논문 18-43-12-26 The Journal of Korean Institute of Communications and Information Sciences '18-12 Vol.43 No.12
https://doi.org/10.7840/kics.2018.43.12.2200

KAFE 계정연합의 연합인증 서비스

조 진 용◆, 장 희 진*, 공 정 욱*, 채 영 훈*

Federated IAM Service of KAFE Identity Federation

Jinyong Jo◆, Heejin Jang*, JongUk Kong*, Yeonghun Chae*

요 약

연합인증은 멀티도메인 간에 수행되는 사용자 인증과 인가체계이다. 연합인증 체계가 수립되면 소속기관의 사용자계정을 이용해 타 기관의 온라인 자원에 접속할 수 있게 된다. 계정연합은 연합인증을 관리하기 위한 국가단위 연합체로써 연합체에 속한 개체들 간에 신뢰관계를 구축하는 역할을 한다. 패스워드 피로도의 감소와 개인정보보호의 강화 및 연구자원의 공동활용 가능성 증대와 같은 효과로 인해 세계 70여개 국가에서 자국 내 계정연합을 확보하고 있다. 우리나라도 2015년부터 KAFE 계정연합을 운영 중이다. 하지만 연합인증 기술 활용을 위한 기반 소프트웨어 산업의 생태가 열악하기 때문에 연합인증의 활용과 확산이 더디게 진행되고 있다. 본 논문은 연합인증에 대해서 소개하고 시스템 구성요소와 구현방법에 대해서 설명한다. 또한, KAFE 계정연합에서 개발한 사용자계정 관리, 메타데이터 관리, 개체 탐색, 사용자 동의 및 상태 모니터링 서비스의 세부 설계와 구현에 대해서 다룸으로써 국내 연구 및 교육기관과 산업체 등에서 연합인증을 이해하고 활용하는데 기여하고자 한다. 마지막으로, 구현결과를 정성적으로 평가한다.

Key Words : Federated IAM, Identity federation, SAML, Trust relationship

ABSTRACT

Federated IAM (Identity and Access Management) is an authentication and authorization scheme that is performed among multiple security domains. Once the federation is made in the domains, users can access the online resources of other organizations using their home organizational accounts. Identity federation is an union of the domains for managing the federated IAM, and its main role is to make them build trust relationship. More than 70 countries around the world have their own identity federations because of its benefits such as the reduction of password fatigue, strengthening of personal information protection, and increasing the possibility of share of online resources. In Korea, KAFE (Korean Access FEderation) identity federation is operating since 2015. However, due to the poor domestic ecosystem regarding the federated IAM, the proliferation of the scheme is progressing slowly. This paper introduces the federated IAM including the description of its system components. In addition, this paper deals with the detailed design and implementation of our federation services to encourage institutions and higher education in Korea understand and adopt the federated IAM more. Finally, the implementation results are qualitatively evaluated.

※ 본 연구는 한국과학기술정보연구원의 지원으로 수행되었습니다.

◆ First Author : (ORCID:0000-0001-6830-3604)Korea Institute of Science and Technology Information, Advanced KREONET Center, jiny92@kisti.re.kr, 정회원

* Korea Institute of Science and Technology Information, Advanced KREONET Center, jhj@kisti.re.kr, kju@kisti.re.kr, 정회원, proin@kisti.re.kr

논문번호 : 201810-312-D-RU, Received September 20, 2018; Revised November 15, 2018; Accepted November 16, 2018

Ⅰ. 서 론

연합인증(Federated identity and access management[1])은 다수의 보안도메인 사이에서 이루어지는 사용자 인증(Authentication)과 인가(Authorization) 체계이다. 학교나 연구소와 같은 개별기관 내부에서 수행되었던 인증·인가체계를 기관 외부까지 확장할 수 있도록 표준화해 적용함으로써 비밀번호 피로도(Password fatigue)를 낮추고 개인정보의 이용을 최소화할 수 있다. 또한 타 기관에서 제공하는 연구데이터와 디지털자원(예, 컴퓨팅 및 스토리지 자원)을 표준 인증체계를 통해 접근케 함으로써 기관 간 연구자원의 공유에도 효과적이다. 예를 들어, A 연구소의 연구원이 소속기관에서 이용하는 포털 계정(사용자 ID와 비밀번호)을 이용해 B 대학에서 제공하는 오픈스택 서비스[2], 컴퓨팅자원[3], 연구데이터[4] 등에 자유롭게 로그인할 수 있게 된다.

계정연합(Identity federation)은 그림 1과 같이 연합인증이 가능한 개체(Service provider 및 Identity provider)들과 제3신뢰기관(Trusted 3rd party)으로 구성된 연합체를 의미한다. 제3신뢰기관은 계정연합을 거버넌스하며 중립성 확보를 위해 각 국가의 연구교육망이 담당하는 것이 일반적이다. 인증·인가를 위한 메시지는 식별경로(Identity path)를 통해서 개체들 간에 교환되며 메타데이터 등 부가정보는 신뢰경로(Trust path)를 통해 배포된다. 제 3신뢰기관은 기본적으로 신뢰경로에서 부가정보의 교환을 담당하며 추가적으로 식별경로를 관리할 수 있다. 식별정보제공자(Identity provider)는 사용자를 인증하고 서비스제공자(Service provider)는 식별정보제공자가 인증한 사용자를 대상으로 디지털자원에 대한 접근권한을 부여한다. 연구기관과 교육기관이 식별정보제공자에 해당된다. 하나의 계정연합은 동일한 정책과 기술 프로파일을 준용하기 때문에 관리주체가 다른 연구자원들도 표준에 따라 용이하게 통합할 수 있다.

국제연구교육연합(REFEDS[5], the Research and Education REDerations group)에 의하면 2018년 중반기 현재 전 세계 70여개 국가에서 자국 내 교육기관과 연구기관을 대상으로 연합인증 서비스를 제공하고 있다. 미국은 국립과학재단(NSF, National Science Foundation)의 사이버인프라 프로그램을 통해 InCommon[6] 계정연합을 지원하고 있다. 연구자원에 대한 접근성(Accessibility)과 이용편의성(Usability) 및 공동활용(Share) 가능성을 높이기 위해 500여 식별정보제공자와 4,300여 서비스제공자가 InCommon 계정연합에 참여하고 있는 상황이다. 일본도 2009년부터 Gakunin[7] 계정연합을 출범하고 자국 내 교육기관을 대상으로 연합인증 서비스를 제공하고 있다. 일본 내 국립대학의 90%이상이 Gakunin에 참여하고 있으며 전자저널을 중심으로 약 90여 서비스제공자를 확보하고 있다.

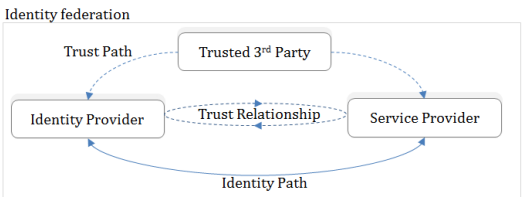

그림 1. 계정연합의 개요
Fig. 1. Brief overview of identity federation

우리나라는 2000년대 중반부터 한국전자통신연구원(ETRI)에 의해 연합인증과 관련된 기술이 개발되었지만[8] 범용서비스로는 확대되지 못하다가 2016년 국가과학기술연구망(KREONET)에 의해 국내 최초의 계정연합인 KAFE(Korean Access FEderation[9])가 출범되었다. KAFE는 현재 국가 간 계정연합인 eduGAIN[10]의 정식 회원으로써 전 세계 52개 국가와 호환되는 연합인증 체계를 갖추고 있다. 본 논문은 신뢰경로와 식별경로를 관리·제어하기 위해 개발된 KAFE 계정연합의 내부 시스템구조를 자세히 소개한다. 국가별 계정연합이 유사한 내부구조를 가지고 있을 것으로 예상되지만, 구성요소가 단편적으로만 공개되어 있어 전체 구조를 파악하는데 한계가 있다. 또한 국가마다 개인정보보호법이 상이하기 때문에 연합인증 서비스를 구성하는 개별 기능요소에도 차이가 존재한다. 본 논문은 KAFE 계정연합의 내부 시스템구조에 대해 체계적으로 소개한 최초의 논문이라는 점에서 의의를 갖는다.

본 논문은 다음과 같이 구성되어 있다. 제 2장에서는 KAFE 계정연합의 연합인증 서비스 구조를 설명한다. 연합인증 개체의 구현방법에 대해서는 제 3장에서 소개한다. 제 4장에서 연합인증 서비스 제공을 위해 개발된 핵심 시스템들을 살펴본 후 제 5장에서 구현결과를 통해 개발 시스템들을 정성적으로 평가한다. 마지막으로 제 6장에서 결론을 맺는다.

Ⅱ. 연합인증의 구조

본 장에서는 KAFE 계정연합에서 연합인증 서비스의 제공과 이용을 위해 구성되는 식별경로 및 신뢰경

로에 대해서 소개하고 개체 간에 교환되는 정보의 처리절차를 간략히 살펴본다. 연합인증에서 신뢰경로와 식별경로의 관리·제어를 위해서는 다수의 시스템 구성요소들이 조화롭게 동작해야 한다. 본 논문에서는 개별 구성요소들을 유사한 연구들과 단순 비교하는 것을 지양하고 시스템의 구조를 전체적으로 소개하는 데 초점을 둔다.

2.1 식별경로(Identity Path)

연합인증은 SAML(Security Assertion Markup Language[11]) 규약을 준용한다. SAML은 식별정보제공자와 서비스제공자 간에 인증 및 인가정보를 교환하기 위한 XML 기반의 공개표준 데이터 포맷이다. 본 논문에서 식별경로는 SAML 인증요청(AuthnRequest)부터 인증응답(AuthnResponse)을 처리하는 전체 과정으로 정의한다. SAML은 웹 브라우저 SSO(Single Sign On) 프로파일을 지원하기 위해서 HTTP Redirect 바인딩이나 HTTP POST 바인딩을 이용한다. 또한 SOAP(Simple Object Access Protocol) 바인딩을 통해 서버 간 통신이 가능하다. 사용자에 대한 인증정보는 식별정보제공자가 생성한 어설션(Assertion)에 포함되어 서비스제공자에게 전달된다. 어설션은 '누가', '언제', '어떤 식별정보제공자'를 통해 인증되었으며 '어떤 속성정보'가 '어떤 서비스제공자'에게 유효한지를 단언한다.

그림 2는 KAFE 연합인증 서비스에서 사용자를 인증·인가하는 전체 과정을 간략히 도시화한 그림이다. 본 논문에서 연합인증 서비스는 계정연합에 포함된 개체들에게 제3신뢰기관이 제공하는 페더레이션 서비스를 의미한다. 먼저, 사용자는 디지털자원에 접근하기 위해 서비스제공자에게 로그인을 요청한다. 연합인증 환경에서 사용자는 자신의 소속기관(또는 계정정보를 저장하고 있는 조직)을 통해 인증을 받기 때문에 탐색서비스(Discovery Service)를 통해 소속기관을 선택해야 한다. 탐색서비스는 계정연합에서 제공하는 중앙형(Central) 탐색서비스와 서비스제공자가 자체적으로 구현한 내장형(Embedded) 탐색서비스로 구분할 수 있다. 일반적으로 연합인증 서비스 구조가 풀 매시[12]일 경우에는 내장형 탐색서비스를 이용한다. 중앙형 탐색서비스를 이용하면 서비스제공자가 내장형 탐색서비스를 구현하지 않아도 된다는 장점이 있지만 단일 장애점(Single point of failure) 문제가 단점으로 작용할 수 있다. 서비스제공자가 하나의 식별정보제공자만을 이용하고자 한다면 탐색서비스는 필요치 않다.

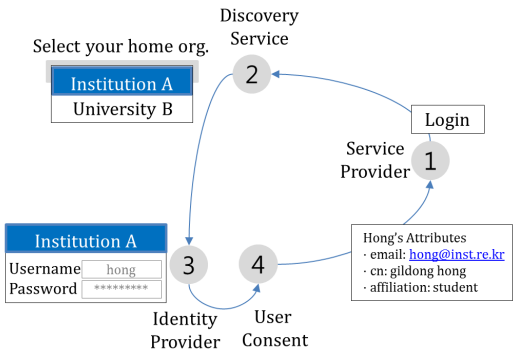

그림 2. 식별경로에서 수행되는 인증절차의 개념도
Fig. 2. Simplified view of authentication flow on Identity path

웹 브라우저는 선택된 식별정보제공자에게 SSO 서비스를 요청하게 되고 사용자는 해당 식별정보제공자에서 크리덴셜(예, 사용자 ID와 비밀번호)을 입력해 사용자 인증을 받게 된다. 인증에 성공한 사용자의 속성(Attributes) 정보는 어설션에 포함되어 서비스제공자에게 전달되며, 서비스제공자는 전달받은 인증정보와 속성정보를 이용해 제공하는 디지털자원의 이용권한을 부여한다. 즉, 식별정보제공자와 서비스제공자는 각각 사용자 인증과 인가를 담당한다. 식별정보제공자가 사용자 크리덴셜을 관리하기 때문에 서비스마다 사용자계정을 생성할 필요가 없다. 국내 개인정보보호법과 정보통신망법은 개인정보(사용자의 속성 정보)를 제3자에게 제공할 경우에 반드시 사용자동의(User consent)를 받도록 규정하고 있다. KAFE 계정연합에 참여하는 모든 식별정보제공자는 전자적 방법을 이용해 사용자동의를 구하고 있다.

2.2 신뢰경로(Trust Path)

연합인증에서는 개체 간에 SAML 메타데이터를 교환함으로써 신뢰관계를 확보한다. 신뢰관계가 사전에 확보되지 않은 개체 간(예, 식별정보제공자와 서비스제공자)에는 식별경로 상의 인증요청과 인증응답이 교환될 수 없다. 본 논문에서 신뢰경로는 SAML 메타데이터를 수집, 서명, 배포하는 전체과정을 의미한다. SAML 메타데이터는 개체식별자(EntityID)와 공개키 및 프로토콜 접속점(Protocol endpoints)을 필수적으로 포함하는 XML 파일이다. 계정연합에 참여하는 모든 개체들은 개체식별자로 정의된 고유 식별자를 갖는다. 인증처리 과정에서 제공자는 개인키를 이용해 SAML 메시지에 전자적으로 서명할 수 있다. 메시지 수신자는 메타데이터에 포함된 공개키를 이용해 전자서명을 검증한다. 또한 공개키는 SAML 메시지를 암호화하는데 이용될 수 있다. 서명 또는 암호화된

SAML 메시지는 메타데이터에 포함된 접속점 URL 주소로 송신된다.

SAML 메타데이터는 확장(Extensions)정보로써 계정연합의 고유식별자, 발행정보, 개체 분류자(Entity Category), 발행기관 및 연락처 등을 포함할 수 있다.

그림 3은 KAFE 계정연합이 SAML 메타데이터를 수집하고 배포하는 과정을 간략히 보여준다. KAFE는 eduGAIN의 정회원으로써 국외 계정연합(Inter-federation)에서 제공하는 서비스제공자와 식별정보제공자의 SAML 메타데이터를 수용(Metadata Aggregator)하고 있다. 따라서 사용자는 연합인증을 통해 국외 서비스 제공자가 제공하는 디지털자원에도 로그인이 가능한 상태이다. 국외 SAML 메타데이터는 KAFE 메타데이터 수용정책에 따라 선별적으로 수용되고 있다.

식별정보제공자와 서비스제공자가 SAML 메타데이터를 개별적으로 교환하면 기술호환성이 낮아지고 정책의 준용여부를 검증하기 어렵기 때문에 KAFE는 자체 메타데이터 등록서비스(Metadata Registry)를 통해 참여 개체의 SAML 메타데이터를 수집 및 검증한 후 일괄 배포 하고 있다. KAFE에 참여하는 모든 개체들은 SAML 메타데이터를 계정연합에 제출해야 한다. 계정연합의 관리자는 메타데이터의 정책준용 여부를 검증한 후 메타데이터 등록서비스에 기록한다. 메타데이터 등록서비스는 등록된 SAML 메타데이터를 주기적으로 취합하고 전자적으로 서명하며 배포 URL을 통해 연합 메타데이터(Federation metadata)를 발행한다.

KAFE 참여개체와 계정연합의 주요 시스템(예, 탐색서비스)들은 연합 메타데이터를 주기적으로 다운로드받아 인증요청과 인증응답에 활용함으로써 참여 개체들 간에 신뢰관계를 구축한다.

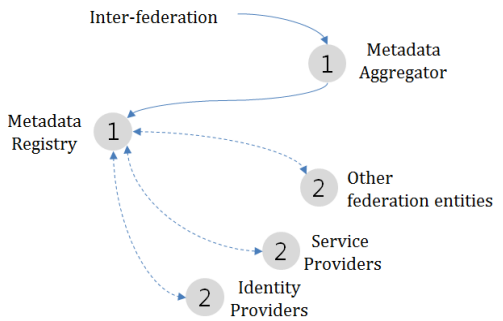

그림 3. 신뢰경로에서 수행되는 메타데이터 배포절차의 개념도
Fig. 3. Simplified view of metadata distribution flow on Trust path

Ⅲ. SAML 개체의 구현

계정연합에 가입하고자 하는 식별정보제공자와 서비스제공자는 각각 인증처리를 위해 게이트웨이 서버를 구축하거나 웹 응용서비스(디지털자원)에 SAML 기능을 통합해야 한다. 본 장에서는 게이트웨이 서버의 역할과 SAML 규약의 웹 응용서비스 연동방법에 대해서 소개한다. 지면 제약 상 자세한 설명은 생략한다.

식별정보제공자의 주요 기능은 사용자로부터 크리덴셜을 입력받아 해당 사용자를 인증하고, 사용자 데이터베이스(Backend user DB)로부터 인증된 사용자의 속성정보를 얻어와 표준 속성형태에 맞게 변환한 후, 서비스제공자에게 전달하는 것이다. 사용자 속성정보의 제3자 제공에 대한 동의 여부와 동의 로그의 관리도 식별정보제공자의 주요 기능이다. 또한 식별정보제공자는 서비스제공자에게 전달해야하는 사용자속성의 필터링과 추가적인 속성의 생성을 담당한다. 서비스제공자($s \in S$)가 요구하는 사용자속성의 집합을 A_s, 식별정보제공자($i \in I$)가 제공하는 사용자속성의 집합을 A_i라고 한다면 i는 s의 요청에 의해 $A_p = A_i \cap A_s$인 사용자 속성을 제공한다. 하나의 계정연합에 포함된 서비스제공자와 식별정보제공자의 집합을 각각 S와 I로 표기한다. 서비스제공자의 SAML 메타데이터는 요구속성(A_s)을 명시하고 있다.

KAFE에 참여하는 개체에게는 표 1과 같은 핵심속성의 이용이 권장된다. eduPersonTargetedID는 사용자의 고유식별자로써 목적한(targeted) 서비스제공자에서만 유효하다. 식별정보제공자 및 서비스제공자의 개체식별자와 사용자의 고유식별자를 조합해 해싱한 값이다(예, d74f17c949df30). eduPersonPrincipalName은 계정연합에 속한 모든 서비스제공자에서 유효한 사용자의 고유식별자이다. 식별자와 범주(예,

표 1. KAFE 계정연합의 핵심속성
Table 1. Core attributes of KAFE federation

Attribute name	Attribute value
cn	common name
displayName	display name
mail	email address
eduPersonTargetedID	Unique identifier of a user
eduPersonPrincipalName	Globally unique identifier of a user

7c949df30@kafe.kr)의 형태로 표현된다.

SAML 개체를 구현하기 위해 다양한 SAML 공개 소프트웨어들이 활용되고 있다.[13,14] 식별정보제공자는 게이트웨이 서버가 구축되어야 하며 서비스제공자는 SAML 규약을 지원해야 한다. 연구 및 교육 분야의 계정연합에서는 simpleSAMLphp[13]나 Shibboleth[14] 패키지를 이용해 게이트웨이 서버를 구축한다. 전자는 소프트웨어의 설치와 환경설정이 상대적으로 쉬우나 제공되는 기능이 제한적이며 후자는 ECP(Enhanced Client or Proxy[15]) 등 다양한 기능을 제공하지만 구축과 환경설정이 어려운 단점이 있다. KAFE는 법령 준수와 보안 강화를 목적으로 simpleSAMLphp에 적용할 수 있는 다양한 소프트웨어 모듈(사용자동의, 속성정보의 필터링, Google™ One Time Password 등)을 개발해 github를 통해 공개하고 있다[16]. 또한 연합인증 환경의 구축 시간을 단축시키기 위해 게이트웨이 설치자동화 소프트웨어도 함께 제공하고 있다.

이질적이고 다양한 웹 서비스 환경으로 인해 서비스제공자의 SAML 연동방법이 단편화되어 있는 상황이다. 웹 서비스 환경은 그림 4와 같이 웹 서버(예, 아파치 웹 서버)와 웹 응용 서버(예, 톰캣 서버)가 동일한 경우와 서로 분리된 경우로 구분할 수 있다. 전자의 경우에는 웹 응용과 동일한 언어로 작성된 SAML 라이브러리를 이용해 SAML 기능을 부여하는 것이 일반적인 방법이다. 예를 들어, 웹 응용이 JAVA 기반의 전자정부 표준프레임워크를 활용한다면 SAML 라이브러리로 Spring security SAML extensions[17]를

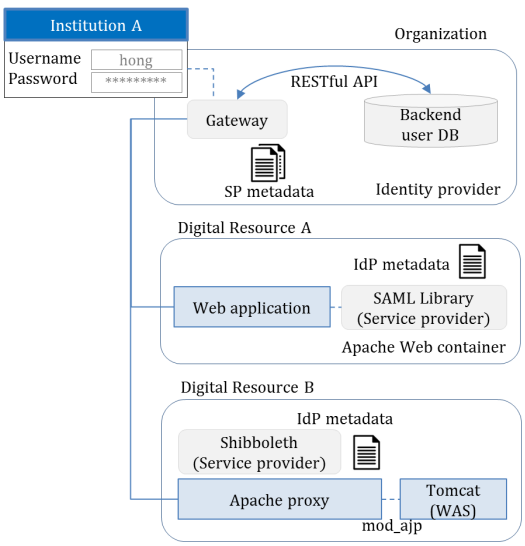

그림 4. SAML 개체의 구현
Fig. 4. Implementation of SAML entities

이용할 수 있다. 관리해야 하는 서버의 수는 줄일 수 있지만 웹 응용에 직접 구현하기 때문에 개발비용이 높아지는 단점이 있다.

웹 서버와 웹 응용 서버가 서로 다른 경우에는 웹 서버의 SAML 모듈을 활용해 연합인증을 수행한다. 웹 서버에서 획득한 인증정보와 속성정보를 웹 응용 서버에 전달하는 방식을 이용한다. 예를 들어, 웹 서버가 아파치라면 Shibboleth의 웹 서버 모듈인 mod_shib를 아파치에 설치해 SAML 인증요청과 인증응답을 처리한다. 웹 서버는 획득한 인증정보와 속성정보를 웹 응용 서버에 전달하고 웹 응용은 전달받은 정보를 이용해 사용자에게 권한을 부여한다. 그림 4의 예처럼 아파치 웹 서버는 AJP(Apache Jserv Protocol)를 이용해 웹 응용 서버인 톰캣에게 속성정보를 전달할 수 있다. 다수의 계정연합에서 검증된 방식으로써 웹 응용의 개발비용이 낮아진다는 장점이 있다. 웹 서버와 웹 응용 서버가 분리되어 있는 경우에도 앞서 설명한 SAML 라이브러리 방식을 이용할 수 있다.

Ⅳ. 연합인증 서비스의 설계 및 구현

SAML 개체가 서비스제공자 및 식별정보제공자로 계정연합에 가입하면 계정연합은 해당 개체들에게 연합인증 서비스를 제공한다. 본 장에서는 제3신뢰기관이 연합인증 서비스의 제공을 위해 개발한 핵심 시스템들을 설명한다. 현재 KAFE 계정연합의 제3신뢰기관이 담당하는 주 역할은 메타데이터의 관리와 배포, 개체상태의 모니터링, 탐색서비스의 제공, 이용현황의 수집 등이고 부가적으로 가상 식별정보제공자와 SAML 기능을 검증하기 위한 시험도구들을 제공하고 있다. 마지막으로 국가법령과 계정연합 정책의 준수를 위해 SAML 소프트웨어를 주기적으로 업데이트하는 역할도 수행 중이다.

KAFE에서 제공하는 연합인증 서비스는 그림 5와 같다. 메타데이터 수집(Aggregator)과 등록(Registry) 서비스는 국내외 계정연합들과 신뢰관계를 구축하며 FaaS(Federation as a Service)를 가능케 한다. 본 논문에서 FaaS는 하나의 계정연합이 다수의 하위 계정연합을 생성하고 관리할 수 있는 서비스로 정의한다. 즉, FaaS는 멀티테넌시(Multitenancy)의 개념과 유사하다. 현재 KAFE 계정연합은 시험 페더레이션(Test federation)과 프로덕션 페더레이션(Production federation)을 포함하여 총 5개의 하위 계정연합을 운영 중이다. 하위 계정연합의 신뢰관계는 독립적으로 구축되

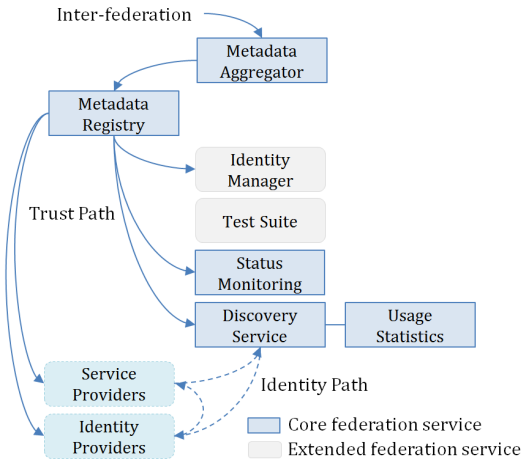

그림 5. KAFE 연합인증 서비스의 시스템 구성요소
Fig. 5. System components of KAFE federation service

기 때문에 특정 하위 계정연합에 포함된 개체들은 타 계정연합에 속한 개체들과 SAML 인증요청이나 인증응답을 할 수 없다.

국내에서는 SAML 기반의 웹 응용서비스를 개발하거나 활용할 수 있는 소프트웨어적 기반이 열악하므로 계정연합이 공용 소프트웨어 인프라를 제공해야 한다. KAFE는 서비스제공자가 개체구현을 쉽게 할 수 있도록 중앙형 탐색서비스를 제공하고 있다. 서비스제공자는 계정연합에서 제공하는 중앙형 탐색서비스를 이용하거나 내장형 탐색서비스를 자체적으로 구현해 사용할 수 있다. 탐색서비스는 로그인을 요청하는 서비스제공자의 개체식별자(EntityID)와 인증요청 메시지가 최종적으로 전달될 식별정보제공자의 개체식별자 정보를 수집함으로써 디지털자원에 대한 이용통계(Usage statistics)를 집계한다.

하나의 계정연합에 참여하는 서비스제공자들(S)은 동일한 계정연합에 참여하고 있는 식별정보제공자들(I)을 대상으로 자원접근을 허가할 수 있다. 즉, 계정연합에 참여하지 않은 기관(식별정보제공자를 구축하지 않은 기관)의 구성원들은 계정연합에 참여 중인 디지털자원에 접근할 수 없다. KAFE는 계정연합에 참여하지 않은 기관의 구성원들도 연구와 교육 목적의 디지털자원에 쉽게 접근할 수 있도록 사용자 계정관리 시스템(Identity manager)을 개발해 서비스 중이다. 사용자 계정관리시스템은 사용자의 계정정보를 저장하는 데이터베이스와 계정정보를 등록하고 관리하는 웹 어플리케이션 및 게이트웨이 서버로 구성된 가상(Virtual) 식별정보제공자이다. 물리적 기관이 아닌 가상 조직이 이용할 수 있는 식별정보제공자로 이해될 수 있다.

SAML 개체(예, 서비스제공자)가 구현되면 인증요청과 인증응답 메시지가 정상적으로 교환되는지 확인해야 하므로 상대 SAML 개체(예, 식별정보제공자)가 필요하다. 서비스제공자나 식별정보제공자가 검증만을 목적으로 상대 개체를 구축하고 구동환경을 설정하는 것은 번거롭고 비용이 소모되는 작업이다. KAFE는 검증목적의 서비스제공자와 식별정보제공자를 개발해 웹 응용서비스의 형태로 공개하고 있다. 검증도구들은 보안 및 낮은 LoA(Level of Assurance)등의 이유로 계정연합의 개체로 인정될 수 없기 때문에 신뢰경로에 포함되지 않는다. 검증도구를 이용하기 위해서는 대상 개체와 검증도구 간에 SAML 메타데이터를 수동으로 교환해야 한다.

4.1 SAML 메타데이터의 취합, 등록 및 배포

풀 매시구조에서 SAML 개체들이 개별적으로 메타데이터를 교환하면 기술 호환성의 문제가 발생할 수 있다. 또한 메타데이터의 교환은 기관 간의 협약을 필요로 하기 때문에 상대 개체의 수가 늘어날수록 협약에 대한 부담이 증가한다. KAFE는 개체들 간의 기술 호환성을 유지하고 협약에 대한 부담을 줄이기 위해 메타데이터 등록서비스를 개발해 서비스를 제공하는 중이다. 결과적으로 하나의 SAML 개체는 상대 개체의 수에 관계없이 한 번의 협약만으로 KAFE에 참여할 수 있다.

계정연합에 가입하는 SAML 개체들의 메타데이터는 정책준용 여부가 검증된 후에 계정연합의 연합 메타데이터에 추가된다. eduGAIN은 정회원을 대상으로 국외 계정연합의 연합 메타데이터를 배포하고 있다. 메타데이터 수용서비스는 eduGAIN을 통해 배포되는 연합 메타데이터를 검사하고 KAFE 정책의 준용 여부를 검증한다. 메타데이터 등록서비스는 공개 소프트웨어인 Jagger[18]를 국내 환경에 맞게 커스터마이즈했다. 개인정보의 관리국가 표기, 메타데이터의 요구기반(On-demand) 생성 및 개인정보의 암호화 등이 주요 수정내용이다. 메타데이터 수용서비스는 PHP 언어를 이용해 구현했으며 전자서명을 위해서 pyFF[19]를 사용하였다.

그림 6은 메타데이터 수용서비스와 등록서비스가 메타데이터를 처리하는 과정을 보여준다. 메타데이터 수용서비스(Metadata Aggregator)는 eduGAIN의 연합 메타데이터를 주기적으로 다운로드한다. 2018년 3분기 현재, 전 세계 53개 계정연합이 eduGAIN의 정회원이며 추가적으로 18개 계정연합이 준회원 또는

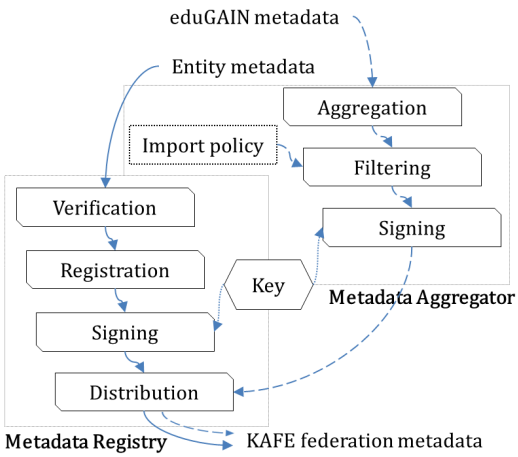

그림 6. 메타데이터의 수집, 등록 및 배포
Fig. 6. Metadata aggregation, registration, and distribution

후보로 등록되어 있다. eduGAIN의 연합 메타데이터는 총 4,951개의 SAML 개체들을 포함하고 있다. 계정연합이 속한 국가마다 법령이 다르기 때문에 모든 개체들을 수용하면 국내법 위반의 가능성이 있다. 메타데이터 수용서비스는 규정된 정책(Metadata import policy)을 위반하는 개별 SAML 메타데이터를 제거한다. KAFE에 최종적으로 수용되는 SAML 개체들은 총 727개로써 eduGAIN 메타데이터의 약 15%에 해당한다.

표 2는 메타데이터 수용정책의 주요 규정을 보여준다. 전자저널 등 상용서비스는 국내 법령의 준용 여부와 라이센스 정책 등을 확인해야하기 때문에 eduGAIN을 통해 연동될 수 없으며 KAFE 계정연합에 직접 가입해야 한다. 국내법령의 준용여부와 라이센스 정책이 확인된 일부 상용서비스는 예외처리를 통해 수용하고 있다. 인증키와 서명키의 길이가 2,048비트 미만이거나 개인정보정책을 포함하지 않은 SAML 메타데이터도 제거된다. 또한 HTTPS를 지원하지 않거나 자가 서명된 SSL(Secure Socket Layer) 인증서를 사용하는 개체들도 수용이 거부된다. 메타데이터 수용서비스는 검증이 완료된 SAML 개체들을 묶어 전자서명을 한 후에 연합 메타데이터를 배포한다.

표 2. eduGAIN 메타데이터의 수용 정책
Table2. Import policy of eduGAIN metadata

Policy	Behavior
Commercial entity	Conditional accept
Weak key length	deny
No privacy policy	deny
No HTTPS or HTTPS with Self-signed SSL	deny

메타데이터 등록서비스는 KAFE 계정연합에 직접 가입하는 SAML 개체들에게 제공된다. 전체적인 처리 절차는 메타데이터 수용서비스와 유사하다. 다만, 수용서비스가 자동화되어 있는 반면에 등록서비스는 등록을 요청하는 SAML 메타데이터를 계정연합의 관리자가 수동으로 직접 검증해야 한다. eduGAIN 메타데이터의 경우, 개별 국가의 계정연합에서 해당 국가의 법령준용 여부를 수동으로 확인한 후에 배포한다.

4.2 탐색서비스 및 이용상태 모니터링

메타데이터 수용서비스와 등록서비스가 연합 메타데이터를 배포하면 계정연합에 가입한 SAML 개체들은 주기적으로 해당 메타데이터를 다운로드 받아 연합인증에 활용해야 한다. 계정연합에 속한 모든 SAML 개체들이 동일한 연합 메타데이터를 확보하면 사용자는 계정연합의 서비스제공자에 로그인할 수 있게 된다. 서비스제공자가 다수의 식별정보제공자를 이용하는 경우에는 사용자계정이 저장된 식별정보제공자를 쉽게 찾을 수 있도록 탐색서비스가 제공되어야 한다. KAFE는 중앙형 탐색서비스를 개발해 회원기관에 제공하고 있다[20].

개발된 중앙형 탐색서비스는 IP 주소를 이용해 사용자의 접근 위치(GeoIP)를 파악하고 해당 사용자가 위치한 곳과 논리적으로 가장 가까운 순서대로 식별정보제공자들을 목록화해 제시한다. 식별정보제공자들이 갖는 기관명과 GeoIP 데이터베이스에 포함된 기관명의 코사인 유사도를 계산해 지리정보의 오류를 보정하고 있다. 중앙형 탐색서비스는 사용자가 접속하려는 서비스제공자($s \in S$)의 개체식별자(s_n)와 인증을 받으려는 식별정보제공자($i \in I$)의 개체식별자(i_m)를 실시간으로 획득할 수 있다. 획득된 개체식별자들의 조합(s_n, i_m)들을 분석함으로써 서비스 이용현황을 집계한다.

4.3 사용자 동의

계정연합에 참여하는 식별정보제공자는 사용자가 로그인에 성공할 때마다 해당 사용자의 속성정보를 서비스제공자에게 전달한다. 이름과 전자우편 주소 등 일부 속성정보는 개인정보로 분류된다. 국내 개인정보보호법의 제 17조(개인정보의 제공) 및 정보통신망법의 제 63조(국외이전 개인정보의 보호)는 개인정보를 제3자에게 제공할 때, 사용자에게 각 호의 항목을 고지하고 동의를 받도록 하고 있다. 각 호는 개인정보의

항목, 이전되는 국가, 이전 받는 자의 성명, 개인정보의 이용목적 및 보유·이용 기간, 거부권 및 그 불이익의 내용 등을 포함하고 있다.

식별정보제공자가 각 호를 고지하고 전자적으로 동의를 받으면 해당 법령들을 준수할 수 있다. KAFE는 전자적 동의를 획득하기 위한 소프트웨어 모듈을 개발하고 식별정보제공자에 탑재해 배포하고 있다. 제 3장에서 언급했듯이, 식별정보제공자는 SAML 메타데이터를 통해 서비스제공자에게 전달해야 하는 사용자의 속성정보를 파악할 수 있다. 즉, 고지해야 하는 개인정보의 항목을 알 수 있다. 또한 고지의 의무가 있는 기타 항목들에 대해서는 해당 내용이 포함된 서비스제공자의 개인정보정책을 전자적 동의 화면에 게시함으로써 법령을 준용하고 있다. 다만, 개인정보가 이전되는 국가명이 서비스제공자의 개인정보정책에 포함되지 않는 경우가 있기 때문에 메타데이터 등록서비스가 SAML 메타데이터에 국가명을 표기하고 개발된 소프트웨어 모듈이 관련된 XML 구성요소(element)를 읽어 동의화면에 게시한다.

표 3은 SAML 개체의 사법관할권(Jurisdiction) 정보를 표기하기 위한 XML 포맷이다. 메타데이터 등록서비스에서 사법관할권(즉, 개인정보가 이전되는 국가명)을 지정할 수 있도록 구현했다. 계정연합의 관리자는 메타데이터 등록서비스를 통해 사법관할권으로 명명된 개체 분류자를 서비스제공자에게 할당할 수 있다. 해당 개체 분류자는 ISO 3166-1 alpha-2에 정의된 국가코드를 값으로 갖는다. 개별 개체의 사법관할권 정보는 SAML 메타데이터에 포함되어 계정연합에 배포된다. 사용자 동의를 얻기 위해 개발된 소프트웨어 모듈(전자적 동의모듈)은 simpleSAMLphp에 탑재될 수 있도록 구현되었다. 사용자가 성공적으로 인증되면 전자적 동의모듈은 메타데이터의 <mdui:PrivacyStatementURL>에서 서비스제공자의 개인정보정책을 얻고 <saml:Attribute>에서 사법관할권 정보를 읽어 동의화면에 게시한다.

표 3. 사법관할권 명시를 위한 XML 구성요소
Table 3. XML elements for jurisdiction

```
<md:Extensions>
  <mdattr:EntityAttributes>
  <saml:Attribute
 Name="http://kafe.kreonet.net/jurisdiction"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for
 mat:uri">
     <saml:AttributeValue>
       Country Code
     </saml:AttributeValue>
  </saml:Attribute>
  </mdattr:EntityAttributes>
</md:Extensions>
```

4.4 가상조직을 위한 계정관리 시스템

가상조직(Virtual organization)은 공통의 목적을 달성하기 위해 조직된 사용자 집합을 의미한다. 소속기관이 서로 다른 연구자들의 집단이 가상조직의 한 예이다. 계정연합에서 하나의 식별정보제공자는 일반적으로 하나의 연구기관 또는 교육기관을 의미하기 때문에 개별 기관에 구축된 식별정보제공자는 해당 기관의 구성원들만 이용할 수 있어야 한다. 따라서 구성원의 소속기관이 서로 다른 가상조직이나 계정연합에 참여하지 않은 기관의 구성원은 연합인증을 이용할 수 없는 문제가 발생한다. KAFE는 가상조직이나 비회원기관의 구성원들도 계정연합에 포함된 디지털자원을 활용할 수 있도록 계정관리 시스템(Identity management system)을 개발해 서비스 중이다. 계정관리 시스템은 PHP 언어로 구현되었고 연합인증을 지원하기 위해 simpleSAMLphp의 소프트웨어 라이브러리를 이용했다. 또한 계정연합에 속한 모든 SAML 개체들과 기술적으로 호환될 수 있도록 설계되었다.

사용자는 계정관리 시스템을 통해 자신의 계정을 생성할 수 있다. 계정관리 시스템의 관리자는 사용자 계정을 생성하거나 등록된 계정 정보를 수정 및 삭제할 수 있다. 또한 계정연합에 포함된 디지털자원의 이용권한을 관리할 수 있으며 전자우편의 교환을 통해 사용자를 확인한다. 사용자가 입력한 계정정보를 이용해 신원을 검증하기 때문에 LoA가 낮은 문제가 있다. 계정연합에서는 중요한 디지털자원(예, 컴퓨팅 자원)의 오용과 남용을 막기 위해 높은 수준의 LoA를 요구한다. 공인인증서나 휴대전화 인증과 같은 비대면 인증수단을 도입해 LoA를 높여갈 예정이다. 계정관리 시스템은 Google™ Authenticator를 이용해 이중(Two-factor) 인증이 가능하도록 설계되었다. 이중 인증은 중간자 공격(Man in the middle attack)이나 재전송 공격(Replay attack)을 방어할 수 있는 주요 보안 수단으로써 시스템의 보안 강화를 위해 구현되었다.

개발된 시스템은 표 1에 표시된 핵심속성과 함께 사용자의 성(sn)과 이름(givenName) 및 소속기관의 이름(organizationName)과 같은 부가 속성을 제공한다. 제공되는 속성정보의 수가 늘어나면 세밀한 권한 부여가 가능하지만 수집해야 하는 개인정보의 수가 늘어나는 문제가 있다. 국제연구교육연합은 개인정보의 수집과 이용을 최소화시킬 목적으로 research-

표 4. research-and-scholarship 개체 분류자에서 사용되는 속성정보
Table 4. Attributes used for research-and-scholarship category

Elements	Recommendation
User identifier	eduPersonPrincipalName(ePPN)
	ePPN, eduPersonTargetedID
Person name	displayName
	givenName, surname
email address	email
Affiliation	eduPersonScopedAffiliation

and-scholarship 개체 분류자를 규정하고 표 4에 명시된 속성정보의 이용을 권장하고 있다. eduPerson ScopedAffiliation은 사용자의 직무를 정의한다. 서비스제공자에서 개별 사용자의 서비스 이용권한을 확인하기 위해 활용된다. 예를 들어, 특정기관(예, ss.ac.kr)의 학생이라면 student@ss.ac.kr과 같이 표기한다.

국제연구교육연합의 권장 사항(표 4의 내용)을 수용하는 SAML 개체는 research-and-scholarship 분류자를 메타데이터에 명기할 수 있다. 특정 SAML 개체가 갖는 개체 분류자를 상대 개체가 지원하지 않으면 기술 호환성을 담보할 수 없다. 개발된 계정관리 시스템(i)은 research-and-scholarship 분류자를 갖는 서비스제공자(s)에 대해서 $A_{rs} = A_i \cap A_s \cap A_c$인 속성정보를 제공한다. A_i와 A_s는 각각 식별정보제공자가 제공하거나 서비스제공자가 요청하는 속성정보의 집합이다. A_c는 표 4에 표시된 속성정보의 집합이다.

가상조직을 위한 계정관리 시스템은 국제연구교육연합의 보안사고 대응프레임워크인 SIRTFI(Security Incident Response Trust Framework for Federated Identity[21]) 분류자도 지원한다. SIRTFI는 계정연합에 참여하고 있는 기관들이 준수해야 하는 보안 지침들과 보안사고의 처리과정에서 교환되는 정보의 공개 범위 등을 규정하고 있다. 국외 계정연합에 속해있는 다수의 서비스제공자들이 SIRTFI와 research-and-scholarship 분류자에 대한 지원을 강제하고 있는 상황이다. 개발된 계정관리 시스템이 국제연구교육연합에서 요구하는 다수의 개체 분류자를 지원함으로써 국가 간의 기술호환성을 높이고 개인정보의 이용을 최소화할 수 있을 것으로 기대한다.

4.5 SAML 개체의 기능 검증

서비스제공자 또는 식별정보제공자가 인증요청이나 인증응답 등과 같은 SAML 기능을 검증하기 위해서는 대응하는 시험용 상대 개체가 필요하다. 검증을 목적으로 시험용 상대 개체를 구축하는 작업은 시간 소모적이다. 또한 연계되어야 할 상대 개체가 타 계정연합에 속해 있다면 자가 구축한 시험용 상대 개체로 SAML 기능을 검증하는 것은 불완전하다. 시험용 개체에 타 계정연합의 정책을 반영하기 힘들기 때문이다. 예를 들어, 국외에서 출판되는 전자저널이 국내 식별정보제공자와 연동되기 위해서는 국내 법령과 계정연합의 정책을 반영한 시험용 식별정보제공자가 상대 개체로 활용되어야 한다. 그러나 국외 전자저널 출판사가 국내 법령과 계정연합의 정책을 파악해 시험용 상대 개체를 구축하는 것은 시간적 비용의 증가를 의미한다. KAFE는 PHP 언어와 simpleSAMLphp를 이용해 시험용 서비스제공자와 식별정보제공자를 개발하고 계정연합에 참여하고자 하는 SAML 개체들을 대상으로 서비스 중이다.

낮은 LoA로 인해 시험용 상대 개체들은 계정연합의 연합 메타데이터에 등록될 수 없다. 개발된 개체(예, 시험용 식별정보제공자)가 계정연합에 등록된다면 임시적으로 생성한 사용자계정을 이용해 다수의 서비스제공자에 로그인하는 등 보안문제가 발생할 수 있다. 시험용 개체를 이용하는 서비스제공자나 식별정보제공자가 SAML 메타데이터를 쉽게 교환할 수 있도록 설계되었다. 사용자는 검증하고자 하는 SAML 개체의 메타데이터를 웹 인터페이스를 통해 시험용 개체에 등록하거나 시험용 개체의 메타데이터를 열람할 수 있다.

시험용 식별정보제공자는 간단한 계정관리 기능을 포함하고 있다. 사용자는 표 1과 표 4에 준하는 속성정보를 입력하고 검증용 계정을 발급받게 된다. 보안문제를 고려해 사용자가 생성한 검증용 계정과 등록한 SAML 메타데이터는 24시간 동안만 유효하도록 설계되었다. 시험용 서비스제공자도 웹 인터페이스를 통해 SAML 메타데이터를 등록하거나 열람할 수 있다. 상대 식별정보제공자의 인증 수준(Level of authentication)을 다양하게 검증할 수 있도록 표 5와 같이 3종류의 SAML Authentication Context Class(AuthnContextClass)를 제공한다. 서비스제공자는 SAML 인증요청을 통해 상대 개체가 AuthnContextClass에 포함된 AuthnContextClassRef의 방법으로 사용자를 인증하도록 요청할 수 있다.

암호로 보호된 전송(Password protected transport)에서는 식별정보제공자가 보호된 세션(예, SSL/TLS)을 통해 비밀번호를 전달받고 사용자를 인증해야 한

다. 일반적으로, SAML 개체는 암호로 보호된 전송을 기본 AuthnConextClassRef로 이용한다. 개발된 시험용 객체는 다중인증 환경의 도래에 선제적으로 대응하기 위해 국제연구교육연합에서 규정한 MFA (Multi-Factor Authentication) 프로파일을 지원한다. 다중인증은 다수의 보안공격에 대응하기 위한 효과적인 보안수단이다. 시험용 서비스제공자는 AuthnContextClass에 사용자 ID와 비밀번호(Username and password) 방식의 인증을 필수적으로 포함하고 있다. MFA 프로파일은 선택적으로 수용될 수 있기 때문에 MFA 프로파일을 지원하지 않는 식별정보제공자는 사용자 ID와 비밀번호 방식의 인증만 수행한다.

표 5. 지원되는 SAML AuthnContextClassRef
Table 5. Supported SAML AuthnContextClassRef

Authentication method	<AuthnContextClassRef> URI
Username and password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Password protected transport	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
REFEDS MFA Profile	https://refeds.org/profile/mfa

4.6 개체 상태의 모니터링

계정연합에 참여하는 개체들은 국가 법령과 계정연합의 정책을 준수해야 하므로 제3신뢰기관은 개체들의 정책준용 여부를 상시적으로 점검해야 한다. 또한 연합인증의 신뢰도와 활용도를 높이기 위해서는 참여 개체들의 가용성도 상시적으로 모니터링되어야 한다. 개체의 관리 주체가 서로 다르기 때문에 에이전트를 이용한 상태 모니터링 방식은 연합인증에 적합하지 못하다. 또한 모니터링 지표(Metrics)도 일반적인 서버나 네트워크 모니터링 시스템과 다르기 때문에 공개소프트웨어를 활용할 수 없다는 문제가 있다. KAFE는 SAML 개체들의 가용성과 정책준용 여부 등을 상시적으로 검사하기 위해 개체상태 모니터링 시스템을 개발해 활용하고 있다.

개발된 시스템은 목표 객체가 구동중인 서버의 HTTP 헤더, SSL 인증서, SAML 메타데이터를 주기적으로 획득한 후 분석해 모니터링을 수행한다. 모니터링 에이전트를 이용하지 않기 때문에 확장성이 높은 반면에 목표 서버의 환경설정에 따라 신뢰도가 저하될 수 있다는 문제가 있다. 개발된 시스템의 신뢰도는 목표 서버로부터 HTTP 헤더와 SSL 인증서를 획득할 수 있는지의 여부에 따라 결정된다. 하지만 목표 서버에서 환경설정을 통해 HTTP 헤더와 SSL 인증서의 제공을 거부할 수 있기 때문에 모니터링의 신뢰도가 낮아질 가능성이 있다. 향후 SAML 메시지를 활용하는 방식으로 문제점을 보완해 나갈 계획이다.

표 6은 개발된 시스템의 모니터링 항목을 보여준다. 메타데이터의 유효성(Metadata validity)은 연합 메타데이터의 유효 기간이 만료되었는지 확인하기 위한 지표이다. 유효 기간이 만료되었다면 오류 등으로 인해 연합 메타데이터가 정상적으로 생성되지 않았을 가능성이 크다. 연합 메타데이터의 EntityDescriptor에 포함된 validUntil 속성값을 읽어 유효 기간을 확인한다. 연합 메타데이터가 7일 이상 갱신되지 않으면 계정연합에 속한 모든 개체들은 연합인증을 이용할 수 없다.

개발된 모니터링 시스템은 개체가 설치된 웹 서버로부터 SSL 인증서를 획득해 CA(Certification Authority) 이름, 인증서의 유효기간, 서명 알고리즘 및 서명키의 길이 정보를 얻는다. 해당 모니터링 지표들은 계정연합의 정책 중 하나인 보안 프로파일의 준용여부를 검사하기 위해서 활용된다. KAFE는 SAML 개체들이 자가 서명된 인증서(Self Signed Certificate)를 사용하지 못하도록 강제하고 있다. 또한 SHA256 이상의 서명 알고리즘과 2,048비트 이상의 길이를 갖는 공개키 사용을 권장하고 있다.

SAML 인증 요청과 응답에 대한 재전송 공격을 방어하기 위해서 계정연합에 포함된 모든 개체들은 시스템 시간을 동기화해야 한다. 서비스제공자와 식별정보제공자 간에 허용되는 최대 시간 왜곡(Clock skew)은 60초이다. 서비스제공자는 상대 식별정보제공자의 시간 왜곡이 60초를 초과하면 수신한 SAML 어설션을 처리하지 않는다. 개발된 모니터링 시스템은 시간 동기화 여부를 확인하기 위해서 HTTP 헤더의 시간정

표 6. SAML 개체 모니터링 항목
Table 6. Metrics for SAML entity monitoring

Metrics	Description
Metadata validity	Less than 6 days
SSL Certification authority	No self-signed CA allowed
SSL validity	No expiration allowed
Signing algorithm	Only accept SHA256 (or more)
Key length	More than 2,048 bits
Time skew	Less than 30 seconds

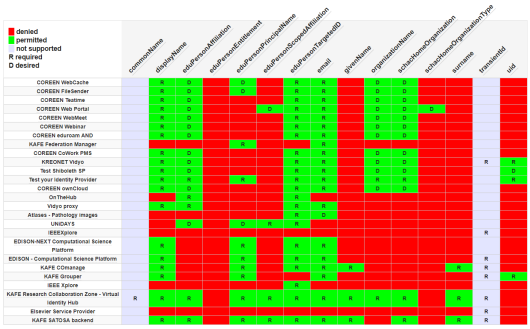

그림 9. 계정관리 시스템이 제공하는 속성표
Fig. 9. Attribute matrix provided by the ID management system

보를 이용한다. SAML 개체가 전달한 HTTP 헤더를 통해 시간정보를 획득하고 모니터링 시스템의 시간정보와 비교함으로써 시간 왜곡을 측정한다.

V. 연합인증 서비스의 설계 및 구현

본 장에서는 KAFE 계정연합의 식별경로와 신뢰경로 상에 구축된 개발 시스템들을 통해 구현결과를 정성적으로 설명한다.

그림 7은 메타데이터 등록서비스에서 활용중인 개체 분류자를 보여준다. 개체 분류자를 포함해 개체이름, 등록한 계정연합의 식별자, 연락처, 개인정보정책, 개체가 위치한 위도와 경도, 객체 식별자, 프로토콜 접속점, 인증서와 속성정보 등의 세부항목을 메타데이터 등록서비스에 등록할 수 있다. 관리자가 개체 메타데이터를 구성하는 세부항목을 입력하면 메타데이터 등록서비스는 XML 형태의 파일로 변환한다. 또한 관리자는 하위 계정연합을 생성하고 개별 계정연합에

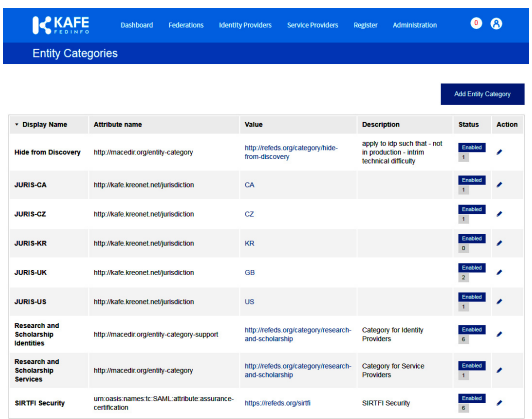

그림 7. 메타데이터 등록서비스
Fig. 7. Metadata registry

개체 메타데이터를 할당할 수 있다. 메타데이터 등록서비스는 하위 계정연합에 포함된 개체들의 메타데이터를 주기적으로 취합하여 연합 메타데이터를 생성한다.

그림 8은 메타데이터 등록서비스가 생성한 하위 계정연합의 EntitiesDescriptor 속성을 보여준다. eduGAIN은 EntitiesDescriptor의 ID 속성을 ds:Signature의 URI 값과 동일하게 지정할 것을 권장한다[22]. 메타데이터 등록서비스도 eduGAIN의 권장사항을 반영해 구현함으로서 국가 간 기술호환성을 높이고 있다. 또한 생성된 모든 연합 메타데이터의 유효기간을 7일로 지정함으로써 28일 이하를 권장하고 있는 eduGAIN의 메타데이터 관리 정책을 준수하고 있다.

표 7은 eduGAIN에서 제공하는 SAML 개체들 중, 메타데이터 수집서비스가 최종적으로 수용한 개체들의 총 수를 보여준다. 메타데이터 수집서비스가 eduGAIN에 포함된 전체 서비스제공자의 17%와 식별정보제공자의 13%를 수용하고 있음을 알 수 있다. 메타데이터 수집서비스는 서비스 활용도 등을 고려해 19개 서비스제공자만 계정연합에 공개하고 있다.

가상조직을 위한 계정관리 시스템, 중앙형 탐색서비스 및 사용자 동의 기능은 서비스제공자로 등록된 웹 응용의 이용절차를 예시함으로써 구현 결과를 평가한다. 앞서 설명했듯이, 계정관리 시스템은 계정연합에 참여하지 않는 기관의 구성원들도 사용자계정을 생성하고 연합인증을 통해 디지털자원을 이용할 수 있게 할 목적으로 개발되었다. 계정연합에 가입된 기관의 구성원들은 별도로 사용자계정을 생성하지 않아도 소속기관에서 이용하는 사용자 ID와 비밀번호를

```
<md:EntitiesDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init"
xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute"
xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xi="http://www.w3.org/2001/XInclude"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="kafe-
20180903030004" Name="urn:mace:kisti.re.kr:kafe:testfed"
validUntil="2018-09-03T03:00:04Z">
```

그림 8. 메타데이터 등록서비스가 생성한 EntitiesDescriptor
Fig. 8. EntitiesDescriptor generated by the registry

표 7. 수집된 개체의 수
Table 7. Number of aggregated entities

eduGAIN entities	Aggregated entities
2,144/2,817	360/367(17%/13%)

이용해 서비스제공자를 이용할 수 있다.

그림 9는 개발된 계정관리 시스템이 서비스제공자에게 제공하는 사용자 속성의 매트릭스(Attribute matrix)를 보여준다. 상단은 해당 시스템에서 제공하는 사용자 속성의 종류를 보여준다. 계정관리 시스템은 현재 15 종류의 속성을 지원하고 있다. 그림의 왼쪽은 계정연합에 속한 서비스제공자들을 나타낸다. 계정연합에 참여하고 있는 다수의 서비스제공자가 eduPersonTargetedID, displayName, email, eduPersonPrincipalName를 필수 속성으로 요구하고 있으며 개발된 계정관리 시스템이 해당 속성들을 제공하고 있음을 알 수 있다.

사용자가 로그인을 요청하면 식별정보제공자를 선택할 수 있도록 웹 브라우저가 탐색서비스로 전환된다. 그림 10은 서비스제공자인 eduroam 대리인증 서비스[24]에 로그인하는 과정에서 호출된 중앙형 탐색서비스를 보여준다. 사용자의 물리적 위치에 근접한 순서대로 식별정보제공자가 목록화되고 있음을 알 수 있다. 사용자의 위치는 대전(위도 36.36, 경도 127.39)이다. 또한 개발된 계정관리 시스템의 식별자 이름(COREEN set.ID by KAFE)이 탐색서비스에 정상적으로 가시화되고 있는 것을 확인할 수 있다.

그림 11은 중앙형 탐색서비스에서 'COREEN set.ID by KAFE'를 선택했을 때 나타나는 로그인 화면을 보여준다. 계정관리 시스템은 식별정보제공자로 동작하며 계정연합에 포함된 SAML 개체이다. 계정관리 시스템에 포함된 게이트웨이가 로그인 화면을 제공한다. 사용자가 탐색서비스에서 타 기관을 선택하면 웹 브라우저는 해당 기관에 구축된 게이트웨이의 로그인 화면으로 전환된다. 보안사고 대응프레임워크(SIRTFI)를 지원하는 식별정보제공자는 사용자에게 서비스 이용약관을 고지하고 이용 동의를 받아야 한다. SIRTFI를 지원하는 식별정보제공자는 User Agreement 링크를 통해 이용약관을 고지한다.

그림 12는 개발된 사용자 동의 화면을 보여준다. 식별정보제공자는 로그인에 성공한 사용자를 대상으로 개인정보의 제3자 제공에 대한 동의 여부를 질의한다. 서비스제공자에게 전달하는 속성정보, 서비스제공자의 개인정보정책, 개인정보가 이전되는 국가, 정보제공에 대해 동의하지 않을 경우에 발생하는 불이익 등 개인정보보호법과 정보통신망법에서 규정한 세부 항목들을 고지하도록 개발되었다. 개인정보정책과 이전되는 국가 정보는 개체 메타데이터의 mdui:PrivacyStatementURL와 saml:Attribute에 포함된 개체 분류자를 통해 획득한다. 사용자가 속성정보의 제3자 제공에 동의하면 동의결과(동의주체, 정보제공 항목, 동의날짜, 접속한 IP 주소 등)는 게이트웨이의 로그파일에 기록된다. 그래픽 인터페이스를 통해 동의기록을 관리할 수 있도록 관련된 소프트웨어 모듈을 고도화할 계획이다. 정보제공에 동의한 속성값은 SAML 어설션에 포함되어 서비스제공자에게 전달된

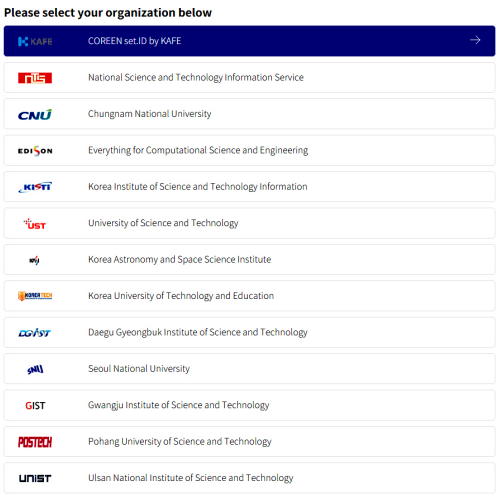

그림 10. 중앙형 탐색서비스
Fig. 10. Central discovery service

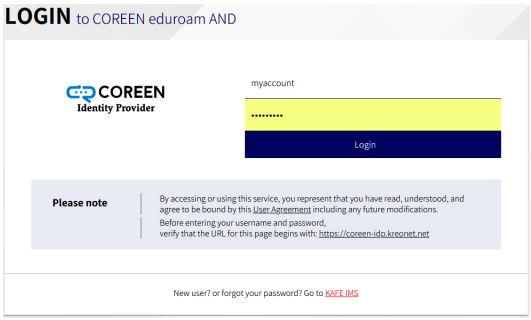

그림 11. 계정관리 시스템을 이용한 사용자 로그인
Fig. 11. Login with the ID management system

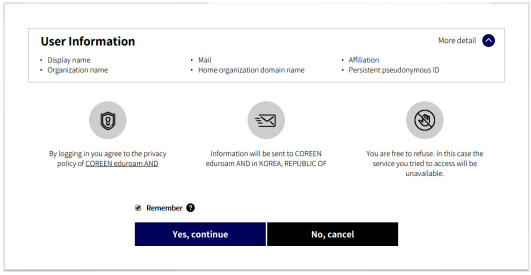

그림 12. 사용자 동의
Fig. 12. User consent

다. 서비스제공자는 전달받은 속성값을 이용(예, 직무정보가 staff이고 소속기관이 res.re.kr이면 관리자)하거나 속성값을 기반으로 사용자의 역할(예, 이름이 user이고 전자우편 주소가 user@res.re.kr인 사용자에게 admin 속성을 추가)을 부여함으로써 디지털자원에 대한 이용권한을 부여할 수 있다.

그림 13은 개발된 검증도구의 일부분을 보여준다. 그림의 상단과 하단은 각각 시험용 식별정보제공자와 시험용 서비스제공자이다. 앞서 언급했듯이, 검증도구들은 LoA가 낮기 때문에 개체 메타데이터가 계정연합에 포함되거나 자동으로 배포될 수 없다. 사용자는 XML 파일을 업로드하거나 복사 후 붙여넣기를 통해 상대 개체의 메타데이터를 등록할 수 있다. 서비스제공자를 검증하기 위해서는 시험용 식별정보제공자에 사용자계정이 등록되어 있어야 한다. 사용자가 시험용 식별정보제공자에 임시계정을 생성할 수 있도록 개발되었다. 검증도구에 등록된 메타데이터와 임시계정은 24시간 동안 유효하다.

그림 14는 시험용 서비스제공자를 활용해 임의의 식별정보제공자를 검증하는 절차이다. 그림 11과 그림 12에서 설명한 메타데이터의 등록과정과 임시계정을 생성하는 과정은 생략되었다. 또한 시험용 서비스제공자가 전달받은 속성정보는 일부만 표시했다. 시험용 서비스제공자가 사용자 ID와 비밀번호, 암호로 보호된 전송 및 MFA 프로파일 등 3가지 인증방식(AuthnContextClassRef)으로 사용자 인증을 요청할 수 있다는 것이 확인된다.

검증도구의 SAML 메타데이터가 연합 메타데이터에 포함될 수 없으므로 시험용 서비스제공자는 그림 10과 같은 중앙형 탐색서비스를 이용할 수 없다. 그림 14의 중앙에 위치한 그림은 검증용 서비스제공자에 구현된 내장형 탐색서비스를 보여준다. 내장형 탐색서비스는 사용자가 시험용 서비스제공자에 등록한 식별정보제공자의 SAML 메타데이터를 이용해 사용자 인증을 수행할 조직을 목록화한다. 사용자가 선택한 식별정보제공자를 통해 로그인하면 시험용 서비스제공자는 전달받은 속성정보를 가시화한다. SAML 인증요청과 인증응답의 송/수신 여부, 고유식별자의 유일성(Uniqueness), 필수속성의 전달여부와 같은 항목들을 검증할 수 있다.

그림 15는 개발된 개체상태 모니터링 서비스의 일부를 보여준다. 계정연합에 참여 중인 34개의 개체들과 5개 연합 메타데이터의 상태를 모니터링 중이다. 앞서 설명했듯이, 모니터링 시스템은 대상 개체가 구동중인 웹 서버에서 HTTP 헤더와 SSL 인증서를 주기적으로 획득한다. 관리자는 목적한 개체의 이름, 개체식별자, 목적 URL과 같은 시스템 정보를 사전에 등록해야 한다. 모니터링 대상인 34개 개체들 중에 약 3%에 해당하는 1개 개체에서 HTTP 헤더와 SSL 인증서 정보를 획득할 수 없었다. 해당 개체가 구동중인 웹 서버에서 HTTP 헤더와 SSL 인증서 정보의 제공을 거부했기 때문이다. SAML 메시지를 활용해 능동(Active) 모니터링을 수행함으로써 모니터링 시스템의 신뢰도를 높여나갈 예정이다.

그림 13. 기능검증 목적의 SAML 개체
Fig. 13. SAML entities for function verification

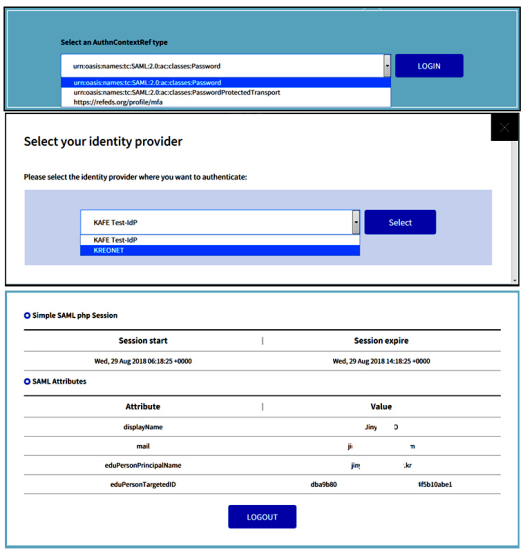

그림 14. 목적한 식별정보제공자의 검증
Fig. 14. Verification of a targeted identity provider

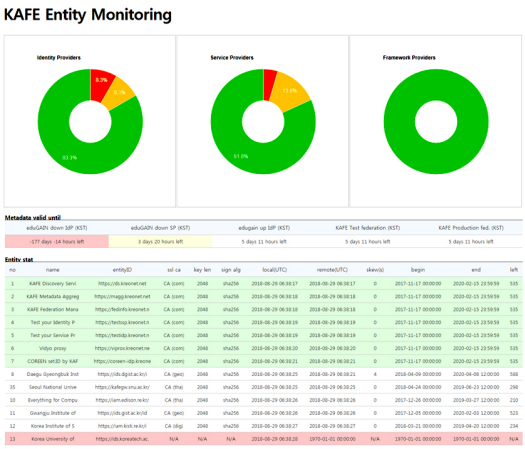

그림 15. SAML 개체들의 연합상태 모니터링
Fig. 15. Federation status monitoring of SAML entities

Ⅵ. 결 론

본 논문은 연합인증에 대해서 소개하고 연합인증 환경구축을 위해 필요한 시스템 구성요소와 구현방법에 대해서 설명했다. 또한 계정연합의 개념에 대해서 소개하고 국내 계정연합에서 제공하는 연합인증 서비스의 세부 구성요소와 설계 내용 및 구현 결과를 살펴보았다. 본 논문은 연합인증의 구조와 내용에 대해서 이해하고 유관기술의 활용확대에 기여할 수 있을 것이다. 마지막으로 계정연합을 통해 국내 연구기관과 교육기관이 보유한 디지털자원과 산업체에서 제공하는 연구교육 목적의 웹 응용서비스들이 보다 쉽고 안전하게 공유될 수 있기를 기대한다.

References

[1] D. W. Chadwick, “Federated identity management,” in *Proc. Foundations of Secur. and Anal. and design V*, Springer, vol. 5705, pp. 96-120, Berlin, Heidelberg, 2009.

[2] V. Koukis, C. Venetsanopoulos, and N. Koziris, “~ okeanos: Building a cloud, cluster by cluster,” *IEEE Internet Comput.*, vol. 17, no. 3, pp. 67-71, May 2013.

[3] EGI Foundation, *EGI: Advanced Computing for Research*, Retrieved Sept., 3, 2018, from https://www.egi.eu/.

[4] N. Rettberg and S. Birgit, “OpenAIRE - Building a collaborative open access infrastructure for European researchers,” *Liber Quart.*, vol. 22, no. 3 pp. 160-175, 2012.

[5] REFEDS, Retrieved Sept., 3, 2018, from https://refeds.org.

[6] W. Barnett, V. Welch, A. Walsh, and C. A. Steward, *A roadmap for using NSF cyberinfrastructure with InCommon*, IUScholarWorks, 2011.

[7] K. Yamaji, et al., “Japanese access management federation gakunin as an eResearch collaborative infrastructure,” in *Proc. eResearch Australasia*, Sept., 2010.

[8] Y. Cho, S. Jin, P. Moon, and K. Chung, “Internet ID management system based on ID federation: e-IDMS,” *J. IEIE-TC*, vol. 7, no. 43, pp. 104-114, Jul. 2006.

[9] Korean Access Federation, Retrieved Sept., 3, 2018, from https://coreen.kreonet.net.

[10] J. Howlett, V. Nordh, and W. Singer, *Deliverable DS3 2.1: eduGAIN service definition and policy initial draft*, Project Deliverable, May 2010.

[11] H. John and M. Maler, *Security Assertion Markup Language (SAML) v2.0 technical overview*, OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08, pp.29-38, 2005.

[12] H. Jang, K. Lee, J. Kong, and J. Jo, “Development of collaboration infrastructure to promote R&D collaboration,” *J. KIICE*, vol. 19, no. 10, pp. 2429-2440, Oct. 2015.

[13] simpleSAMLphp, Retrieved Sept., 3, 2018, from https://simplesamlphp.org.

[14] P. Kamal, S. Mustafiz, F. M. A. Rahman, and R. Taher, “Evaluating the efficiency and effectiveness of a federated SSO environment using Shibboleth,” *J. Inf. Secur.*, vol. 6, no. 3, pp. 166-178, May 2015.

[15] S. Cantor, *SAML ECP profile schema*, OASIS SSTC, Mar. 2005.

[16] *KAFE Software Packages*, Retrieved Sept., 3, 2018, from https://github.com/coreen-kafe.

[17] N. Nachimuthu, *Spring Security Essentials*, Packt Publishing Ltd., 2016.

[18] Jagger - *Free federation management tool*,

Retrieved Sept., 3, 2018, from http://jagger.heanet.ie/.

[19] D. Pohn, S. Metzger, and W. Hommel, "Geant-TrustBroker: Dynamic, scalable management of SAML-based inter-federation authentication and authorization infrastructures," in *Proc. IFIP Int. Inf. Secur. Conf.*, pp. 307-320, Berlin, Heidelberg, 2014.

[20] J. Jo, H. Jang, and J. Kong, "Development of identity-provider discovery system leveraging geolocation information," *J. KIICE*, vol. 21, no. 9, pp. 1777-1789, Sept. 2017.

[21] *A Security Incident Response Trust Framework for Federated Identity* v.1, Retrieved Sept., 3, 2018, from https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf.

[22] Metadata Validator, Retrieved Sept., 3, 2018, from https://wiki.geant.org/display/eduGAIN/Metadata+Validator#MetadataValidator-1.

[23] G. Wang, J. Cho, and G. Cho, "Global wireless LAN roaming status in Korea and its development methods," *J. IEIE*, vol. 52, no. 7, pp. 15-21, Jul. 2015.

[24] K. Lee, J. Jo, and J. Kong, "Design and implementation of eduroam authentication-delegation system," *J. KIICE*, vol. 20, no. 9, pp. 1730-1740, Sept. 2016.

[25] R. Widdowson and S. Cantor, "*Identity Provider Discovery Service Protocol and Profile*," OASIS Committee Specification 1, 2008.

조 진 용 (Jinyong Jo)
1999년 2월 : 전남대학교 컴퓨터공학과 졸업
2002년 8월 : 광주과학기술원 정보통신공학과 석사
2013년 8월 :광주과학기술원 정보통신공학과 박사
2003년 8월~현재 : 한국과학기술정보연구원
<관심분야> SDN, Federated Identity Management

장 희 진 (HeeJin Jang)
2001년 2월 : 포항공과대학교 컴퓨터공학과 졸업
2003년 2월 : 포항공과대학교 컴퓨터공학과 석사
2003년~2009년 : 삼성종합기술원
2010년~현재 : 한국과학기술정보연구원
<관심분야> Federated Identity Management, 기계학습

공 정 욱 (JongUk Kong)
1993년 2월 : 한국과학기술원 졸업
1998년 2월 : 포항공과대학과 석사
2015년 8월 : 충남대학교 정보통신공학과 박사
1993년~2001년 : ㈜데이콤
2001년~2002년 : ㈜맥스웨이브
2002년~현재 : 한국과학기술정보연구원
<관심분야> 네트워크 자원 제어, SDN

채 영 훈 (Yeonghun Chae)
2015년 2월 : 고려대학교 전자 및 정보공학과 졸업
2017년 8월 : 과학기술연합대학원대학교 빅데이터과학 석사
2017년 9월~현재 : 한국과학기술정보연구원
<관심분야> Federated Identity Management, 심층학습