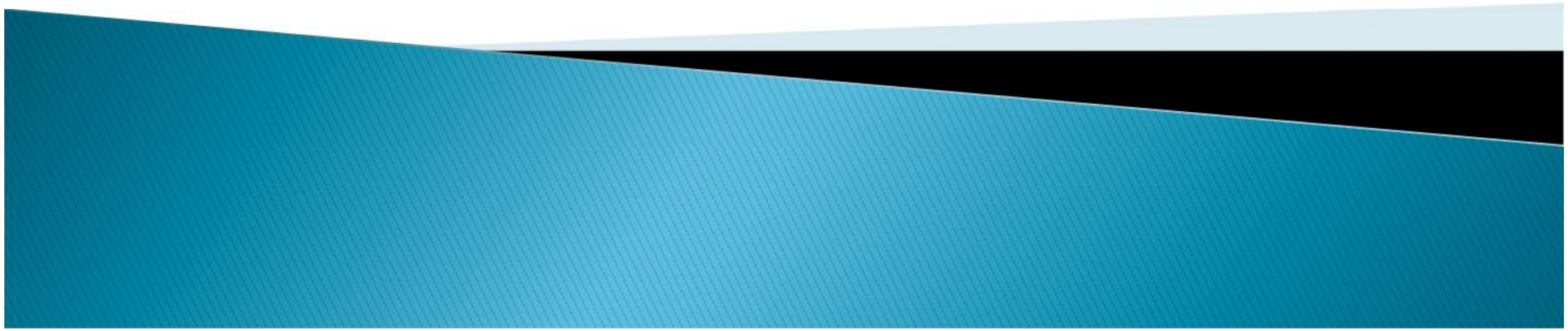
ID Federation 개요 및 KREONET/KISTI 현황

조진용(jiny92@kisti.re.kr)
한국과학기술정보연구원
2015-07-23(목), TEIN-CC 주최

본 발표의 내용은 국가과학기술연구망/한국과학기술정보연구원의 공식적인 입장을 대변하지 않습니다.



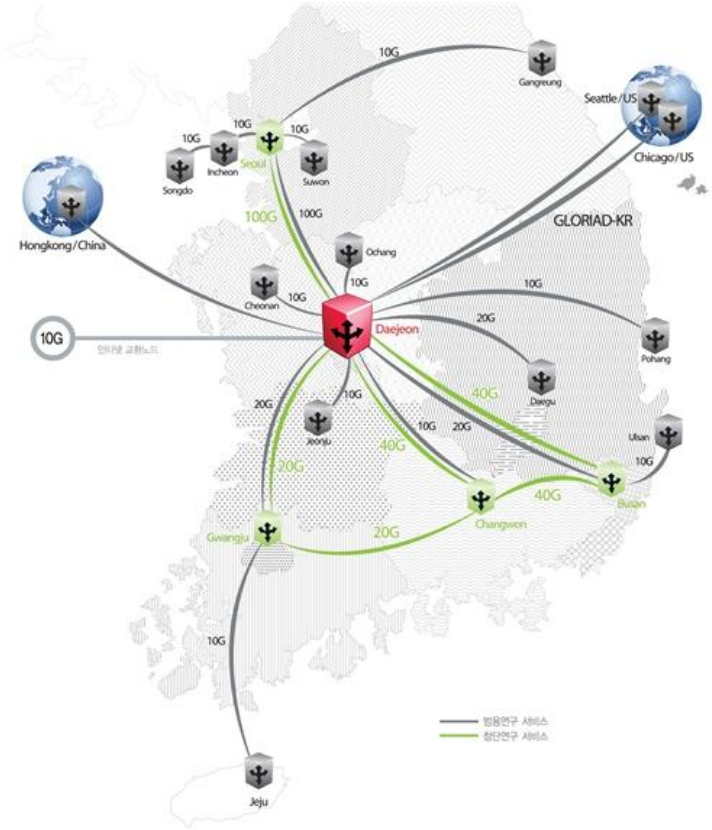
목차

- 큰 그림 – ID Federation
- ID Federation 기술
- KREONET/KISTI의 ID Federation 현황

KISTI 조직

NII(일본)과 JISC(영국)과 유사한 성격: 지식정보서비스 + 연구망

KREONET 소개



- 교육과학기술부(1988) 지원으로 구축된 국가과학기술연구망
- KISTI, 경북대, GIST, 제주대 등 전국 16개 지역, 16개 지역망센터로 구성
- 국가과학기술연구망 가입기관 수: 192개
- KAIST, KBSI, 충남대 등 7개 기관 대덕첨단 과학기술연구망(SuperSiReN) 10 Gbps 연동
- 글로벌 과학기술협업연구망(GLORIAD)을 통해 70여 개 국 100여 개 연구교육망과 연동
- 고에너지물리, 천문우주, 극지연구, 기상기후, 원격교육, 문화기술 등 연구개발 커뮤니티 지원
- KISTI는 글로벌무선로밍서비스(eduroam)의 국가단위운영주체(National Roaming Operator)

Big picture: ID Federation

aka ID 연계, ID 연합, Federated Identity Management,
Identity & Access Management

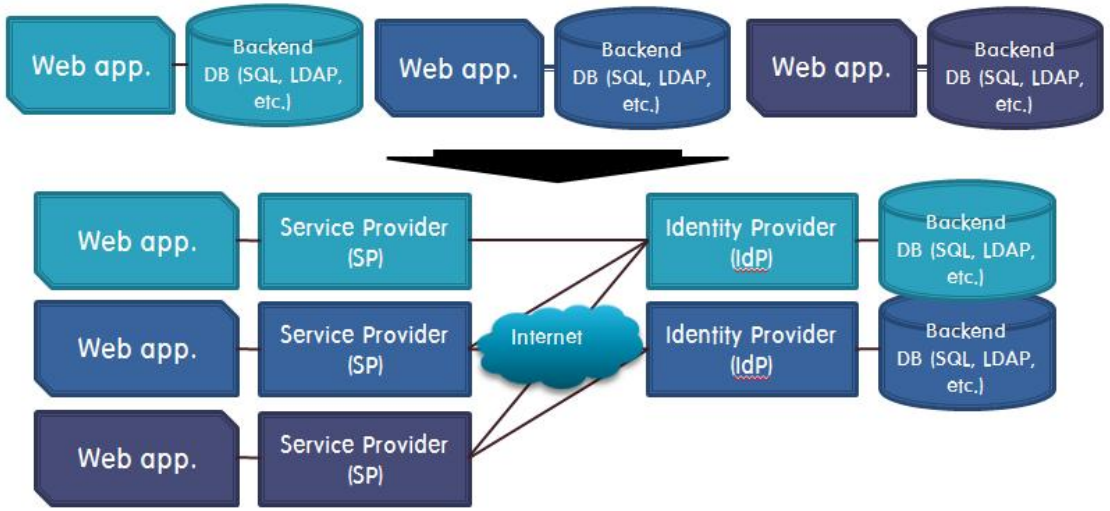
ID Federation이란?

- 서비스 제공자(Service Provider)가 원격지에 분산된 ID 제공자(Identity Provider)로부터 사용자 인증을 받는 방식

  - Identity 또는 ID:
    - 사용자의 id, 신상정보, 비신상정보, credential 등으로 구성
  - ID 제공자(Identity Provider, Identity Assertion Provider, IdP):
    - 서비스 제공자에게 사용자 인증기능과 사용자 속성정보를 제공하는 시스템 개체(system entity)
  - 서비스 제공자(Service Provider, SP):
    - ID 제공자가 제공하는 사용자 속성정보를 다른 시스템 개체들에 서비스하는 시스템 개체

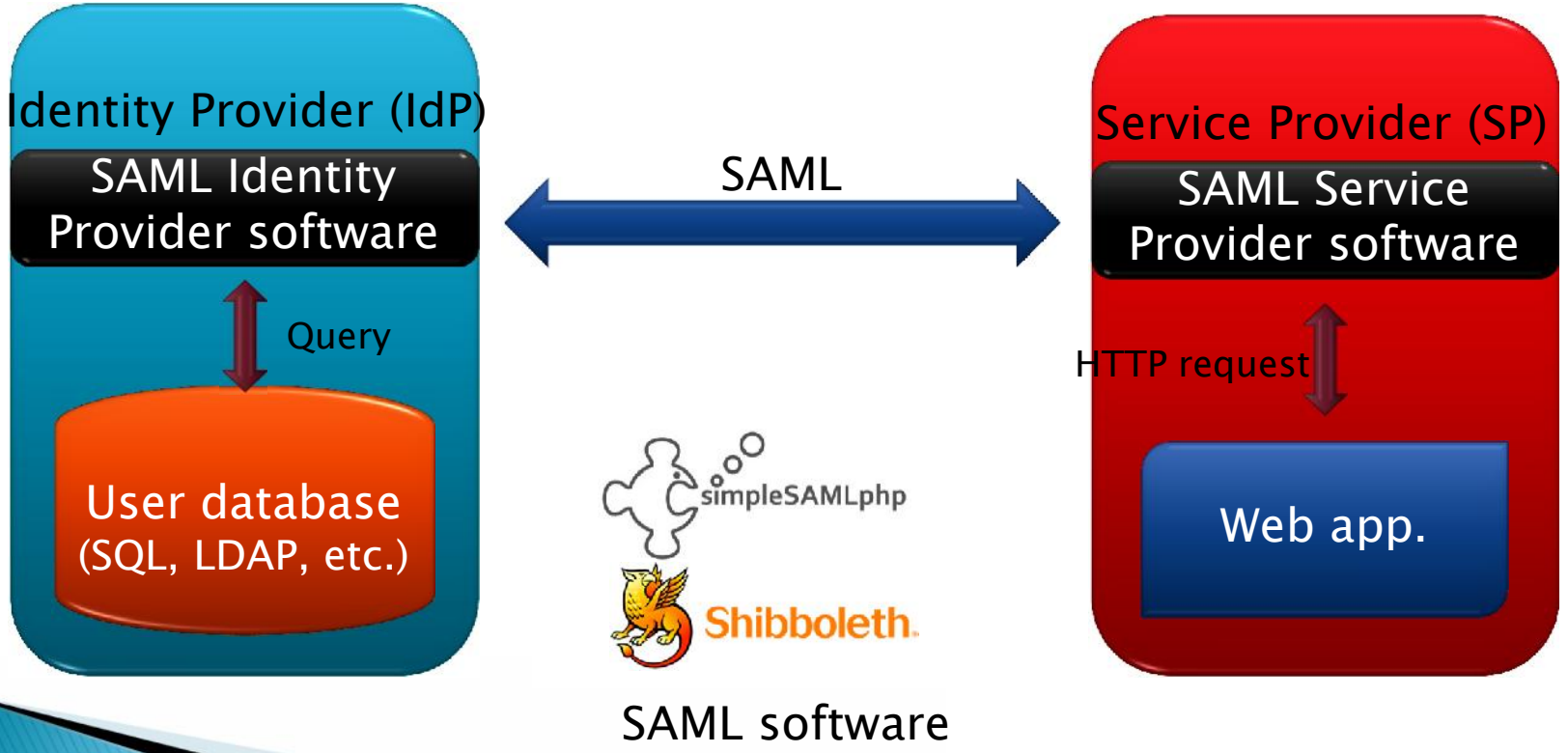
ID Federation의 목적

- 인증 및 사용자정보 관리의 표준화/간소화
- 연구자원 및 정보자산들의 국가적 공동 활용환경 조성



ID Federation의 기본 시스템 구조

- Service Enabler: SAML (Security Assertion Markup Language)



ID Federation 관련 국내외 연혁

- 2000-2005, Cyberinfrastructure(미)/e-Science(영) 사업의 산출물
- 2005-2008, 시범서비스 개시(기술 선도국)
  - 2008: SAML기반 경량화한 SSO 기술개발(ETRI)
- 2005-2011, Grid, e-Science 구축(KISTI)
- 2014-, ID 연계 및 협업응용서비스 제공환경 구축 (KREONET/KISTI)
- 2015, 전세계 52개국에서 국가적 ID 연계 서비스 제공, 33개국에서 국제적 ID 연계 서비스 제공 중

선도국의 ID Federation 서비스 현황

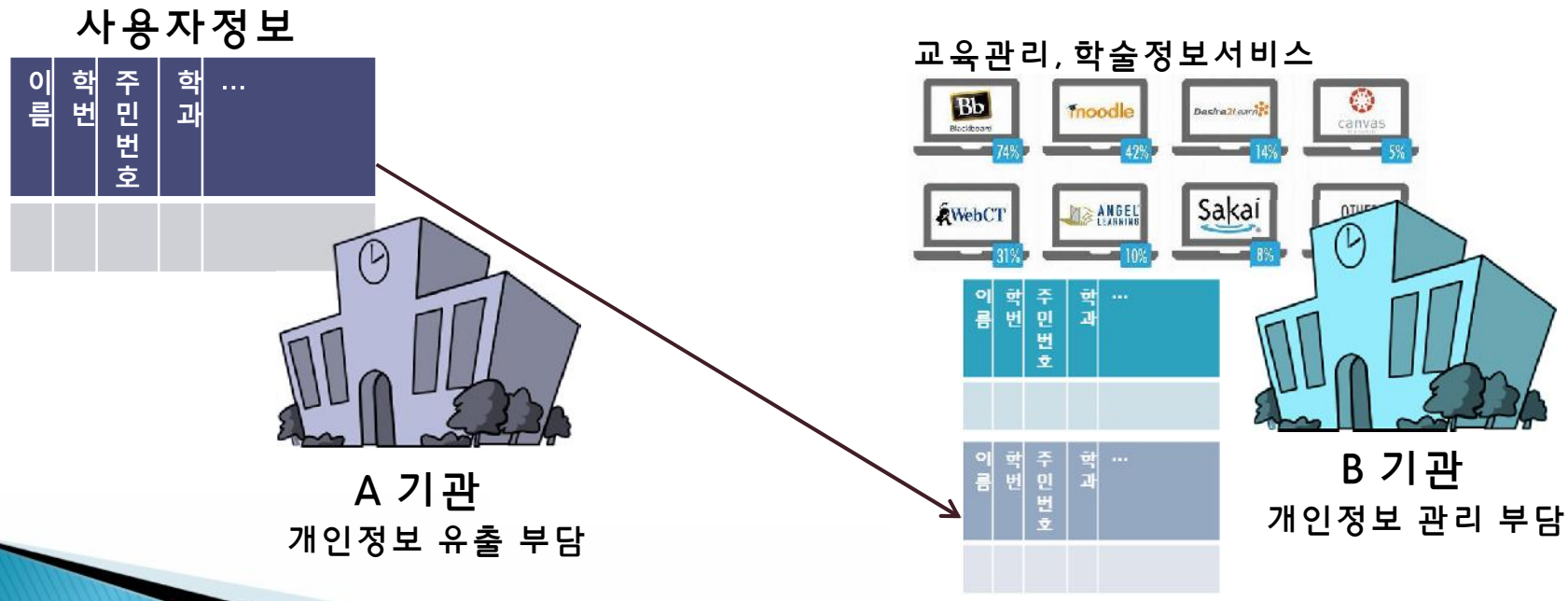
ID 연합체	ID 제공자	서비스 제공자	사용자	비고
InCommon/ Internet2 (미국)	500여 기관 참여	204여 클라우드 서비스 업체	750만명	상용
SURFconext/ SURFnet (네덜란드)	112개 기관	150개 이상 클라우드 업체	자국 내 연구 및 교육기관의 90% 수용	
Gakunin/ NII (일본)	170여 기관	100여 지식정보서비스 (2013년 기준)	국립대학의 90%이상	
AAF (호주)	50여 기관	100여 서비스 (저널,스토리지,협 업서비스 등)		상용
eduGain/Geant (네덜란드)	1,400여 기관	950여 서비스		33개국 연동

왜 연구교육망이 주도하는가?

- 네트워크를 활용하는 통신 기술
  - SAML 2.0 Profiles (SSO, SLO 등)
- 개인정보를 다루는 기술
  - 연구교육망들은 정보보호관련 조직을 보유
- 기관 전산/정보보호 책임자의 승인이 필요한 기술
  - 연구망의 종단 접속점은 개별 기관의 전산부서

ID Federation 서비스가 없다면?

- 정보자산의 공동활용이 어려움
  - 학교 간 서비스연계
  - 클라우드 및 상용 웹 응용의 연계
- 자국내 소프트웨어 산업(클라우드, 웹응용, 오픈소스 등)의 경쟁력 저하



장점 및 기대효과

사용자	ID 제공기관	서비스 제공기관 /업체	국가
• 하나의 사용자ID/패스워드만 기억 • 사용자등록이 필요하지 않음 • 다양한 유/무료 서비스 이용가능 • 개인정보 유출의 위험성 저하 • 개인정보의 일관성유지 가능	• 비 필수 서비스의 아웃소싱 • 외부 서비스에 대한 접근제어 강화 • 서비스 다양성 확보 • 향상된 연구협업환경 제공	• 서비스 개발범위 축소 및 개발시간 단축을 통한 조기 상품화 가능 • 마켓팅비용 절감 • 사용자확보 용이 • 기관별 접근제어가 가능 • 운영관리비용(Help desk 등) 절감	• 서비스 공동활용과 중복투자 방지 • 공동구매를 통한 정보자산 구입비용의 절감 • 개인정보의 유출 위험 감소 • 클라우드 및 SW 산업육성에 기여 • 연구협력 활성화 및 연구정보의 신속한 공유를 통한 국가과학기술 경쟁력 향상 • 서비스가 이용하는 사용자 정보의 표준화

ID Federation 기술

aka ID 연계, ID 연합, Federated Identity Management,
Identity & Access Management

Guest IdP와 SP 간 ID 연계 예

- 문제점: 사용자 Identity에 대한 검증

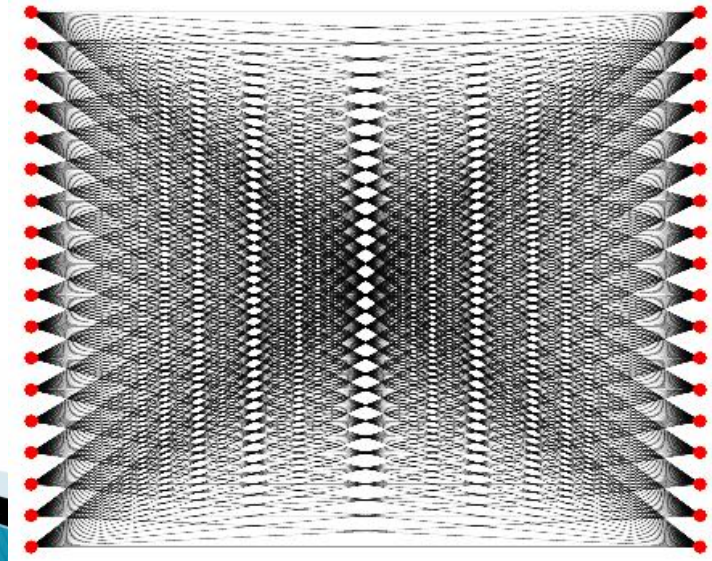
Home IdP와 SP 간 ID 연계 시나리오

ID Federation 위한 기술적 요구사항

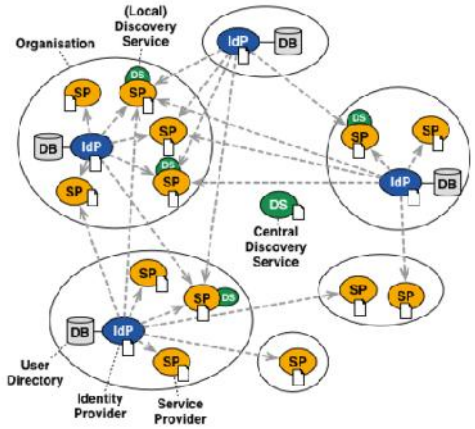
- Identity 정보를 나타낼 수 있는 표준화된 포맷
  - eduPerson, inetOrgPerson, SCHAC 등의 schema에 사용자 속성 정보를 포함
- Identity 정보의 교환을 위해 표준화, 보안, 개인정보보호, 호환성을 갖춘 프로토콜
  - SAML
- 기술적/법적 테두리 내에서 Identity 정보를 공유할 수 있는 Trust Relationships
  - 메타데이터의 교환, 정책 공유, 협약

메타데이터의 교환 및 관리의 어려움

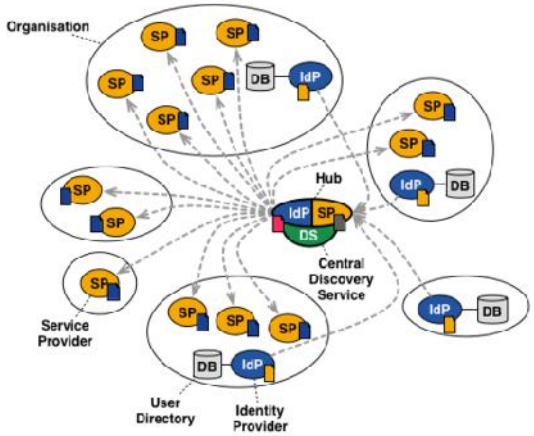
- 메타데이터
  - 시스템 entity가 제공하는 endpoint URL, key값, 프로파일지원방법 등을 담은 파일
- SP/IdP는 각자의 metadata를 대상 IdP/SP와 교환함으로써 Trust Relationship 관계를 형성
- 연계되는 IdP나 SP가 늘어난다면?
  - Service Discovery, 사용자 속성값 배포 관리, 메타데이터 관리의 문제가 발생



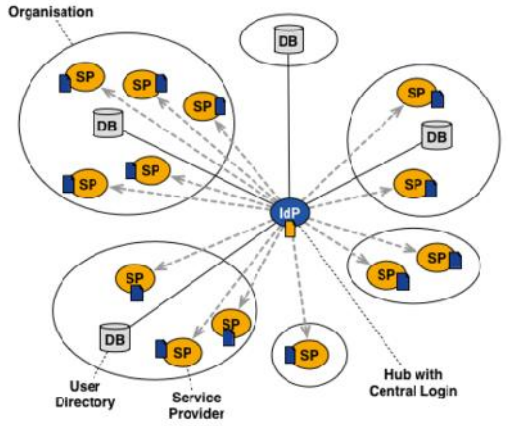
관리 및 제어의 편의성 향상을 위한 구조적 접근



Full Mesh 구조



Hub and Spoke 구조
(분산 로그인)

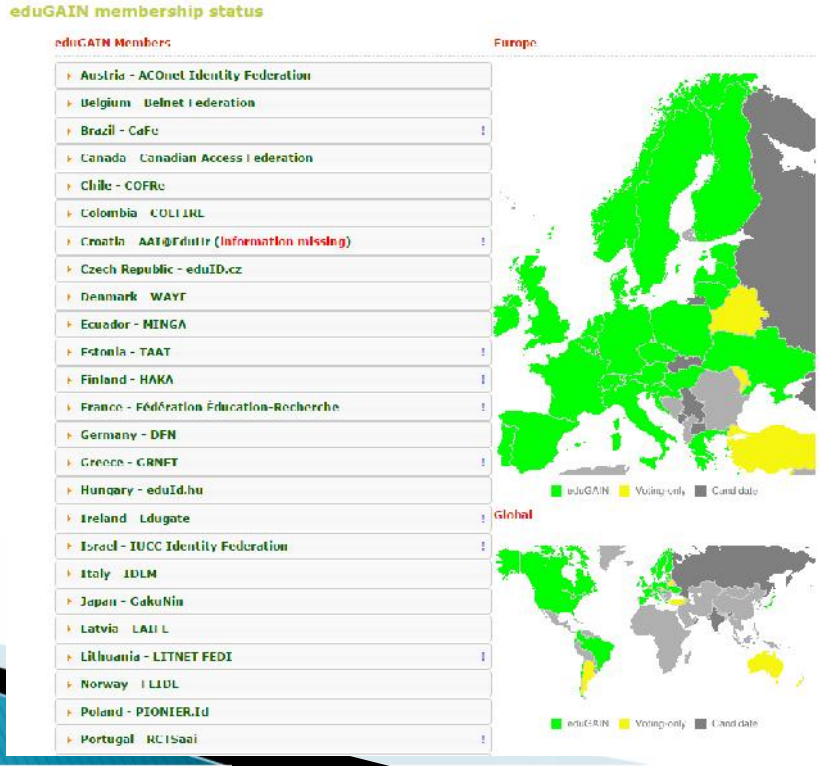


Hub and Spoke 구조
(중앙 로그인)

방식	장점	단점	비고
Full mesh	- Federation서비스 제공자측 보안관리	- 메타데이터 관리 - 사용자속성정보 관리	- 80%의 NREN Federation에서 채택
Hub-and-spoke (분산로그인)	- 메타데이터 관리 - 사용자속성정보 관리	- 제공자측 보안관리 - Single-point of failure	- 15% 의 NREN Federation에서 채택
Hub-and-spoke (중앙로그인)	- H&S의 장점 - 정부규제 적용 용이	- 확장성(Scalability) - 제공자측 보안관리 - Single-point of failure	- 5% 의 NREN Federation에서 채택

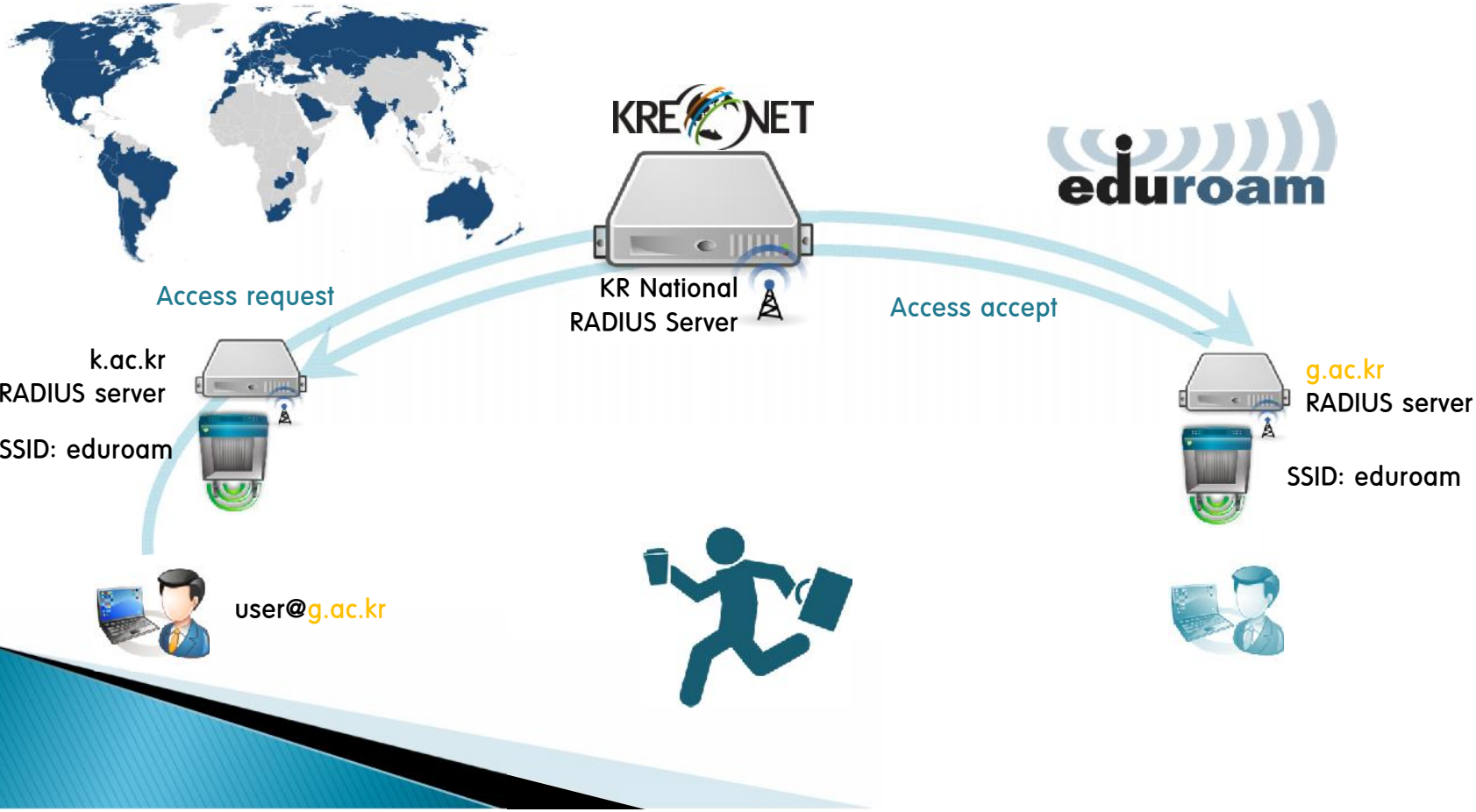
국가 간 ID Federation은?

- eduGain
  - TERENA에 소속된 한 Team에서 운영
  - Identity, 인증, 권한부여와 관련된 정보들을 안전하게 교환하기 위한 국가 간 federation 서비스
- 국가 간 ID 연계를 통해 서비스 이동성(?)이 향상
- eduroam(글로벌무선로밍서비스)은 국가 간 ID 연계의 예



국가 간 ID Federation의 예

- eduroam
  - 연구/교육 기관들의 무선**인증정보를 연계**해 타 기관의 무선인터넷 자원을 **공유**하는 서비스



eduroam vs., SAML ID Federation

- 비교

	eduroam	SAML ID Fed.
프로토콜	RADIUS	SAML
응용 서비스	무선접속 (단일)	Web 응용 (다수)
인증	O	O
권한부여	X	O
국제연계 주체	TERENA	eduGain(TERENA)
연계국가 수	74개국	33개국

KREONET/KISTI 현황

연혁

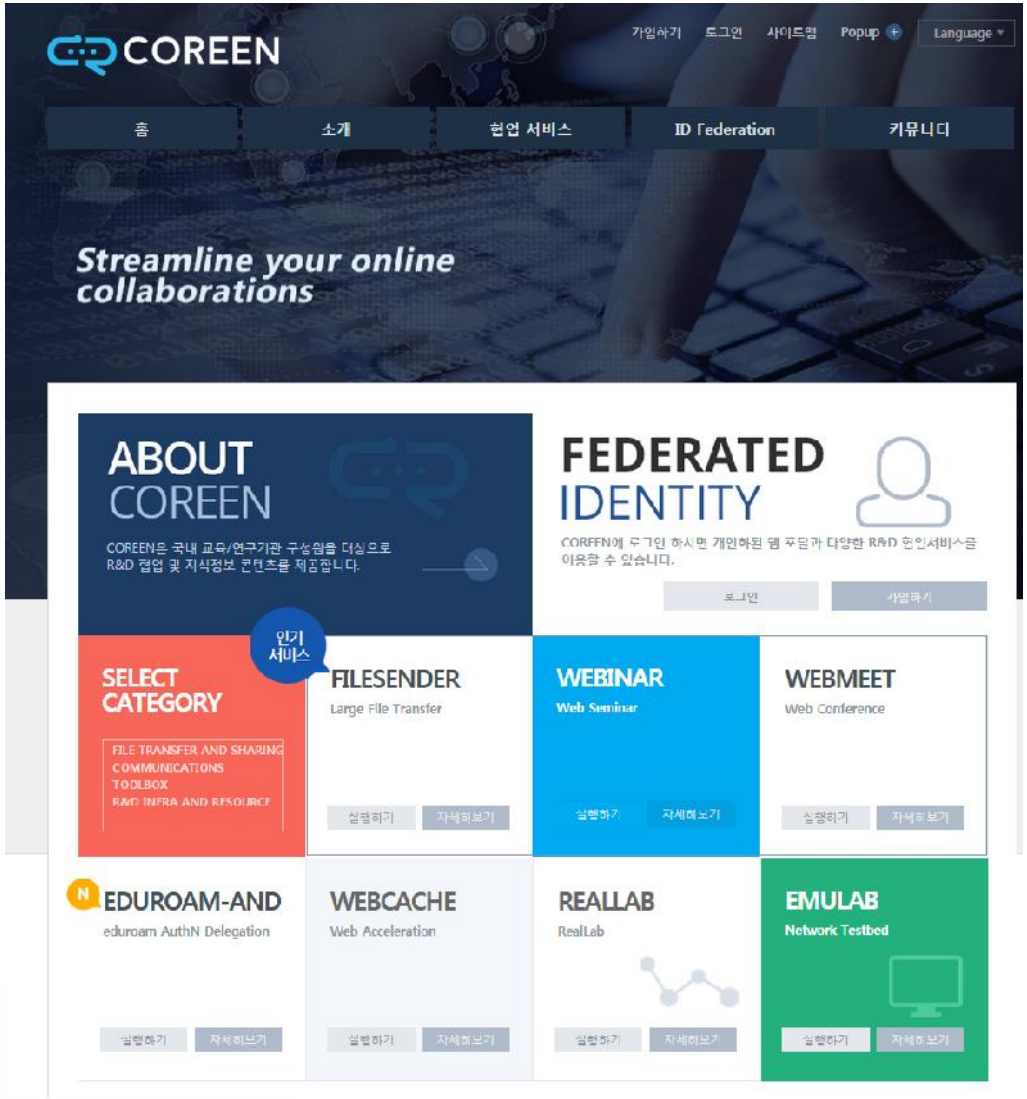
- 2012년
  - "통합협업환경 지원" 연구망 중점추진과제 제안, ADL Consulting
- 2013년
  - 기술 분석 및 유관 시스템 설계
- 2014년
  - IAM 시스템, 1 IdP, 4 SP의 프로토타입 자체 개발 및 적용가능성 검증
- 2015년
  - 알파서비스 시작
  - ID 연계 국가 대표기관(KISTI) 등록, REFEDS(Geant)
  - DGIST(대경과기원)와 기관 간 ID 연계 중(8월말 완료예정)
  - eduGain 연동 예정

COREEN 서비스

- 목적
  - 국내 교육 및 연구기관 구성원들이 타 기관/업체에서 제공하는 정보자산을 편리하고 안전하게 공동 활용할 수 있는 환경을 제공
- 추가 목적
  - 연구망 활용 활성화
  - 국내 클라우드/SW 산업 육성에 기여
- 서비스환경
  - 협업응용서비스(아카데믹 클라우드 서비스, 학술정보 서비스)와 ID 연계서비스(KAFe)로 구성
- 기관 기본사업(인큐베이터)으로 진행 중
- www.coreen.or.kr을 통해 알파서비스 제공 중

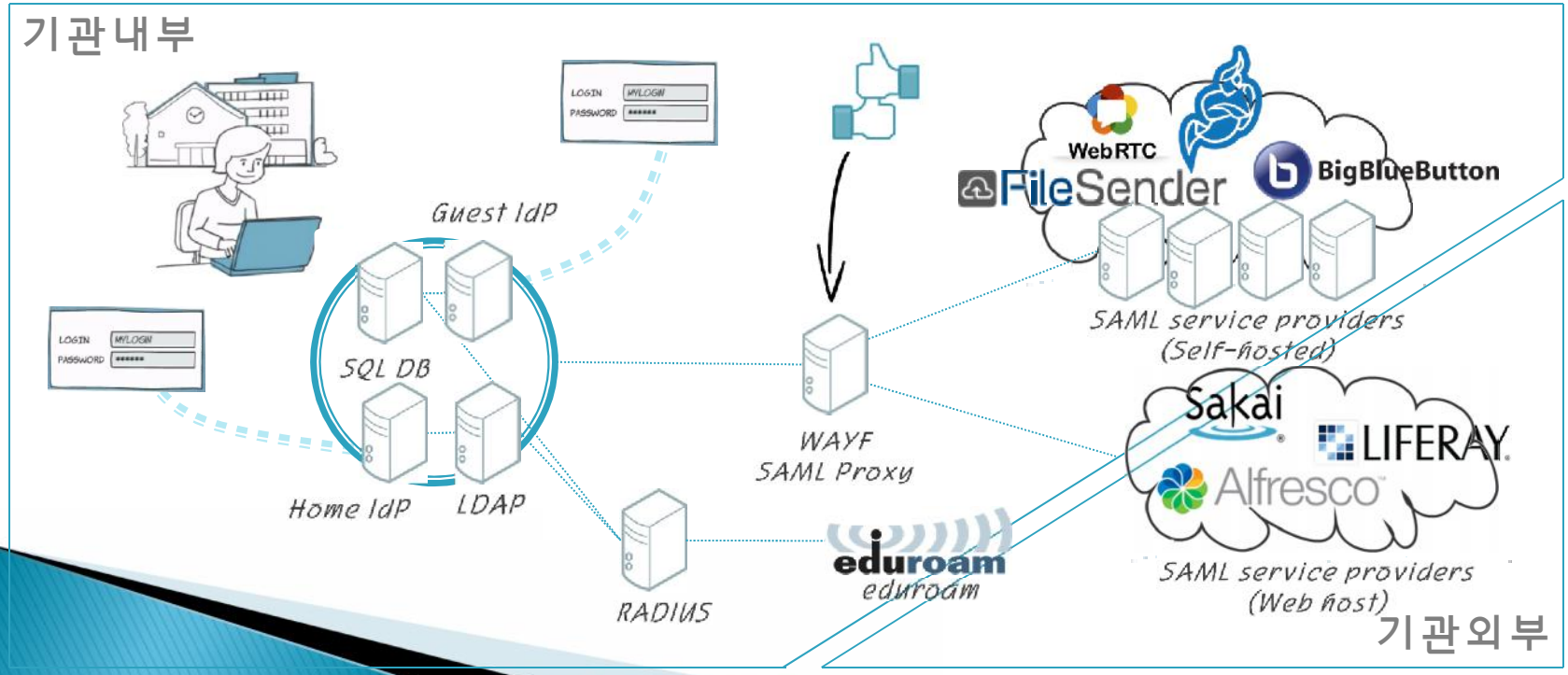
COREEN 서비스(계속)

- 현황(2015)
  - 12개 응용/서비스 (7개 SP)
  - 1 Guest IdP
  - 1 KREONET Home IdP 구축
  - ID 연계정책 수립 중
  - 39개 기관소속 사용자 이용 중



COREEN 적용 기술 및 구조 상세

- SAML 2.0
  - (주)simpleSAMLphp 기반의 IdP/SP
  - (부)Shibboleth기반의 IdP/SP 연동가능
- Federation 구조
  - (주)Full mesh
  - (부)Hub and Spoke – OpenConext 기반



KAFe에서 규정한 사용자속성 정보

- ID 제공자가 공급, 서비스 제공자가 활용

1. 핵심속성

Attribute	Schema	Notes	PIPL
eduPersonTargetedID	eduPerson	pseudonym	
displayName	inetOrgPerson	화면 표시 이름	○
mail	inetOrgPerson	사용자 이메일 주소	○
eduPersonAffiliation*	eduPerson	아래 표 참조	
organizationName*		소속기관 이름	

필수속성

2. 권고속성

Attribute	Schema	Notes	PIPL
schacHomeOrganization	SCHAC	소속기관 최상위 도메인 (ex. kafe.net)	
eduPersonPrincipalName	eduPerson	도메인 내 사용자 Identity 정보 (ex. kildong@kafe.net)	
eduPersonScopedAffiliation	eduPerson	도메인 내 사용자 직무 정보 (ex. student@ee.kafe.net)	

제공 중인 협업응용 서비스

- 자체 개발 및 제공 서비스(2015)

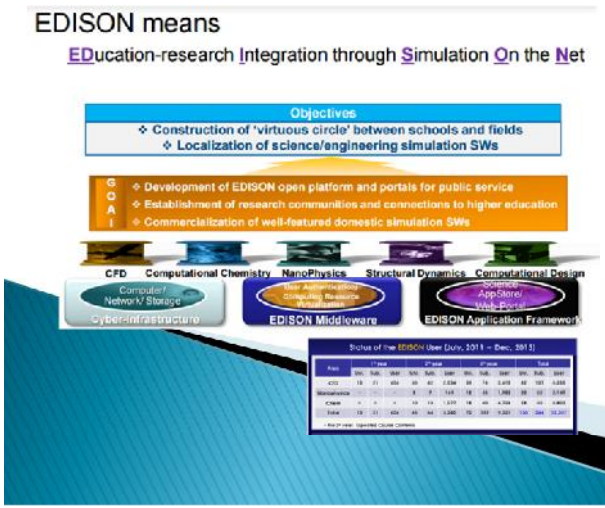
서비스 카테고리	서비스 명	ID 연계
화상회의 및 세미나	Webmeet Webinar	O
파일전송 및 저장	WebCache FileSender FileStore WebFTP	△
무선로밍	eduroam-AND	O
정보시스템(연구장비)	RealLab Emulab	예정
시간 스케쥴링 등 기타	Foodle XMPP	O

서비스 연계 시 고려사항

- 상용제품의 자체구축 및 활용 시 어려움
  - 기술지원 부족
  - 높은 가격
- 클라우드 등 국내 SW 인프라 열악
  - 제공 가능한 외부 서비스에 한계가 있음
- 상용 클라우드 서비스는 공공기관에서 이용할 수 없음
  - 클라우드 법 시행 이전(2015.9)
- 국내 사용자들이 "pay and go" 환경에 익숙하지 않음

Provider(SP,IdP) 확장 계획

- 서비스 제공자
  - KREONET/KISTI 내부 서비스 연계
    - 184개 웹 응용(지식정보/정보자산)
  - 유/무료 상용 서비스 연계
    - 14개 국내 중소업체 대상
    - Open-source 커뮤니티 협력
  - 학술정보/학습관리 서비스 연계
- ID 제공자
  - 5개 과학기술특성화대학교
    - DGIST, GIST, KAIST, UNIST, POSTECH
  - KREONET 가입 기관으로 점진적 확대
    - 산학연 192개 기관



기술개발 요구 부분

개발내용	개발이유	활용계획	완료시기
Home IdP용 ID 등록관리시스템	기관 내부 인증시스템의 IdP 연동 시 정책적, 기술적 어려움 존재	(IdP제공)기관배포	2015
WayF (Service Discovery)	보안 및 개인정보보호관련 정부규제준수, 운영인력 및 예산 등을 고려했을 때, 국내 실정에 맞는 활용가능한 WayF 서비스 존재하지 않음	국내 ID Federation 환경 적용	2016
Entity 모니터링 및 SAML연동 검증시스템	표준화된 연동 환경(속성, 메 타데이터 등)에서 IdP, SP 연결 테스트를 수행할 공용 시스템이 존재하지 않음	국내 ID Federation 환경 적용	2017
NonWeb SSO(Single Sign On) 솔루션	정보자산 활용서비스 중 상 당수는 NonWeb 환경이지만 SSO 솔루션이 부족한 상황	서비스 제공자 연계	장기

Lessons Learnt

- 참여기관 설득 문제
  - 개인정보보호 및 보안관련 정부규제 준수
    - 국정원 CC인증 및 보안성 검토
    - 클라우드 서비스의 공공기관 활용(2015년 클라우드법 시행)
- 연구/교육 기관은 대부분 SQL기반의 상용솔루션 이용
  - 기관 내부 인증솔루션에 대해 학습되어야 지원 가능
- 전문 인력 및 커뮤니티 부재
  - 대상 기관(IdP, SP)의 인력, SSO 구축업체의 SAML 관련 경험 부족, 관련 연구개발커뮤니티 및 인력 부족
- 기존 웹응용의 업그레이드 비용 (서비스제공자 기능부여)
  - 전산부서 자체인력 부족; 업체를 통해 업그레이드 수행
- 국내 웹응용 및 클라우드 서비스 업체의 수적 부족
  - 국외 클라우드 서비스(SaaS) 업체의 97%가 SAML 기반 SSO 지원
- 법적 책임 등의 정책 반영
  - 법률 자문 등 필요

결론

- 국가적 ID Federation이 필요한 상황
  - 클라우드 산업 육성, 정보자산의 국가적 공동활용
- 아쉽게, 대한민국은 시작 단계로 기술/경험 부족
- 지금은 협력해야 할 때
- 국가과학기술연구망은 협력할 준비가 되어 있습니다.