ntp나 chronyd를 통해 ntp 재설정 및 동작 여부 검증

   - 기관 DB 연결 실패

     - 데이터베이스 서버 또는 IdP 서버의 방화벽 설정 변경

   - 메타데이터 오류

     - 서비스제공자가 KAFE에 가입되어 있지 않거나; KAFE에서 차단(정책 위반으로 인해)한 경우

     → 정상 동작임

     → 해당 서비스제공자를 이용해야 하는 경우 support@kafe.or.kr 로 문의

관리 운영 도구

1. 관리 기능 (KAFE Admin Panel)

- 사용자 관리: 계정 잠금 및 해제
- 서비스 관리: 서비스제공자 접근 권한 설정(속성 기반)
- 로그 관리: 로그인 미 사용자 동의기록 조회
- 보안 관리: OTP 설정

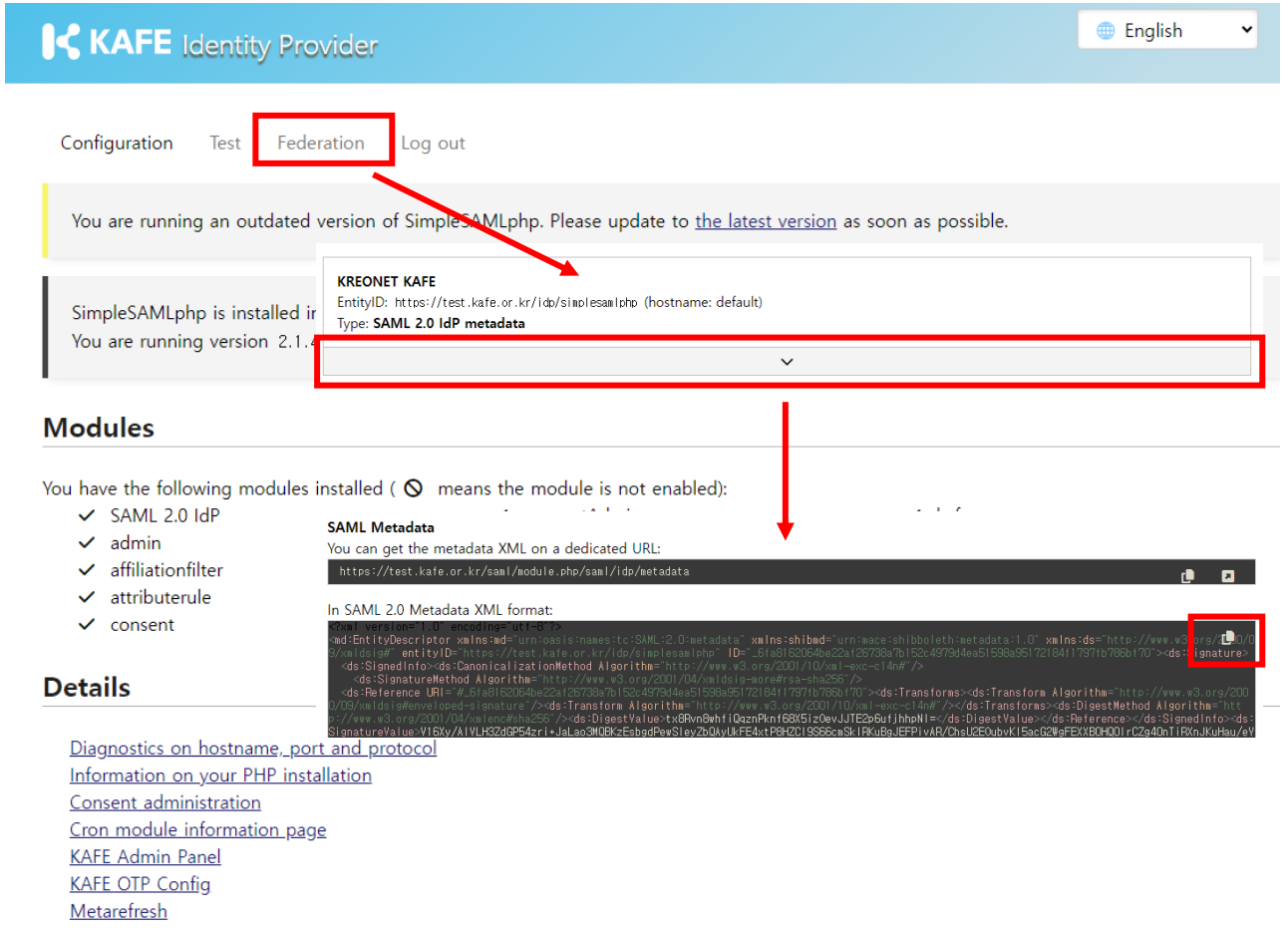
2. 기타

- 시스템 상태 모니터링
- 로그인 오류 분석 지원
- 메타데이터 업데이트 지원

구축된 IdP의 검증: IdP 메타데이터 확보

1. 관리자 페이지 접속
   - https://[test.kafe.or.kr]/saml/module.php/admin
   - 암호는 .env 파일의 ADMIN_PASSWORD 값

2. 메타데이터 추출
   - Federation 탭 클릭
   - SAML 2.0 IdP metadata 클릭
   - In SAML 2.0 Metadata XML format의 메타데이터를 복사

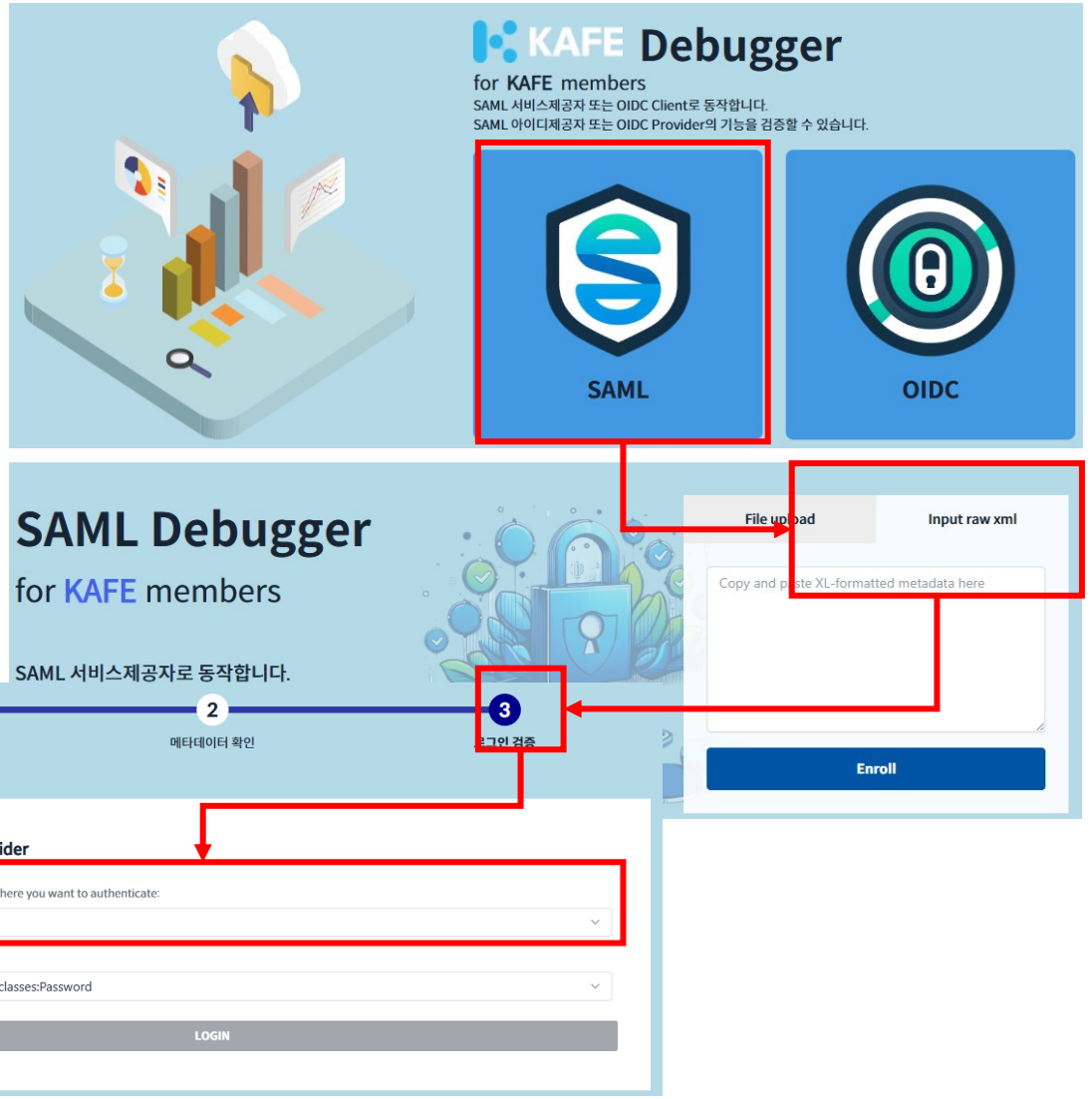


구축된 IdP의 검증: KAFE Debugger 이용

1. KAFE Debugger 접속
   - https://debug.kafe.or.kr
   - SAML 선택

2. 메타데이터 등록
   - Input raw xml에 복사한 IdP 메타데이터 붙여넣기

3. 로그인 테스트
   - 로그인 검증으로 이동
   - 구축된 IdP 선택하여 로그인
   - 사용자 정보 전달 확인



중요 검증 사항

- 2명 이상의 사용자로 테스트
- eduPersonTargetedID 값이 사용자별로 다른지 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

5차시: IdP 운영 및 KAFE 가입

KAFE 가입 등 회원기관 등록

1. 가입신청서 작성 및 제출
   - 필수 준비 사항

     - support@kafe.or.kr에 가입 신청서 요청
     - IdP 가입신청서는 기관장(원장, 총장 등) 직인 필수

   - 제출 방법

     - 공문 발송(수신처: 한국과학기술정보연구원)
     - 또는 이메일: support@kafe.or.kr

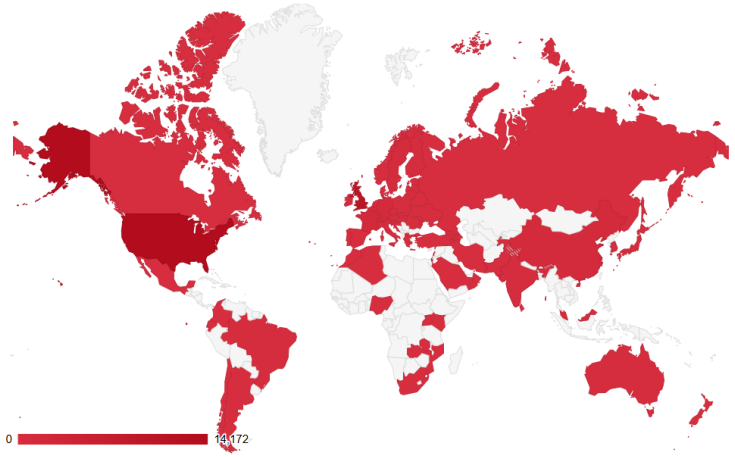
   - 함께 제출할 필수 자료

     - 구축된 IdP의 메타데이터 파일

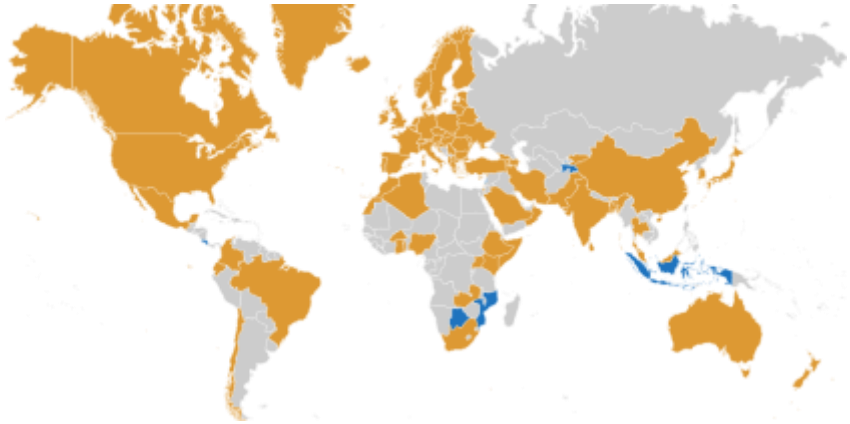
eduGAIN 국가 간 연합 참여

- eduGAIN이란?
  - 국제 교육연구 연합 네트워크: 전 세계 연구기관과 교육 기관을 서비스제공자와 연결하는 글로벌 연합 서비스
  - GEANT(EU)에 의해 운영
- KAFE와 eduGAIN 연동 현황
  - 2016년부터 eduGAIN에 연결
  - KAFE 가입 시 eduGAIN 연동 여부 결정
  - 글로벌 협업 연구 지원: 국제 공동연구 프로젝트 참여시 원활한 자원 접근
- eduGAIN 연동 시 준수 사항
  - eduGAIN 정책 준수(KAFE는 eduGAIN 정책을 상속 함)
  - REFEDS SIRTFI(연합 신원 관리를 위한 보안 표준) 준수

<참고> 연합체 운영 국가



자국내 연합체 운영 국가



국가 간 연합체 참여 국가

REFEDS SIRTFI 및 TLP

- SIRTFI(Security Incident Response Trust Framework for Federated Identity)
  - 보안사고 대응 신뢰 프레임워크
  - SIRTFI 인증 요구사항
    - 기술적 요구사항
      - 보안사고 대응팀(CSIRT) 운영 또는 연계
      - 보안사고 신고 및 대응 절차 수립
      - 정기적인 보안 점검 및 모니터링 체계
    - 운영적 요구사항
      - 24시간 보안사고 대응 연락체계 구축
      - 보안사고 발생 시 72시간 내 대응 절차
      - 정기적인 보안 교육 및 훈련 실시
- TLP(Traffic Light Protocol)
  - 정보의 민감도와 공유 범위를 색상으로 표시

- TLP:RED
  - 수신자 개인만 이용 가능
  - 절대 외부 공유 금지
  - 극도로 민감한 정보

- TLP:AMBER
  - 조직 내부 또는 신뢰할 수 있는 파트너만 공유
  - 제한적 공유 허용
  - 민감한 정보

- TLP: GREEN
  - 커뮤니티 내에서 공개
  - 일반적 보안 정보
  - 광범위한 공유 허용

- TLP: WHITE
  - 공개 정보
  - 제한없는 공유/배포

IdP 운영 관리 및 문제 해결

- 시스템 상태 모니터링: 필수 서비스 상태(active) 확인

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

- 메타데이터 관련 오류
  - Metadata for the entity expired 오류

원인: NTP 동기화 또는 메타데이터 업데이트 불량
해결: Admin 화면에서 metarefresh 클릭

  - Metadata not found 오류

원인: KAFE에 가입되지 않은 서비스 제공자 접근
해결: 정상 동작이므로 무시하거나
(서비스 이용이 반드시 필요한 경우) support@kafe.or.kr에 문의

상용서비스 연계를 위한 정보 제공

- 필수 제공 정보: 상용서비스 연계 시 서비스제공자에게 전달해야 하는 정보

  - EntityID(개체식별자): IdP의 고유 식별자로 메타데이터에서 entityid로 검색 가능
  - Scope(기관 대표 도메인): 메타데이터에서 scope로 검색 가능
  - Affiliation(직무정보)
    - 학생: student@scope (예, student@korea.ac.kr)
    - 교수: faculty@scope (예, faculty@korea.ac.kr)
    - 직원: staff@scope (예, staff@korea.ac.kr)

- EntityID와 Scope 정보의 확인 방법

  - IdP admin 화면의 Federation 메뉴 접속
  - SAML metadata 탭 선택
  - XML format에서 해당 정보 검색

Korean Access Federation

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