

Korean Access Federation; 2018' Update

Jinyong JO

jiny92@kisti.re.kr

25th Oct., 2018

Background

- 연합인증(Federated Authentication)
 - 보안도메인 간 사용자 인증/인가 체계 및 방법
- 계정연합/ID 연합(ID Federation)
 - 동일한 연합인증 정책을 준용하는 보안도메인의 집합

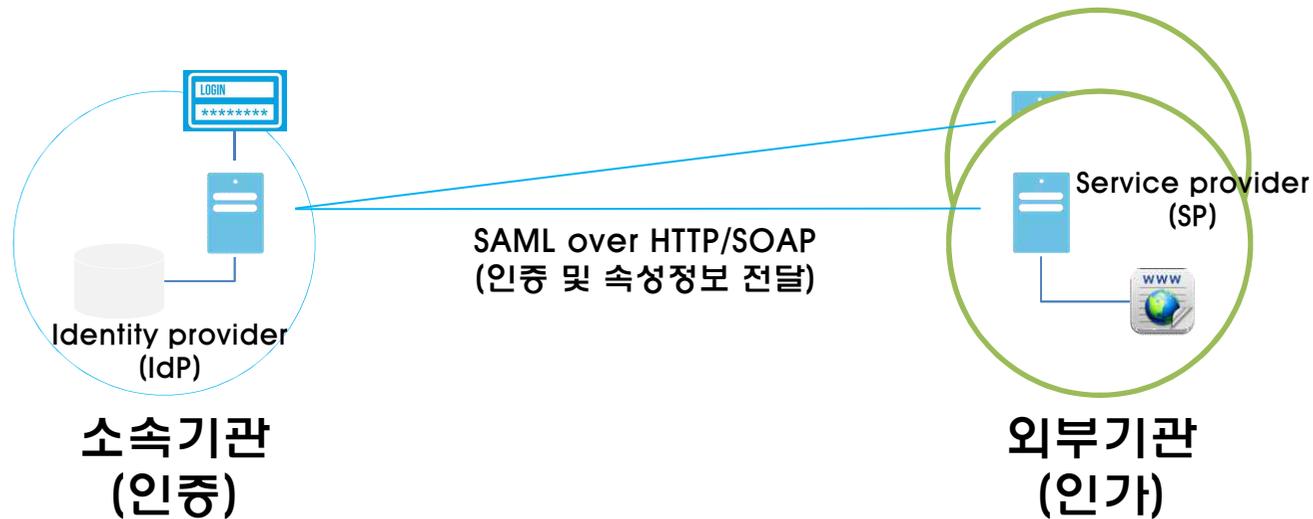
자세한 내용은 다음 주소를 참조

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

소속기관의 내 ID로 기관외부 웹 응용을 이용

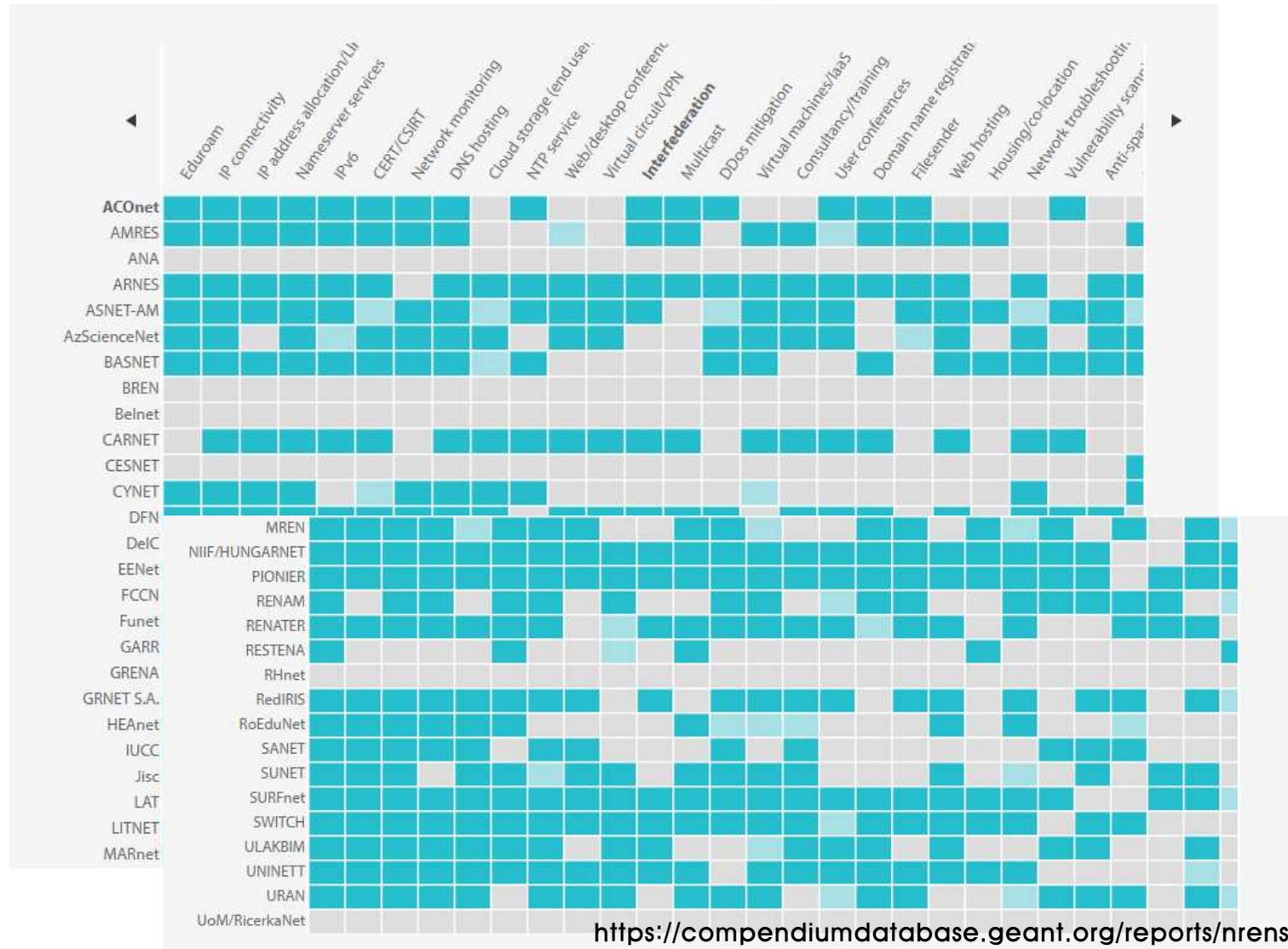
Background (Contd.)

- 소속기관의 내 ID로 기관외부 웹 응용을 이용



상대방을 어떻게 믿을 수 있는가? Metadata 교환

GEANT Compendium



https://compendiumdatabase.geant.org/reports/nrens_services

Korea Access Federation

- KAFE

- 국내 계정연합(국내 연구/교육기관, 국내외 산업체 대상)
- 국가과학기술연구망(KREONET) 운영

- History

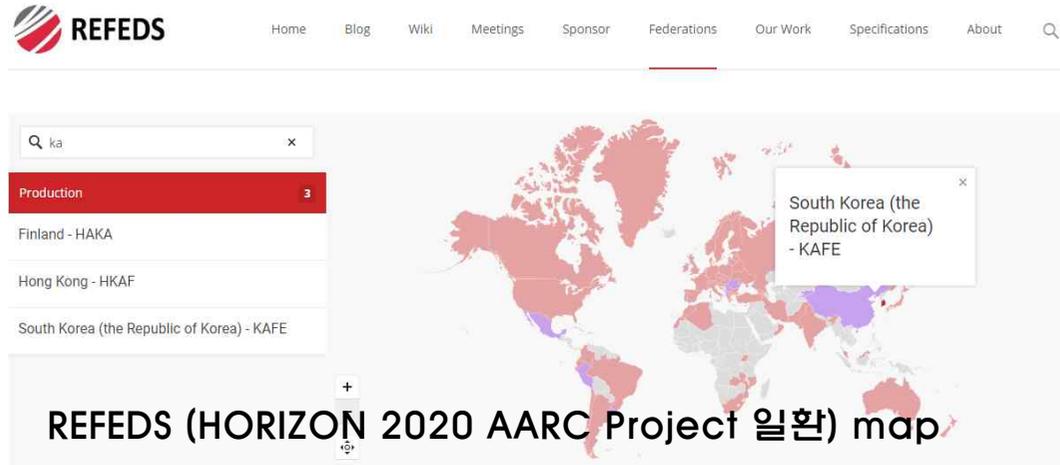


eduGAIN: 국가 간 연합인증을 가능케 하는 서비스(GEANT 운영)

KAFE (Contd.)



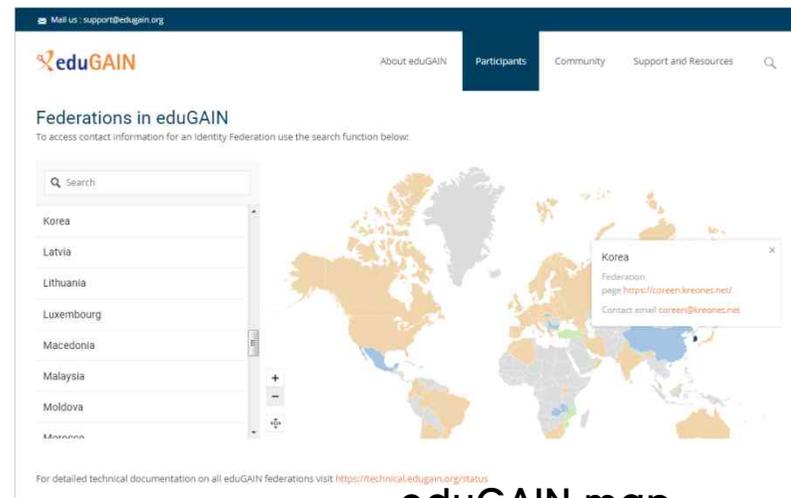
eduGAIN map (2015)



REFEDS (HORIZON 2020 AARC Project 일환) map



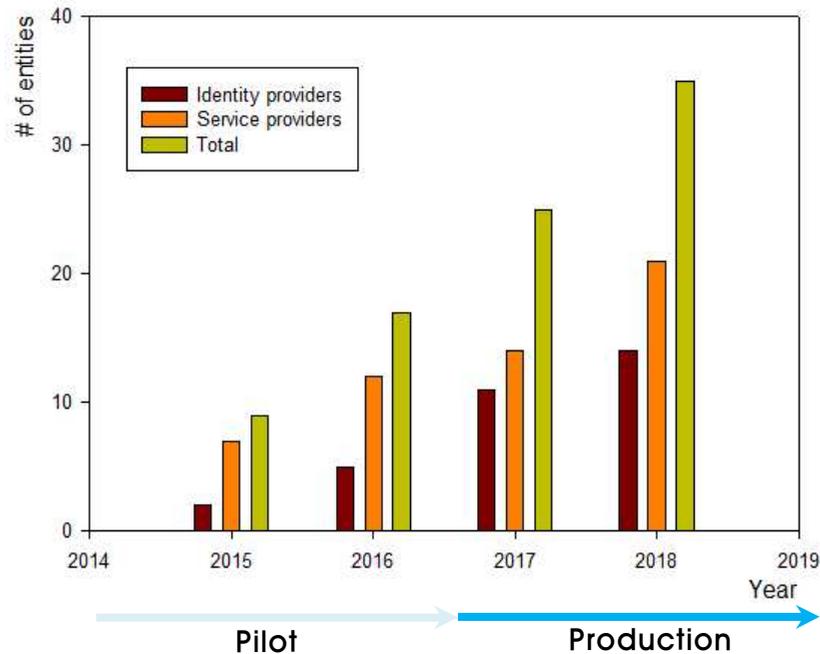
SIRTFI adoption (2017)



eduGAIN map

Growth

- 18년도 서비스 규모(17년도 대비)
 - 40 → 54 entities (eduGAIN 포함)
 - 25 → 35 entities (KAFE Production Fed.)
서울대, 천문연 등 참여
 - 8만 → 23만 federated users



Total: 66 Export ▾

NAME	COUNTRY	ENTITIES	IDP	SP	AA
InCommon Federation	United States	8761	2909	5857	5
WAYF Federation	Denmark	84	67	17	0
LAIFE Federation	Latvia	59	18	41	0
Grid Identity Pool Federation	Italy	50	8	42	0
INFED	India	44	24	20	0
LITNET FEDI Federation	Lithuania	44	19	25	0
COFRe Federation	Chile	38	6	32	0
KAFE	South Korea	35	14	21	0
CSTNet Cloud Federation	China	32	3	29	0
TAAT Federation	Estonia	26	21	5	0
FEDUrus Identity Federation	Russia	24	10	14	0
PIONIER.Id	Poland	22	12	10	0
RCTSaai Federation	Portugal	20	19	1	0
FEIDE Federation	Norway	19	1	18	0
Hong Kong Access Federation (HKAF)	Hong Kong	17	9	8	0
Sifulan	Malaysia	17	5	12	0
OMREN Federation	Oman	13	13	0	0
Singapore Access Federation (SGAF)	Singapore	10	2	7	1

Available App/Services

<p>production</p> <p>ownCloud storage</p> <p>File Transfer and Sharing</p>	<p>production</p> <p>EDISON Platform for Computational Science</p> <p>R&D Infra and Resource</p>	<p>production</p> <p>coWork PMS</p> <p>Communications</p>	<p>production</p> <p>ontheHub</p> <p>Etc.</p>	<p>production</p> <p>Elsevier Service Provider Proxy</p> <p>R&D Infra and Resource</p>	<p>production</p> <p>KAFE Web portal</p> <p>Etc.</p>
<p>production</p> <p>KREONET GitLab</p> <p>ToolBox</p>	<p>production</p> <p>FileSender</p> <p>File Transfer and Sharing</p>	<p>production</p> <p>Teatime</p> <p>ToolBox</p>	<p>edugain</p> <p>OpenAIRE</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>ORCID</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>NERD - Database of malicious entities</p> <p>Etc.</p>
<p>production</p> <p>vidyo</p> <p>Communications</p>	<p>production</p> <p>eduroam-AND</p> <p>R&D Infra and Resource</p>	<p>production</p> <p>WebCache</p> <p>File Transfer and Sharing</p>	<p>edugain</p> <p>CloudStor</p> <p>File Transfer and Sharing</p>	<p>edugain</p> <p>Worldwide LHC Computing Grid</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>GEANT mailing list</p> <p>Communications</p>
<p>production</p> <p>Webinar</p> <p>Communications</p>	<p>production</p> <p>Webmeet</p> <p>Communications</p>	<p>production</p> <p>IEEE Xplore</p> <p>Etc.</p>	<p>edugain</p> <p>Indico</p> <p>ToolBox</p>	<p>edugain</p> <p>Okeanos-global</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>CERN</p> <p>R&D Infra and Resource</p>
<p>production</p> <p>Atlases - PATHOLOGY IMAGES</p> <p>R&D Infra and Resource</p>	<p>production</p> <p>MyUniDAYS</p> <p>Etc.</p>	<p>production</p> <p>Test your Identity Provider</p> <p>Etc.</p>	<p>edugain</p> <p>LIGO</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>Internet2 Wiki</p> <p>ToolBox</p>	<p>edugain</p> <p>Globus Online</p> <p>File Transfer and Sharing</p>
<p>edugain</p> <p>TERENA SP Proxy</p> <p>Etc.</p>	<p>edugain</p> <p>DataONE</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>OOI</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>vi-seem</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>OpenMinted</p> <p>R&D Infra and Resource</p>	<p>edugain</p> <p>EGI</p> <p>R&D Infra and Resource</p>

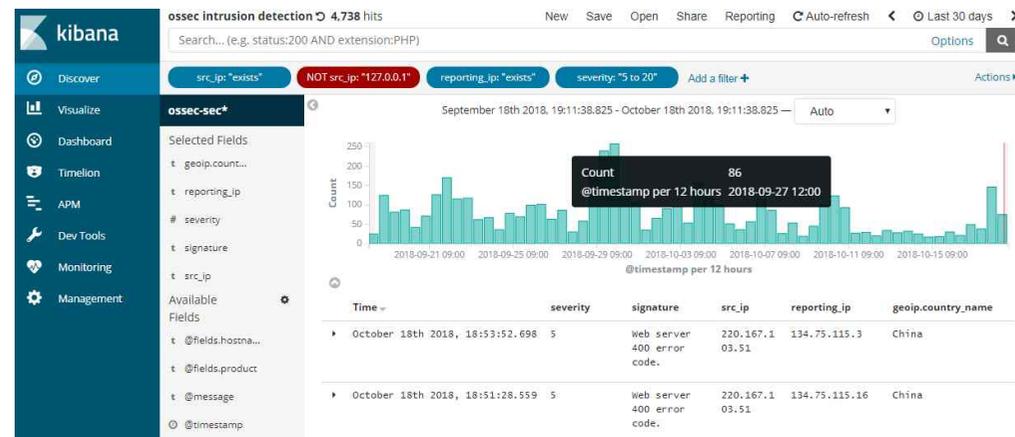
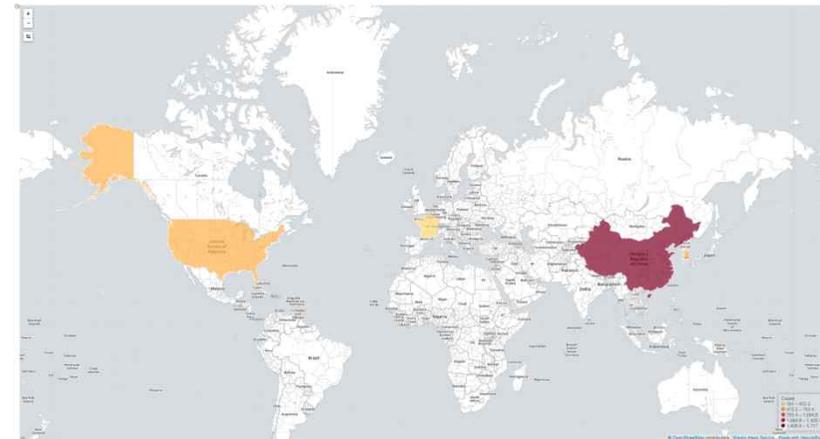
<https://www.kafe.or.kr/collaboration#/>

Interoperation/Compliance

- KAFE SW package 적용 완료(2018 배포판)
 - Inter-federation
 - Research and scholarship category
 - SIRTFI category
 - Name format: 우리는 CN만, 저들은 GN과 SN을
 - Compliance
 - 정보통신망법/개인정보보호법
 - 전자적 사용자동의 기능
 - eduGAIN import policy 적용 (필터링 자동화)
- Policy profile (on-going)
 - KAFE baseline LoA
- 자체 속성 정의(한글 속성)
 - KAFE 부가속성을 추가적으로 정의 함
(<https://www.kafe.or.kr/attributeMap> 참조)

Operation/Monitoring

- 40 VMs on 9 Physical Machines (app server 포함)
 - Vmware ESXi hosts 이용
 - High availability
 - Best effort or with HAproxy (vCenter HA 또는 Kubernetes로 전환 계획 중)
 - Weekly VM backup
- Host/process monitoring
 - Zabbix 이용
- Security concern
 - Physical + Software firewall/IPS
 - OSSEC과 Elastic stack을 이용해 모니터링
- Entity monitoring
 - SSL, NTP, availability
- Usage status monitoring



Organization Support

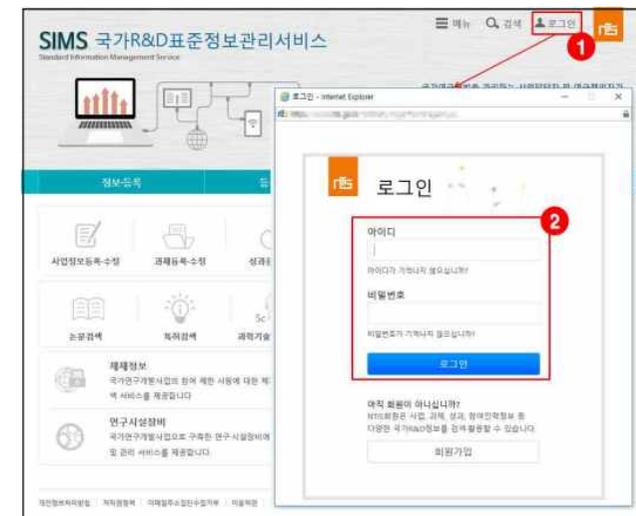
- ID 제공자
 - simplesamlphp SAML 소프트웨어
 - KAFE staff 직접 지원(1-2일* 완료가능)
* <https://www.kafe.or.kr/services> 구비 시
- 서비스제공자(SAML Integration)
 - KAFE staff 간접 지원(1-6개월 소요)
 - Shibboleth
 - Apache (WS) and/or Tomcat (WAS)
 - simplesamlphp
 - PHP app on Apache (WS)
 - Spring security SAML extension
- KAFE manpower 30~40% 소비
 - 향후, 직접지원 비중을 줄이고 업체 통한 자가개발 유도 예정

KAFE for Data Content

- E-Journal
 - IEEEExplore (2018.5)
 - Elsevier – ScienceDirect, Mendeley (2018.9)
 - Web of Science, ACM, etc. (on-going)
- 문제점
 - eduGAIN 메타데이터 이용불가(opt-in policy, 국내법 등)
 - Bi-lateral agreement, 시간이 오래 걸림(최소 3~6개월)
 - 3자(ID 제공자, 서비스제공자, KAFE) 간 모두연동 필요
 - 비 상용 응용의 경우, ID 제공자와 서비스제공자가 직접 연동되지 않음
 - 사용자 별 이용통계 수집 불가
 - eduPersonTargetedID 또는 eduPersonEntitlement만 수집
- 계획
 - KAFE IdP SW package에 이용통계 수집SW 추가 예정

KAFE for Data Science

- Open Data Platform(가칭)
 - OpenAIRE-like 데이터 수집 및 분석 플랫폼
 - Spring security SAML 연동 및 인증기능 검증 완료
 - 당해년도 KAFE 등록 기대
- 연구데이터 플랫폼(가칭)
 - 연구도메인 별 특화된 데이터 Repository(25개 연구원 대상)
 - 진행 예정
- NTIS(과학기술지식정보서비스) 성과물 등록 서비스
 - 성과물 등록을 위해 최대 12개 응용서비스(기관)에 사용자 계정 생성 필요
 - 연합인증(NTIS 계정만 사용)을 통해 ID/password fatigue를 줄이고자 함
 - 당해년도 2개 기관(KISTI, KBSI) 연동 완료 기대(11월 말 예상)



KAFE for Computational Science

- EDISON 계산과학 플랫폼(2018. 4)
 - 계산과학시뮬레이션 서비스
 - 서비스접근성 향상 및 타 과학기술응용서비스와 통합가능성 제고 목적
 - Shibboleth와 Liferay plugin 제공
- MathWorks
 - MathWorks Korea의 요청에 의해 진행
 - 연합인증을 통한 Matlab 이용환경 제공
 - 진행 중



EDISON

Enter Your ID

Enter Your Password

로그인

KAFE

아이디 찾기 비밀번호 찾기

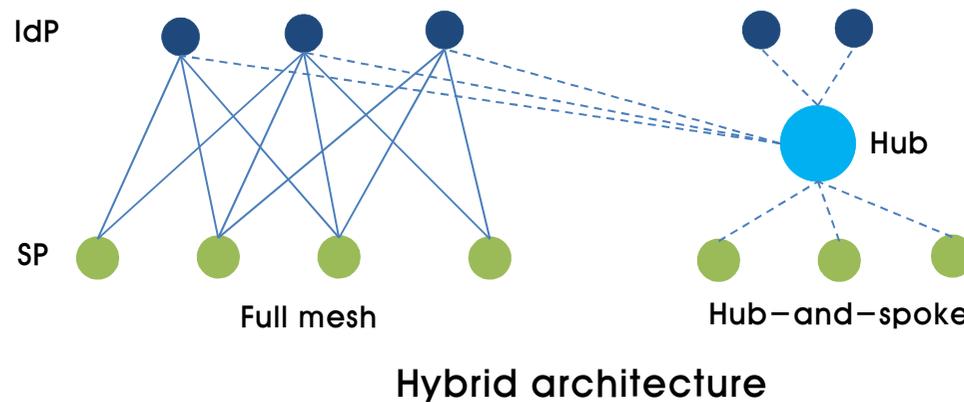
회원가입

Problems of SAML integration

- 웹 서비스제공 환경의 이질성
 - Apache Web Server +
 - Tomcat WAS(Web Application Server)
 - JEUS WAS
 - WebtoB Web Server +
 - JEUS WAS
 - Tomcat only
 - 전자정부 프레임워크(Java Spring Framework)
- 기존 로컬 인증체계(SSO 등)와 충돌
 - 개발자 숙련도 문제
- 통합 방법
 - Shibboleth + mod_ajp(상대적으로 쉽지만 적용가능 대상이 많지 않음)
 - Spring security SAML extensions

Architectural Change

- Full mesh to Hybrid
 - Full mesh with hub-and-spoke
- 이유
 - (SP)유관 소프트웨어 산업 기술력 낮음
 - (IDP)기관 IT 부서의 개발/구축 능력 편차 심함
 - (TTF)기술지원 부하경감
- 방향
 - 종단은 가볍게, 중앙은 무겁게



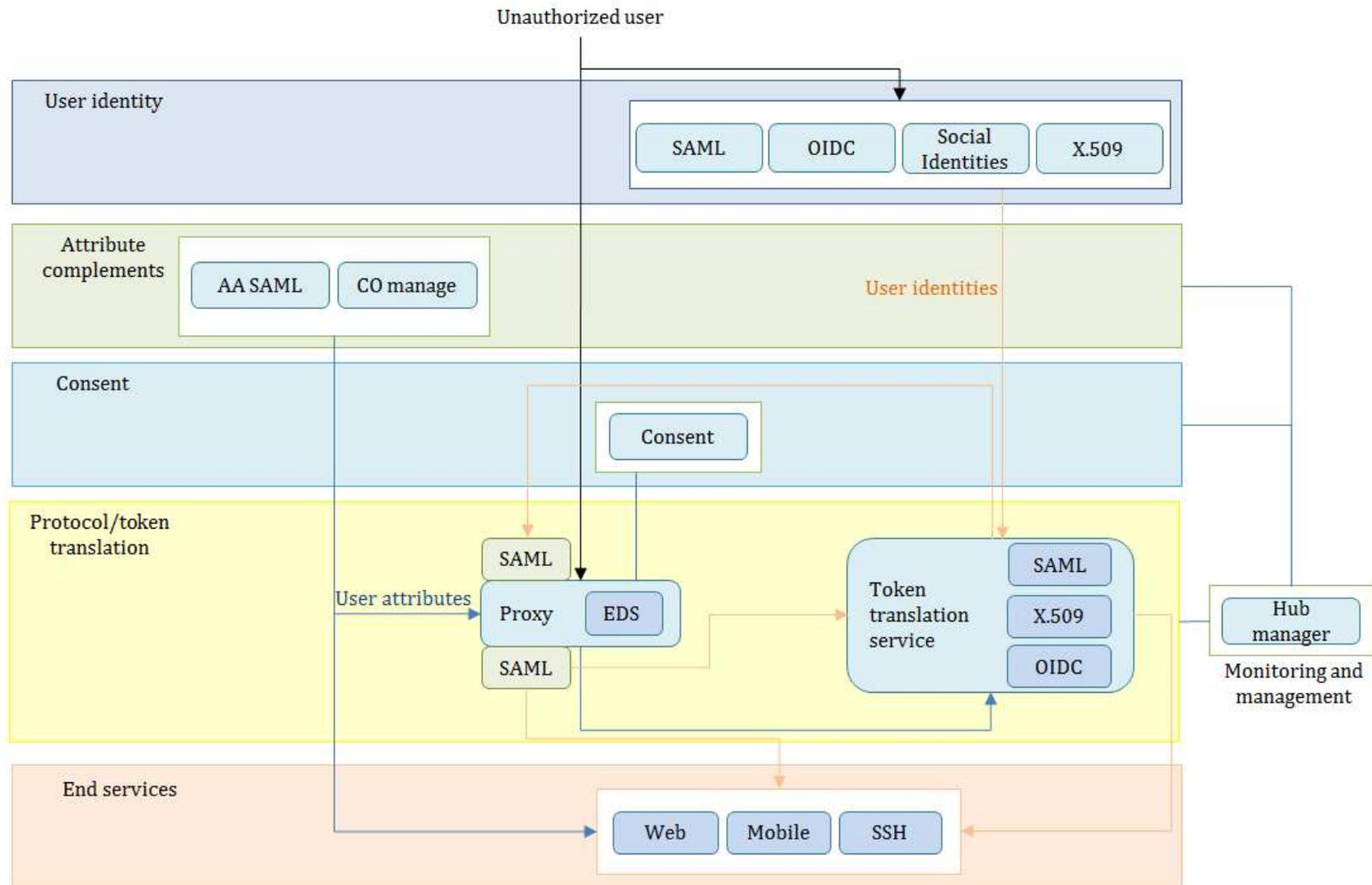
Hub Development

- Research Collaboration Zone
 - Hub 시스템의 이름
 - 3년 개발계획 중 1년 완료
 - Reference model: NSF CILogon 프로젝트
- User/Organization feedback
 - OIDC adoption
 - SAML이 너무 어려워요. 시스템 통합하는데 시간이 너무 많이 걸려요. 내년에도 기관 지원을 해야 하나요?
 - Social login
 - 우리는 소셜 로그인을 이용할 거예요. 그런데 통합비용이 비싸요.
 - Attribute(group/entitlement) management
 - Openstack group 관리하는 방법이 있나요? 상용서비스는 이용권 한 제어가 어렵네요(이용권한을 부여하고 싶은데 all or nothing이네요).
- Our need
 - Non web browser apps (e.g., SSH)

Research Collaboration Zone

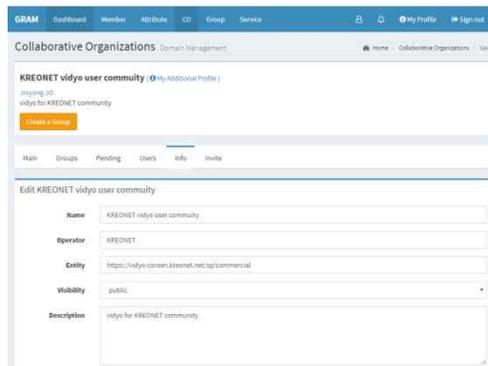
- **Key challenging**
 - **Token translation**
 - SAML ↔ OIDC/OAuth/REST
 - **Component interfacing/control**
 - Social login, IdP proxying, Attribute authority, SAML–OIDC proxying, **User consent**, Embedded discovery, etc

rZONE Architecture

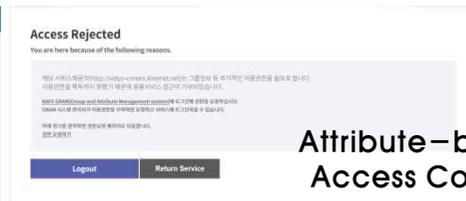


1st year Output

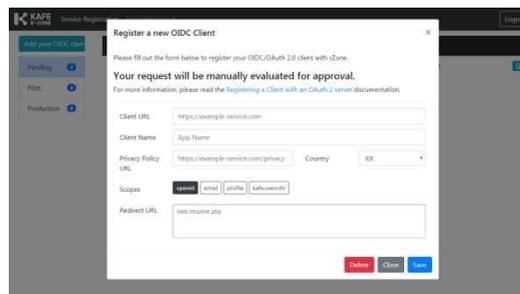
- **OIDC adoption**
 - OIDC provider: pilot ready
- **Social Login**
 - Google (NIST LoA 0)
 - Naver (LoA 문제발생 시, ORCID로 변환 계획)
 - 화상회의(Webmeet, Webinar) 서비스 Social login 허용 예정
- **GRAM attribute management**
 - Entitlement-based access control
 - Vidyo 서비스(화상회의) 대상 서비스 적용



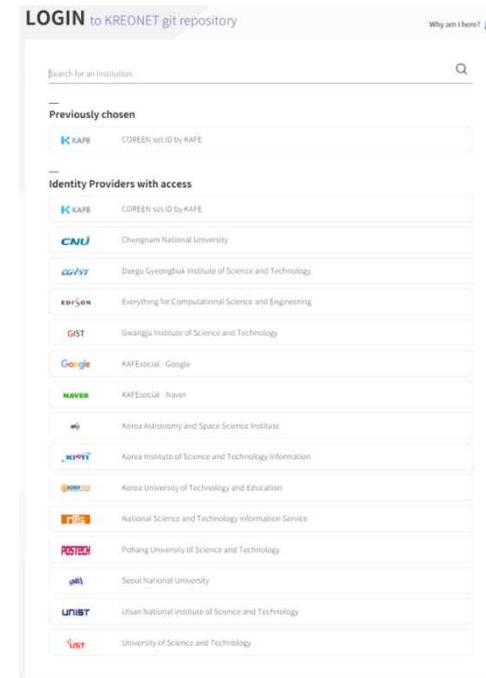
Attribute Authority
(KAFE GRAM)



Attribute-based
Access Control



OIDC client registration



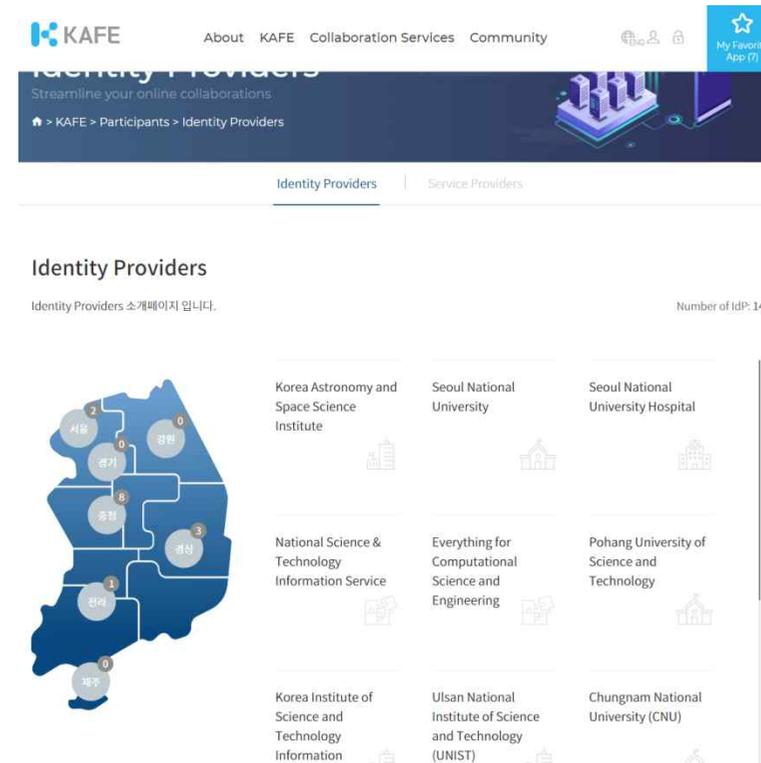
Social login support

rZONE Next

- Non-web 환경 지원 (-2020)
 - X.509, SSHkey 예정
 - Oauth for Myproxy, SSH key management, ECP(Enhanced Client or Proxy) 대상 기술분석 중

Etc.

- KAFE portal update
 - 연구협업 응용서비스 → 계정연합 서비스
 - 회원기관 등급별 서비스이용기준 차별화
 - 개인화
- 도메인 통합
 - 중립성 확보 차원
 - {coreen, kafe}.kreonet.net → kafe.or.kr



To-do

- E-journal/교육용 온라인 서비스 수용 확대
- OIDC 관련 기능 프로덕션화
- OIDC 및 GRAM 관련 Best Practices 확보
 - JupyterHub, Kubernetes, OpenStack 대상
- Non-Web 지원 시스템 프로토타입 개발
 - SSH Key and/or X509 PKI