JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 9 : 1730~1740 Sep. 2016

eduroam 사용자 대리인증 시스템의 설계 및 구현

이경민 · 조진용* · 공정욱

Design and Implementation of eduroam Authentication-Delegation System

KyoungMin Lee · Jinyong Jo* · JongUk Kong

Korea Institute of Science and Technology Information, KISTI, Daejeon 34141, Korea

요 약

본 논문은 eduroam의 사용자 대리인증 시스템인 eduroam AND를 소개한다. eduroam은 전 세계 연구기관과 교육기관을 대상으로 서비스 중인 글로벌 무선인터넷 접속 서비스이다. eduroam AND(AutheNtication Delegation)는 eduroam 서비스에 가입되지 않은 국내 연구기관과 교육기관의 구성원들이 eduroam의 사용자 계정을 자가 생성하고 eduroam 서비스에 접속할 수 있게 할 목적으로 개발된 시스템이다. eduroam AND는 국제 표준에 따르는 연합 인증 기술을 구현해 적용함으로써 서비스 접근 편의성 향상, 사용자 신원확인과 검증의 용이, 사용자 식별정보의 효율적 관리, 사용자 인증정보의 관리부담 완화 등의 기대효과를 갖는다. 또한 계층적 라우팅 구조를 갖는 eduroam의 노드 상태 및 메시지 라우팅 상태 등을 상시 모니터링 함으로써 운영 관리의 효율성을 높일 수 있다. eduroam AND는 오픈소스 소프트웨어를 이용해 구현되었으며 국가과학기술연구망에 구축되어 운영 중이다. 마지막으로 구현결과를 중심으로 eduroam AND를 정성적으로 평가한다.

ABSTRACT

This paper introduces a guest identity provider system for eduroam which is a global Wi-Fi service targeting users enrolled in higher education and research institutions. Developed eduroam AND (AutheNtication Delegation) system enables users to create their eduroam user accounts and to access eduroam regardless of their locations. Users with no organizational eduroam account therefore can freely access eduroam using the system. A federated authentication model is implemented in the system, and thus the system has merits of having high accessibility, indirectly verifying users and organizations possible, saving management overhead. Status monitoring is essential because authentication request and response messages are routed by eduroam network. eduroam AND performs active monitoring to check service availability and visualizes the results, which increases operational and management efficiency. We leveraged open-source libraries to implement eduroam AND and run the system on KREONET (Korea REsearch Open NETwork). Lastly, we present implementation details and qualitively evaluate the system.

키워드 : eduroam, 연합 ID 관리, SAML, 사용자 인증, Wi-Fi 접속 서비스

Key word : eduroam, Federated Identity Management, SAML, User Authentication, Wi-Fi Access Service

Received 15 July 2016, **Revised** 18 July 2016, **Accepted** 05 September 2016

* **Corresponding Author** Jinyong Jo(E-mail:jiny92@kisti.re.kr, Tel:+82-42-869-0585)
Korea Institute of Science and Technology Information, KISTI, Daejeon 34141, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.9.1730 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

연구자들의 연구협력 편의성 확보를 위한 다양한 노력들이 진행되고 있다[1, 2]. eduroam[2]은 전 세계 77개 국가에서 참여하고 있는 글로벌 무선인터넷 접속서비스이다. eduroam 계정을 보유한 사용자는 무선단말에 eduroam 이외의 추가적인 SSID(Service Set IDentifier)를 설정하지 않아도 eduroam 서비스에 참여 중인 국내외 연구기관과 교육기관에서 무선인터넷 서비스를 자유롭게 이용할 수 있다.

eduroam 서비스에 참여하는 기관은 사용자 인증을 담당할 RADIUS(Remote Authentication Dial in User Service[3]) 서버와 eduroam 접속이 가능한 WAP (Wireless Access Point)을 설치해야 한다. eduroam 참여기관의 구성원은 접속위치에 관계없이 소속기관에 등록된 eduroam 사용자ID와 비밀번호를 이용해 글로벌 무선인터넷 접속 서비스를 이용할 수 있다. 하지만 인증 서버 및 eduroam WAP 장치 등 eduroam 서비스 환경을 구축하기 위한 비용과 관리운영의 문제, 무선인터넷 보안 위협에 대한 우려[4]등으로 인해 eduroam 서비스의 국내 확산이 제한적인 상황이다[5].

본 논문은 국내 연구기관과 교육기관을 대리해 eduroam 사용자의 계정을 등록 관리하고 사용자 인증기능을 제공하는 eduroam AND(AutheNtication Delegation) 시스템을 소개한다. 국내 연구 및 교육기관의 구성원들은 소속 기관이 별도의 사용자인증 및 계정관리 서버를 제공하지 않아도 eduroam AND를 이용해 국내외 타 기관에서 제공하는 eduroam 서비스를 이용할 수 있게 된다. 개별 기관은 인증 서버의 구축비용 및 관리운영 문제를 해소할 수 있으며 eduroam 서비스 도입으로 인한 무선인터넷 보안 관리 문제를 완화시킬 수 있다. 연합 ID 관리[1] 서비스를 제공하는 몇몇 국가단위 페더레이션 운영기관(Federation operator)들은 eduroam AND와 유사한 eduroam 대리인증 시스템(예, DEAS[6]와 EduShib[7])을 개발해 자국 내 연구기관과 교육기관을 대상으로 서비스하고 있다. DEAS와 EduShib은 Shibboleth[8] 소프트웨어와 웹 컨테이너의 사용자 인증 모듈을 이용해 구현된 반면 eduroam AND는 simpleSAMLphp[9] 소프트웨어의 API(Application Programming Language)를 이용해 구현함으로써 시스템의 유지관리 용이성이 높다. 또한 eduroam 사용자에 대한 인증 기능과 eduroam 네트워크에 대한 모니터링 기능을 통합 구현함으로써 eduroam 서비스의 가용성을 쉽게 확인할 수 있는 장점이 있다.

본 논문의 기여 점은 다음과 같다. 첫째, 연구기관과 교육기관을 대리해 eduroam 사용자의 계정을 관리하고 인증하기 위한 대리인증 구조를 설계하고 구현하였다. 연합 인증 기술을 적용함으로써 개별 사용자의 eduroam 서비스에 대한 접근성을 높이고 사용자 계정의 생성 및 관리 편의성을 높였다. 둘째, eduroam 대리인증 시스템에 RADIUS 노드상태 모니터링 기능을 통합해 설계하고 구현했다. 라우팅 경로 상의 RADIUS 노드를 모니터링하고 오류발생 시 실시간 통지함으로써 eduroam 서비스의 가용성 확인이 용이해졌다. 마지막으로, 국가과학기술연구망(KREONET)에 개발된 eduroam AND 시스템을 구축해 대리인증 서비스를 제공함으로써 eduroam 서비스의 활용확산에 기여할 것으로 판단된다.

본 논문의 2장은 eduroam 서비스와 연합 인증 등 eduroam AND의 배경기술에 대해 간략히 소개한다. 제3장에서는 eduroam AND의 설계목표를 기술하며 제 4장은 설계 및 구현 내용에 대해 상세히 살펴본다. 제 5장에서 구현 결과를 정성적으로 검증하고 제 6장에서 결론을 맺는다.

Ⅱ. 배경 기술

본 장에서는 eduroam 서비스의 구조를 간략히 살펴본 후 eduroam AND에 구현된 연합 인증 기술에 대해서 소개한다.

2.1. eduroam 서비스의 구조

eduroam은 범 유럽 연구망(GEANT)에 의해 관리되고 있는 글로벌 무선인터넷 접속서비스이다. eduroam 서비스에서 사용자 인증은 해당 사용자의 무선인터넷 접속위치와 관계없이 항상 사용자의 소속기관에서 수행된다. eduroam은 인증 요청과 응답 메시지의 라우팅을 위해 그림 1과 같은 계층적 트리 구조를 이용한다.

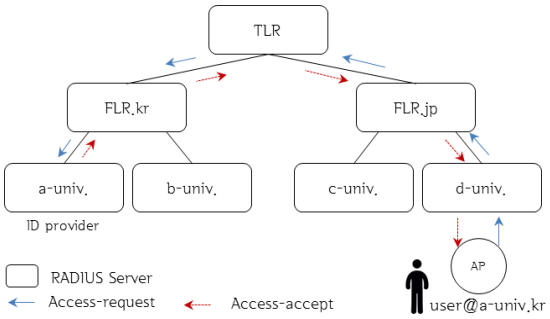


Fig. 1 Routing tree of eduroam user authentication message

eduroam의 트리구조는 TLR(Top Level RADIUS), FLR(Federation Level RADIUS), ILR(Institution Level RADIUS)을 포함한다. RADIUS 노드는 인증 메시지를 라우팅하거나 사용자를 인증하는데 이용된다. TLR은 범 유럽 연구망에 의해 관리·운영되는 최상위 계층 RADIUS 서버로써 인증 메시지를 국가 간에 라우팅한다. FLR은 국가단위 운영주체(National roaming operator)에 의해 운영되며 자국 내 ILR, 또는 TLR과 연동되어 메시지 라우팅을 수행한다. ILR은 개별 기관이 운영하며 FLR과 상호 연동된다.

eduroam의 사용자 인증은 사용자의 무선인터넷 접속 위치에 관계없이 항상 소속 기관에서 수행되기 때문에 높은 이동성을 보장한다. 그림 1은 a-대학 소속의 사용자가 국외 d-대학을 방문해 eduroam 서비스에 접속할 때, 사용자 인증 요청과 응답 메시지가 d-대학과 a-대학 간에 교환되는 과정을 보여준다. eduroam은 계층적 라우팅을 위해 그림 1의 user@a-univ.kr과 같은 [식별자]@[기관명].[국가코드] 형태의 사용자ID를 이용한다.

인증 요청 메시지가 전달될 최종 목적지는 사용자ID에 포함된 [기관명].[국가코드] 정보를 이용해 결정된다. TLR, FLR 또는 ILR에 할당된 [기관명].[국가코드]가 인증 요청 메시지에 포함된 [기관명].[국가코드]와 다를 경우, 해당 메시지는 개별 RADIUS 노드에 저장된 라우팅 정보를 이용해 부모 또는 자식 노드에게 전달된다.

2.2. 연합 ID 관리 및 사용자 인증

연합 ID 관리는 식별정보 제공자(Identity provider)와 자원 제공자(Service provider) 간에 사용자 인증 기능을 상호 연동하기 위한 기술적·정책적 체계이다. 대표적인 연합 ID 관리 및 사용자 인증 기술은 SAML (Security Assertion Markup Language[10]), OAuth[11], OpenID[12] 등이 있다. 본 논문에서 언급하는 연합 ID 관리 기술(이하, 연합 인증)은 SAML을 의미한다.

연합 인증은 다수의 식별정보 제공자와 자원 제공자 간에 신뢰관계(Trust relationship)를 바탕으로 구축된 식별정보 관리체계이다. 식별정보 제공자와 자원 제공자는 SAML 메타데이터[12]를 상호 교환함으로써 신뢰관계를 수립한다. SAML 메타데이터는 전자 서명키, 접속 URL 등 시스템 부가정보를 기록한 파일이다. 사용자는 식별정보 제공자에 등록된 크리덴셜(사용자ID와 비밀번호)을 이용해 다수의 자원 제공자에 접속할 수 있게 된다. 통합 로그인(Single-Sign On)을 지원하기 때문에 서비스 이용 동선의 간소화 등 높은 사용자 편의성을 제공한다.

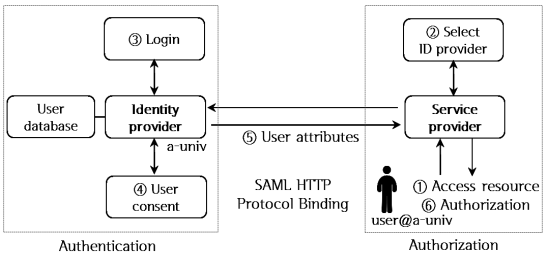


Fig. 2 Authentication and authorization with SAML

연합 인증에서 식별정보 제공자는 사용자를 인증하고 자원 제공자는 자원에 대한 이용권한을 부여(인가)한다. 식별정보 제공자와 자원 제공자는 SAML 메시지를 상호 교환하며 통신을 위해 HTTP Redirect/POST/Artifact를 바인딩하여 사용한다. 통신 기능은 SAML에 포함되어 있지 않다. 식별정보 제공자와 자원 제공자 간의 사용자 인증 및 인가(Authentication and authorization) 과정은 그림 2와 같다. 사용자는 접속이 제한된 자원을 이용하기 위해 식별정보 제공자를 선택하고 사용자 인증을 요청한다(그림 2의 ①, ②). 식별정보 제공자는 사용자를 인증하고 인증된 사용자의 속성정보(예, 사용자명, 이메일 주소 등)는 SAML 주장(Assertion)을 통해 자원 제공자에게 전달된다(③, ④, ⑤). 자원 제공자의 ACS(Assertion Consumer Service)는 식별정보 제공자가 전달한 속성정보를 해석하고 웹

응용에게 포워딩한다. 마지막으로 웹 응용은 전달받은 속성정보를 이용해 자원에 대한 이용권한을 부여한다 (⑥).

Ⅲ. 설계 목표

eduroam AND는 국내 연구기관과 교육기관을 대리해 신뢰할 수 있는 제 3 기관(Trusted 3rd Party)에서 eduroam의 사용자 계정을 관리하고 인증요청을 처리하기 위한 일종의 게스트(Guest) 식별정보 제공자 시스템이다. 게스트 식별정보 제공자는 사용자 계정이 관리자의 개입 없이 사용자에 의해 자가 관리되는 시스템을 의미한다. eduroam AND는 다음과 같은 설계 목표를 갖는다.

첫째, 게스트 식별정보 제공자 시스템의 이용 편의성을 높이고 로그인 보안을 강화해야 한다. 일반적으로 게스트 식별정보 제공자와 같은 웹 응용들은 웹 응용에 접근하기 위한 계정과 eduroam을 이용하기 위한 계정 등 2개의 사용자 계정이 필요하다. 여러 번의 계정 등록은 이용 편의성을 저하시킨다. 또한 자원 제공자에서는 다수의 계정 유지로 인한 보안 문제가 발생할 수 있다. 게스트 식별정보 제공자는 동일한 사용자의 계정 등록 횟수와 저장되는 사용자 정보를 최소화해야 한다.

일반적으로 자가 관리되는 사용자 계정은 신원증명과 기관식별이 어려운 문제점이 있다. eduroam은 기관 간의 신뢰관계를 기반으로 동작하는 시스템이기 때문에 사용자의 신원증명과 소속기관에 대한 식별이 중요하다. 게스트 식별정보 제공자 시스템은 등록된 사용자로 인한 보안 침해를 예방 및 추적하고 기관 간 신뢰관계의 저하를 막기 위해 사용자 신원과 소속기관 정보에 대해 신뢰할 수 있는 기술적 방법이 필요하다.

둘째, 게스트 식별정보 제공자를 통해 eduroam 서비스에 대한 상시 모니터링이 가능해야 한다. 게스트 식별정보 제공자가 관리하는 eduroam 사용자DB는 네트워크를 통해 RADIUS 노드와 연동되며 사용자 인증을 위해 이용된다. 게스트 식별정보 제공자가 eduroam 서비스의 사용자 접점으로 간주되는 경향이 있기 때문에 국가단위 운영 주체에서 모니터링 정보를 제공하지 않으면 사용자 지원에 문제가 발생할 수 있다. 또한 국가단위 운영 주체는 일반적으로 RADIUS 노드들 사이의 물리적 연결 상태만을 모니터링하기 때문에 무선 단말의 서비스 접속 가능 여부를 파악하기는 쉽지 않다.

추가적으로 게스트 식별정보 제공자 시스템이 모니터링 기능을 제공하지 않으면 시스템 관리자는 무선 단말을 물리적으로 이동해 가며 eduroam 사용자에 대한 인증 가능 여부를 검사해야 하는 문제가 발생한다. 서비스 장애 발생 지점의 파악과 사용자 인증의 결과를 쉽게 파악하기 위해 상태 모니터링 기능이 필요하다.

Ⅳ. 시스템 구현

본 장은 제 3장에서 설정한 설계 목표를 반영하여 eduroam AND 시스템을 구현하고 세부 구조를 살펴본다.

4.1. eduroam 계정 관리 및 시스템 구성 개요

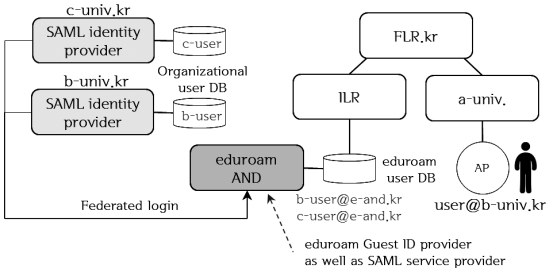


Fig. 3 Federated login to create an eduroam account

eduroam AND는 그림 3과 같이 SAML 자원 제공자 및 eduroam 식별정보 제공자로 동작한다. SAML 자원 제공자로 동작할 경우, SAML 식별정보 제공자를 통해 인증 받은 사용자에게 eduroam 계정의 생성 권한을 부여한다. eduroam 식별정보 제공자로 동작할 경우에는 사용자가 등록한 크리덴셜 정보를 RADIUS 노드에게 제공한다. eduroam AND는 eduroam 서비스를 이용하는데 필요한 계정 정보만 유지하도록 구현되었다. 웹 응용에 로그인하기 위해 필요한 사용자 계정은 SAML 식별정보 제공자가 관리하기 때문에 이용 편의성의 제고와 보안 강화에 효과적이다. eduroam AND에 저장된 모든 사용자ID는 동일한 [기관명].[국가코드]를 갖는다. 따라서 eduroam AND에 계정이 등록된 모든

사용자들의 인증 요청은 eduroam AND와 직접 연동된 RADIUS 노드에서 처리된다. eduroam AND는 *n*개 기관에서 관리해야 되는 *n*개의 RADIUS 노드를 1개로 줄이고 eduroam의 라우팅 트리를 단순화시키는 효과가 있다.

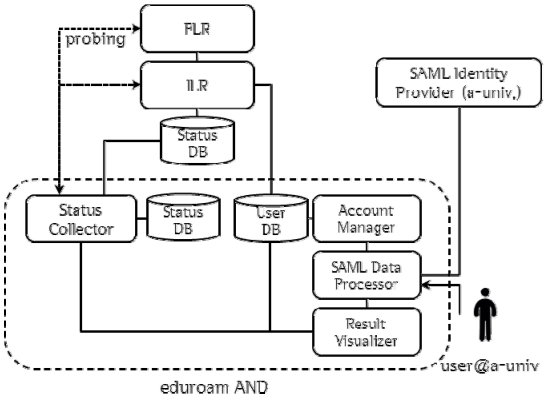


Fig. 4 Building blocks of eduroam AND

그림 4는 eduroam AND의 구성 요소들을 보여준다. eduroam AND는 eduroam 계정관리기(Account Manager), SAML 처리기(SAML Data Processor), eduroam 네트워크상태 수집기(Status Collector) 및 결과 가시화기(Result Visualizer)로 구성되고 ILR 및 SAML 식별정보 제공자와 상호 연동된다. 사용자 DB(User DB)는 eduroam 사용자의 크리덴셜을 저장하고 상태 DB(Status DB)는 인증 처리의 결과 및 eduroam 서비스의 가용성 상태를 저장하는데 이용된다.

eduroam AND와 연동된 ILR은 사용자 DB를 eudroam AND와 공유한다. eduroam AND는 웹 응용의 사용자 인증을 위해 다수의 SAML 식별정보 제공자들과 연동될 수 있다. SAML 처리기는 식별정보 제공자에게 사용자 인증을 요청하고 속성정보를 해석하는 등 SAML 메시지를 처리한다. HTTP Redirect 바인딩을 이용하여 SAML 프로토콜 메시지가 처리되도록 구현하였다.

SAML 처리기를 통해 연합 인증에 성공한 사용자는 eduroam 계정을 생성할 수 있다. eduroam 계정관리기는 PHP 언어로 구현된 웹 응용으로써 사용자 계정의 생성, 정보 변경, 삭제 등의 기능을 포함한다. 생성된 계정 정보는 사용자 DB에 저장된다.

eduroam 네트워크상태 수집기는 ILR에 저장된 사용자 인증 결과(예, Access-accept 또는 Access-reject)를 수집한다. 또한 FLR과 ILR을 액티브 모니터링(Active monitoring)하고 eduroam 서비스의 가용성 정보와 인증 처리에 소요된 시간지연 정보를 수집한다.

결과 가시화기는 웹 GUI를 이용해 등록된 사용자의 계정 정보와 eduroam 서비스의 이용 이력 등을 보여준다. 또한 상태DB에 저장된 가용성 정보와 시간지연 정보를 주기적으로 가시화해 관리자에게 제공한다.

4.2. 사용자 신원 및 소속기관 식별

eduroam은 연구·교육기관이 무선인터넷 자원을 공유하기 위한 서비스이다. 사용자 인증기관과 자원 제공기관이 물리적으로 분리되어 있기 때문에 사용자의 신원증명 등 기관 간 신뢰관계의 확보가 요구된다. 일반적으로 게스트 식별정보 제공자의 계정은 사용자에 의해 자가 관리되기 때문에 신원증명 수준이 낮은 단점이 있다. eduroam AND는 SAML 식별정보 제공자가 전달한 SAML 주장의 속성 값을 이용해 사용자와 소속기관을 식별함으로써 신원증명 수준을 높였다.

Table. 1 PHP code for SAML integration

```
<?php
  require_once('_autoload.php');
  $as =
    new SimpleSAML_Auth_Simple('default-sp');
  $as->requireAuth();
  $attributes = $as->getAttributes();
?>
```

표 1은 simpleSAMLphp API를 이용해 구현된 SAML 처리기 코드의 일부이다. SAML 자원 제공자의 객체($as)를 생성하고 웹 응용에 접근한 사용자의 인증 여부를 확인(requireAuth)한 후 인증된 사용자의 속성 값을 얻는데(getAttributes) 이용되는 코드이다. 연합 인증 환경에서 SAML 식별정보 제공자는 사용자 인증을 수행하고 인증된 사용자의 속성 값을 SAML 자원 제공자에게 전달한다. SAML 자원 제공자는 전달 받은 속성 값을 활용해 이용 권한을 부여하기 때문에 웹 응용 이용을 위한 사용자 계정을 유지하지 않아도 된다.

Table. 2 Attributes

Name	Description
eduPersonTargetedID	pseudonym identifier
displayName	display name
mail	e-mail address
eduPersonAffiliation	users's affiliation
organizationName	organization name
schacHomeOrganization	FQDN of user's org.

표 2는 eduroam AND에서 이용하는 사용자 속성 명과 의미를 보여준다. 속성들의 스키마(Schema)는 SCHAC[13], inetOrgPerson[14] 등에 정의되어 있다. eduPersonTargetedID는 고유 식별자로써 사용자 정보의 조합을 SHA256으로 암호화한 값이다. 사용자ID의 충돌과 개인정보의 노출을 방지하기 위해 eduPerson TargetedID를 이용했다. SAML 식별정보 제공자는 신원이 증명된 사용자에게만 해당 속성을 발급한다. eduPersonAffiliation은 사용자의 직무정보(예, faculty 등)를 의미한다. organizationName과 schacHome Organization은 각각 소속기관의 영문명과 도메인명(예, a-univ.ac.kr)에 해당한다.

eduroam AND는 사용자의 소속기관을 식별하기 위해 schacHomeOrganization 속성을 이용했다. 해당 속성은 공인된 도메인명을 값으로 갖기 때문에 기관명을 파싱(Parsing)하기 쉬운 장점이 있다. eduroam AND는 사용자 소속기관을 식별하기 위한 목적 이외에 서비스 접근권한과 이용권한의 부여를 위해 schacHome Organization 속성을 이용한다. 예를 들어, 직무정보와 기관명을 이용해 관리자 권한을 부여하거나 특정 기관명을 갖는 사용자의 서비스 접근을 제한할 수 있다.

최종적으로 이용권한을 부여받은 사용자는 eduroam 계정을 생성할 수 있게 된다. eduroam의 사용자ID는 [식별자]@[기관명].[국가코드]의 형태를 갖는다. MD5와 SHA1 암호화에 보안 취약점이 존재[15]하기 때문에 비밀번호는 SHA256으로 암호화한 후 사용자DB에 저장하게 구현되었다.

4.3. RADIUS 연동

RADIUS의 구성요소는 서버와 프록시(Proxy)를 포함한다. 서버는 사용자 인증 요청을 처리하며 프록시는 요청 및 응답메시지를 라우팅한다. eduroam AND와 연동된 RADIUS 서버와 프록시는 공개 소프트웨어인 FreeRADIUS[16]를 이용해 구축되었다.

RADIUS 서버는 eduroam AND에 등록된 사용자크리덴셜 정보를 이용해 eduroam 사용자를 인증한다. 일반적으로 ID/비밀번호 기반의 사용자 인증방식은 TLS(Transport Layer Security) 터널(Tunnel)을 생성하고 내부 인증프로토콜로 PAP(Password Authentication Protocol) 등을 사용한다.

Table. 3 EAP type vs. password compatibility

	Clear text	MD5 hash	SHA1 hash	SHA256 hash
PAP	○	○	○	○
CHAP	○	×	×	×
PEAP	○	×	×	×
EAP-MD5	○	×	×	×

표 3은 TLS 터널에 적용 가능한 내부 인증프로토콜을 예시한다. 또한 내부 인증프로토콜과 비밀번호 암호화 방식 간의 호환성을 보여준다. eduroam AND가 SHA256을 이용해 비밀번호를 암호화하기 때문에 내부 인증프로토콜도 SHA256과 호환되는 PAP로 설정되었다. 결과적으로, eduroam AND에 계정 정보를 보유한 사용자는 PAP를 내부 인증프로토콜로 갖는 EAP-TTLS (Extensible Authentication Protocol-Tunneled TLS) 방식으로 인증을 받게 된다. EAP[17]는 크리덴셜의 적용과 전송을 규정한 인증 프레임워크이다.

RADIUS 프록시는 연결 요청 및 응답 메시지들을 관리 영역(Realm) 간에 라우팅하는 역할을 한다. 프록시는 표 4와 같이 영역 정보를 저장하고 있는 일종의 라우팅 테이블을 유지한다. RADIUS 프록시는 이웃하는 프록시와 비밀키를 교환함으로써 신뢰관계를 확보하기 때문에 비밀키가 교환되지 않은 프록시 사이에는 통신이 불가능하다. 본 논문에서 별도의 언급이 없는 한 RADIUS 서버는 프록시를 포함하는 개념이다.

Table. 4 Configuration of RADIUS Proxy

```
realm ORGANIZATION.TLD {
  type = radius
  authhost = FLR_ADDRESS:PORT
  accthost = FLR_ADDRESS:PORT
  secret = SHARED_SECRET
  nostrip
}
```

[기관명].[국가코드](ORGANIZATION.TLD)는 관리 영역의 이름이며 사용자ID에 포함된 [기관명].[국가코드]와 동일한 형태를 갖는다. RADIUS 프록시에 인증 요청이 전달되면 사용자ID에 포함된 [기관명].[국가코드] 정보와 테이블의 영역 정보를 비교해 메시지를 라우팅한다. 메시지가 라우팅되어야 하는 이웃 RADIUS 프록시 또는 서버의 IP 주소와 포트번호는 authhost에 설정되었다. eduroam은 계정 서버의 정보를 설정하는 accthost는 이용하지 않는다.

4.4. 모니터링 및 가시화

eduroam 서비스의 국가단위 운영주체가 모니터링 정보를 공개하지 않거나 서버의 물리적 가용성 정보만을 제공하는 경우, 메시지 전달 과정에서 발생하는 오류의 원인을 파악하기 어렵게 된다. 또한 eduroam AND와 같은 웹 응용은 eduroam 서비스에 대한 사용자 접점으로 인식될 수 있기 때문에 사용자 지원을 위해 모니터링 기능을 자체적으로 확보해야 한다. eduroam AND는 사전 설정된 인증 요청 메시지를 FLR과 ILR 서버에 주기적으로 송신하고 피드백된 인증 메시지의 수신 여부를 파악함으로써 도달 가능성(Reachability)을 검사한다. 노드상태 수집기는 인증 메시지를 송·수신하고 결과를 해석하는 무선단말의 역할을 한다. 메시지의 도달 가능성을 검사하기 위해 WAP_supplicant(eapol_test)[18]를 이용했다. WPA_supplicant는 IEEE 802.11i 요청자(Supplicant)를 구현한 공개 소프트웨어로써 EAP-TTLS 등 다양한 인증 프로토콜을 지원한다.

Table. 5 Configuration for eapol_test

```
network ={
  ssid="eduroam"
  key_mgmt=WPA-EAP
  eap=TTLS
  identity="[test ID]"
  password="[test password]"
  phase2="auth=PAP"
}
```

표 5는 도달 가능성을 검사하기 위해 이용하는 환경설정 파일의 내용이다. 설정 파일은 eapol_test가 인증 요청 메시지를 송신하기 위해 사용하며 SSID, 검증용 사용자ID와 비밀번호, 인증 프로토콜 등이 정의된다.

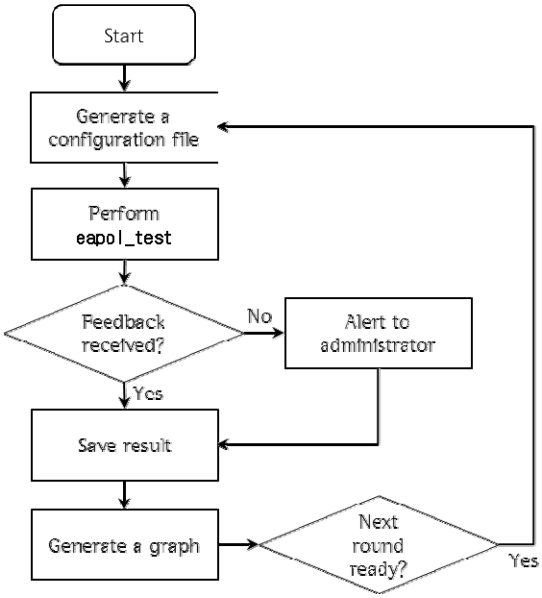


Fig. 5 Flowchart for active monitoring and visualization

그림 5는 eduroam AND에 구현된 모니터링 및 가시화 절차를 보여준다. 먼저 eduroam AND는 표 5에 예시된 환경설정 파일을 생성한다. 설정 파일이 동적으로 생성되게 구현함으로써 다양한 EAP 인증 프로토콜과 인증 환경에서 모니터링을 수행할 수 있다. 생성된 설정 파일과 eapol_test를 이용해 ILR과 FLR에게 인증 요청 메시지를 송신한다. 일정 시간 내에 응답 메시지를 수신하면 소요시간(Turnaround time)을 측정한 후 응답 메시지의 내용을 해석해 인증 성공 여부(Access-accept 또는 Access-reject)를 판별한다. 응답 메시지를 수신하지 못하면 관리자에게 전자우편으로 통보된다. eduroam AND는 측정 및 처리 결과를 상태 DB에 저장하고 공개 그래픽 라이브러리인 pChart[19]를 이용해 서비스 가용성 정보와 응답시간 정보를 그래프 파일로 생성한다.

Ⅴ. 구현 결과

본 장은 eduroam AND의 구현 결과를 제시하고 정성적으로 평가한다. eduroam AND 및 ILR 서버는 국가과학기술연구망(KREONET)에서 관리하는 국가단

위 RADIUS 서버와 연동됐으며 KAFE(Korean Access FEderation[20])에 참여 중인 연구기관과 교육기관의 구성원들을 대상으로 서비스되고 있다.

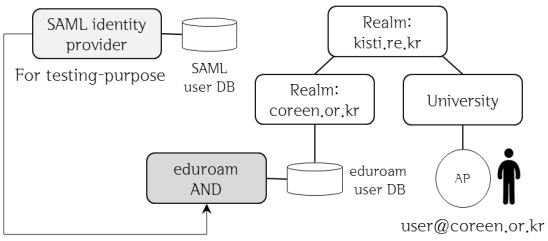


Fig. 6 Test environment

검증을 위해 그림 6과 같은 테스트 환경을 구축하고 모의 SAML 식별정보 제공자와 eduroam AND 간에 연합 인증이 가능하도록 설정했다. 구축된 RADIUS 서버의 관리 영역명은 coreen.or.kr이며 국가단위 RADIUS 서버인 kisti.re.kr과 직접 연동되었다.

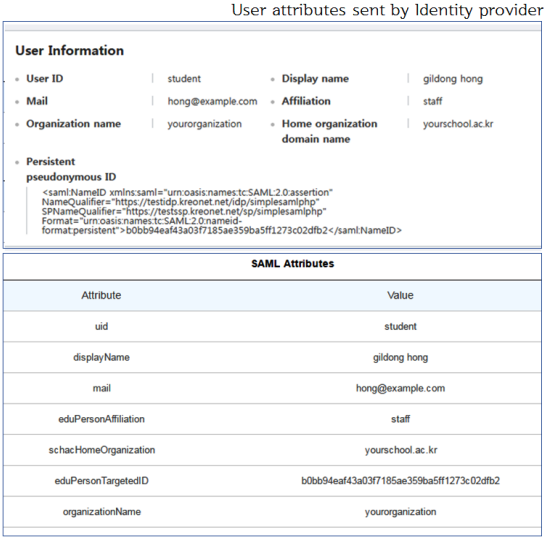


Fig. 7 User attributes

그림 7은 인증에 성공한 사용자의 속성 값을 모의 식별정보 제공자에서 출력한 내용(상단)과 SAML 응답 메시지를 수신한 자원 제공자(eduroam AND)에서 출력한 속성 값(하단)을 비교한다. 연합 인증을 통해 사용자의 신원증명과 기관식별이 가능함을 확인할 수 있다. 일반적으로 개별 기관이 식별정보 제공자일 경우, 구성원의 신원확인과 신원검사를 수행하기 때문에 연합 인증을 통해 확보한 사용자의 신원 정보는 신뢰할 수 있다고 볼 수 있다. 그림 상단과 하단의 NameID(Persistent pseudonymous ID와 eduPersonTargetedID)가 상이하게 표현되고 있으나 동일한 이름과 값을 갖는다.

Fig. 8 Creation of eduroam user account

그림 8은 eduroam 사용자 계정을 생성하기 위한 웹 GUI이다. 연합 인증을 통해 신원이 증명되고 소속기관이 식별된 사용자는 eduroam 사용자 계정을 생성할 수 있다. 구축된 RADIUS 서버가 eduroam 사용자를 최종적으로 인증해야하기 때문에 사용자는 RADIUS 서버의 관리 영역명(coreen.or.kr)을 포함하는 사용자ID를 갖게 된다. 연합 인증을 이용하면 이름, 전자우편 등 사용자 정보를 입력하지 않아도 사용자 속성 값으로부터 관련 정보를 확보할 수 있다는 장점이 있다.

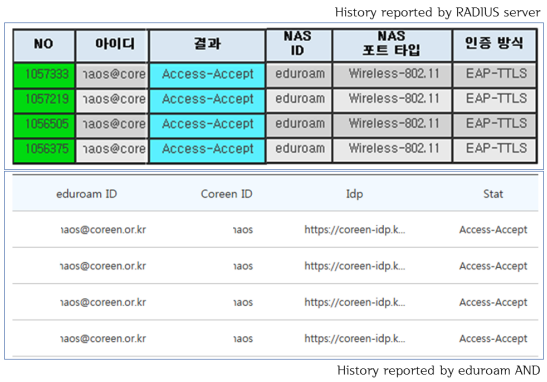


Fig. 9 Authentication history

그림 9는 무선 단말의 인증 요청에 대해 RADIUS 서버가 접속 허가(Access-accept)한 이력을 보여 준다. 사용자는 eduroam 서비스를 제공하는 국내 대학에서 무선인터넷 접속을 시도했다(그림 6 참조). 그림 9의 상단은 관리 영역이 kisti.re.kr인 RADIUS 서버가 제공한 사용자 인증 이력이다. 하단은 관리 영역이 coreen.or.kr인 RADIUS 서버의 인증 이력을 eduroam AND가 수집해 가시화한 그림이다. 인증 요청 메시지의 라우팅 거리가 최소 2홉(Hop) 이상이며 관리 영역이 coreen.or.kr인 RADIUS 서버에서 사용자가 최종적으로 인증되었음을 그림 9에서 확인할 수 있다. 결론적으로, eduroam AND가 국내 연구기관과 교육기관의 구성원들의 eduroam 사용자 인증을 위해 효과적으로 이용될 수 있음을 알 수 있다.

eduroam AND가 coreen.or.kr을 도메인으로 갖는 테스트 계정을 이용해 매 시간마다 두 RADIUS 서버들에게 인증 요청 메시지를 송신함으로써 서비스 가용성을 확인했다. 총 4,212회 인증 요청 메시지가 송신되었으며 RADIUS 서버 점검으로 인해 발생한 1회의 인증 실패를 제외하고 모두 정상적으로 인증되었다. 결과를 통해 eduroam AND를 이용한 사용자 인증이 신뢰성 있게 동작함을 확인할 수 있다.

Table. 6 Average turnaround time

	1 hop	2 hops
Turnaround time(ms)	312	644

표 6은 라우팅 거리에 따른 평균 소요시간(Turnaround time)을 보여준다. 소요시간은 eduroam AND에서 인증 요청 메시지를 송신한 후 응답 메시지를 수신할 때까지 걸린 시간으로 정의한다. 사용자 인증은 항상 관리 영역이 coreen.or.kr인 RADIUS 서버에서 수행되기 때문에 관리 영역이 kisti.re.kr인 RADIUS 서버에 인증 요청 메시지를 송신하면 총 2홉의 라우팅 거리를 갖게 된다. eduroam AND와 두 RADIUS 서버 간의 RTT(Round Trip Time)가 1ms 이하인 점을 감안하면 소요시간은 대부분 RADIUS 서버에서 발생한 것으로 추측된다. 국내에서는 라우팅 거리가 4홉 이하이기 때문에 eduroam 서비스에1~2초 이내로 접속할 수 있게 된다.

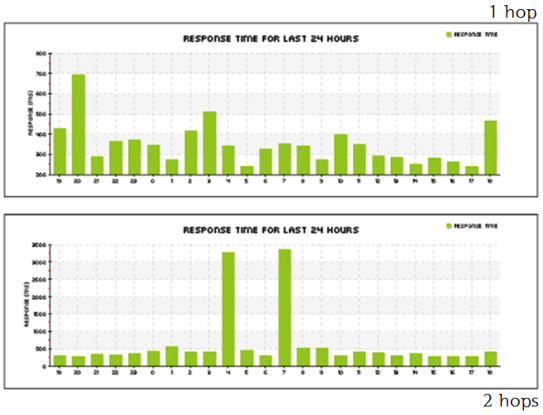


Fig. 10 Turnaround-time graph

eduroam AND는 소요 시간을 그림 10과 같이 가시화한다. 가용성 그래프는 지면 관계 상 생략한다. 그림의 상단과 하단은 각각 관리 영역이 coreen.or.kr인 RADIUS 서버와 kisti.re.kr인 RADIUS 서버에게 1시간 간격으로 인증 요청 메시지를 보내 소요 시간을 측정하고 그래프로 가시화한 것이다. 인증 처리에 소요되는 시간과 RADIUS 프록시의 가용성을 상시 모니터링해 가시화함으로써 오류의 원인 분석 등에 효과적으로 이용될 수 있을 것으로 판단된다.

Ⅵ. 결 론

본 논문은 eduroam 서비스의 이용 편의성 향상을 목적으로 개발된 eduroam AND를 소개하고 구현 결과를 평가하여 시스템의 적용 가능성을 검증했다. eduroam AND는 사용자에게 계정생성 권한을 부여하고 eduroam 서비스에 접속할 수 있게 함으로써 국내 연구기관과 교육기관 구성원들의 이동성 향상에 기여할 것으로 기대된다.

개발된 eduroam AND는 연합 인증을 통해 사용자의 소속기관을 식별하고 있다. 식별된 사용자와 소속기관의 증명 수준을 높이기 위한 방법과 SAML 식별정보 제공자를 eduroam 식별정보 제공자로 활용하는 방법에 대해서 추가적인 연구가 진행될 예정이다.

ACKNOWLEDGMENTS

This work was supported by K-16-L01-C02-S03 project, Korea Institute of Science and Technology Information.

REFERENCES

[1] D. W. Chadwick, "Federated Identity Management," in *Foundations of security analysis and design V*, New York, NY: Springer pub., part. 2, pp. 96-120, 2009.

[2] F. Licia and K. Wierenga, "Eduroam, providing mobility for roaming users," in *Proceedings of the EUNIS 2005 Conference*, Manchester, UK, 2005.

[3] IETF RFC 2865, *Remote authentication dial in user service (RADIUS)*, IETF, Fremont, C.A., 2000.

[4] W. A. Arbaugh, N. Shankar, and Y. J. Wan, "Your 802.11 Wireless Network has No Clothes," *IEEE Wireless Communications*, vol. 9, pp. 44-51, Dec. 2002.

[5] G. Wang, J. Cho, and G. Cho, "Global Wireless LAN Roaming Status in Korea and Its Development Methods," *Journal of the Institute of Electronics and Information Engineers*, Vol. 25, No. 7, pp. 1239-1245, July 2015.

[6] T. Niizuma and H. Goto, "Centralized Online Sign-up and Client Certificate Issuing System for eduroam," in *Proceedings of IEEE 38th Annual International Computers Software and Applications Conference Workshops*, Vasteras, Sweden, pp.174-179, July 2014.

[7] EduShib VA (Virtual Appliance) [Internet]. Available: http://infohub.sifulan.my/display/EV/EduShib+VA+Home

[8] The Shibboleth Project [Internet]. Available: http://shibboleth.internet2.edu/

[9] SimpleSAMLphp official homepage [Internet]. Available: https://simplesamlphp.org

[10] OASIS Std. sstc-saml-tech-overview-2.0-draft-08, *Security assertion markup language (saml) v2.0 technical overview*, OASIS, Burlington, M.A., 2005.

[11] IETF RFC 6749, *The OAuth 2.0 Authorization Framework*, IETF, Fremont, C.A., 2012.

[12] David Recordon and Drummond Reed, "OpenID 2.0: a platform for user-centric identity management," in *Proceedings of the second ACM workshop on Digital identity management*, New York: NY, pp. 11-16, 2006.

[13] IETF RFC 6338, *Definition of a Uniform Resource Name (URN) Namespace for the Schema for Academia (SCHAC)*, IETF, 2011.

[14] IETF RFC 2798, *Definition of inetOrgPerson LDAP Object Class*, IETF, 2000.

[15] T. Chad and R. Svetlana, "The security of cryptographic hashes," in *Proceedings of the 49th Annual Southeast Regional Conference*, Kennesaw: GA, pp. 103-108, 2011.

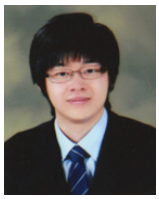
[16] FreeRADIUS official homepage [Internet]. Available: http://freeradius.org/

[17] IETF RFC 3748, *Extensible authentication protocol (EAP), IETF, Fremont*, C.A., 2004.

[18] Linux WPA/WPA2/IEEE 802.1X Supplicant [Internet]. Available: http://w1.fi/wpa_supplicant/

[19] pChart – a PHP class to build charts [Internet]. Available: http://pchart.sourceforge.net

[20] KAFE [Internet]. Available: https://coreen.kreonet.net



이경민(KyoungMin Lee)

안동대학교 컴퓨터공학과 공학석사
한국과학기술정보연구원 연구원
※관심분야 : 네트워크, TCP/IP, QoS, 웹 서비스

조진용(Jinyong Jo)

광주과학기술원 정보통신학과 공학석사
광주과학기술원 정보통신학과 공학박사
한국과학기술정보연구원 선임연구원
※관심분야 : Collaboration application and service, Federated ID management

공정욱(JongUk Kong)

㈜ 데이콤 선임연구원
㈜ 맥스웨이브 책임연구원
충남대학교 정보통신학과 공학박사
한국과학기술정보연구원 책임연구원
※관심분야 : 네트워크 자원 제어, SDN