

글로벌무선로밍서비스(eduroam) 가입 신청서

본 기관은 'eduroam 규정'과 '글로벌무선로밍서비스 전국 대학 운영 규정'에 동의하고 준수할 것을 약속하며 아래와 같이 가입 신청합니다.

IdP/SP : _____ 역할
기관명(직책) : _____ (_____)
서명 : _____ 날짜: _____

- ※ 이 문서에 서명함으로써 eduroam IdP와 eduroam SP는 'eduroam 규정'과 '글로벌무선로밍서비스 전국 대학 운영 규정'에 기술된 규칙을 지켜야 하며, 규칙을 지키지 않을 때는 무선랜을 공동 활용 할 수 없고 'eduroam'이라는 이름 등을 사용할 수 없음을 의미합니다.
- ※ 일반적으로는 Idp/SP 역할을 동시에 하지만, 무선랜인증서버가 없는 경우에는 SP역할만 가능합니다.
- ※ 교육 및 연구기관을 제외한 타 기관(ISP, 지방자치단체 등)에서 eduroam 사용자를 위해 망을 개방한 경우에는 이들 기관은 SP역할만 수행합니다.
- ※ 정보서비스를 담당하고 있는 기관장서명 후 스캔하여 홈페이지(www.eduroam.kr) 에 기관관리자 아이디로 등록하면, 운영센터 검토과정을 거쳐 가입 승인됩니다.

교육(대학)기관 글로벌무선로밍서비스 운영 규정문 v.1.0

eduroam(15)01- 2015년 5월 15일

본 규정문은 글로벌무선로밍서비스(이하, eduroam서비스) 대한민국 국가 eduroam 운영자(National Roaming Operator, 이하 NRO)인 한국과학기술정보연구원(KISTI)의 위임을 받아, 대한민국 교육(대학)기관에 eduroam 서비스를 제공함에 있어, Roaming Operator(이하, RO), 방문기관 서비스제공자(SP)와 소속기관 계정관리자(IdP)가 지켜야 할 최소한의 기술적, 관리적 표준을 기술한다.

이 문서는 기술변화나 RO, 그리고 각 eduroam 사용자로부터의 의견을 수렴하여 eduroam서비스 대한민국 교육(대학)기관 운영조직의 실무위원회(IdP/SP) 검토와 기술 및 정책위원회 의결로 수정할 수 있다. 수정된 문서는 버전관리를 통해 관리되며, 이는 선행 버전에 동의한 기관까지 그 영향을 받는다.

1. 용어

가. eduroam

eduroam은 사용자가 속한 IdP에 의해 발급된 사용자 본인 계정에 의한 신원확인을 통해 안전한 네트워크 접근 서비스를 제공한다.

나. eduroam Identity Provider (eduroam IdP)

사용자 Id 관리와 해당 사용자의 eduraom 접근을 위한 인증서버 제공자이다. IdP는 "소속기관"이라고도 부른다.

다. eduroam Service Provider (eduroam SP)

소속 eduraom에 의해 인증이 된 사용자들에게 Internet 서비스를 사용할 수 있도록 Access망을 운영하는 기관이다. "방문 기관"이라고도 부른다.

라. Roaming Operator (RO)

RO는 'eduroam 운영자'라고 불리며, 대한민국 교육(대학)기관 eduroam RO는 NRO의 위임을 받아 전남대학교에서 그 역할을 수행한다.

마. RADIUS Proxy Server (RPS)

RPS는 eduroam 서비스를 제공하기 위해 Authentication(인증), Authorization(인가), Accounting(사용량)의 관리를 제공하는 RADIUS Server 간 계층구조를 갖고 상호 간접적으로 연결해주는 중계 체계다.

2. 사용자 확인 절차

eduroam은 eduroam SP망에 접속한 사용자의 신원 확인 절차를 수행한다. 사용자 신원 확인은 eduroam SP와 eduroam IdP 사이에 내부 EAP 터널을 통해 식별한다. 사용자 신원 확인을 위해 충분한 로깅 정보를 eduroam SP 및 eduroam IdP에 기록해야 한다. eduroam IdP는 사용자를 분명하게 확인할 책임이 있다. 사용자 확인 절차는 eduroam SP에게 전달되는 것을 명시적으로 포함하고 있지는 않다.

3. eduroam EAP 패킷 전송을 위한 기술

RO 또는 SP에 의해 운영되는 RPS는 반드시 자신이 받은 EAP 메시지를 수정하지 않고 eduroam 라우팅 방식에 따라 전달해야 한다.

4. RO가 지켜야 할 관리적 기술적 요건들

가. RO는 eduroam 서비스가 잘 동작하게 하는 책임이 있다.

나. RO는 eduroam IdP가 해당 국가의 교육과 연구 기관에 속한 기관인지에 대한 적격성을 판단할 권한을 갖는다.

다. RO는 eduroam SP의 적격성을 판단할 권한을 갖는다. 해당 eduroam SP가 기술적 요구조건을 만족하고 모든 eduroam 사용자에게 차별없이 무료로 서비스를 제공한다면 적격성에 문제가 없다.

라. RO는 사용 가능한 eduroam SP 정보를 홈페이지에 게시 한다.

마. RO는 요구조건이나 문제 해결 방식 등의 변화를 소통할 수 있도록 eduroam SP들과 대화 채널을 반드시 수립하여야 한다.

바. RO는 지정한 웹 페이지를 통해 다음과 같은 정보를 최소한 포함한 eduroam 서비스에 대한 정보를 발표하여야 한다.

- IdP 리스트와 eduroam 사용가능 지역을 나타내는 목록이나 지도 및 각 SP의 웹 페이지 접근 URL
- eduroam 서비스 및 메일링 리스트 관리 책임이 있는 적절한 기술지원팀과 상세 연락 정보

사. RO는 eduroam IdP와 eduroam SP가 사용자의 신원 확인 절차가 성공적으로 종료될 수 있도록 충분한 로그 정보를 유지해야 한다.

5. eduroam IdP의 관리적, 기술적 조건

가. eduroam IdP는 반드시 eduroam 라우팅 체제에 연결하기 위해 RADIUS 인터페이스를 구현해야 한다.

나. eduroam IdP는 반드시 관할 사용자들을 위해 무선과 유선망에 적합한 EAP 방식을

구현하여 상호 인증 및 단대단 인증서를 암호화해야 한다.

- 다. eduroam IdP는 반드시 접근 요청을 받은 이용 자격이 있는 관할 지역 사용자들을 위해 'RADIUS 승인' 메시지를 보내야 한다.
- 라. eduroam IdP는 인증되지 않는 불법 사용자에게 대해서는 반드시 'RADIUS 승인' 메시지를 보내지 않아야 한다.
- 마. eduroam IdP들은 자신의 사용자들에게 필요한 지원을 해야 한다. 어떤 지원은 협력과 해결을 위해 RO수준에서 지원될 수 있다.
- 바. eduroam IdP들은 모든 인증 시도에 대해 로그 정보를 저장해야 하며, 로그 정보에는 다음과 같은 내용들이 포함되어야 한다. 이 정보는 달리 규정이 없는 한 최소 6개월은 저장하여야 한다.
 - 인증 요청 및 응답에 대한 타임스탬프
 - 인증 요청의 외부 EAP 아이덴티티 (User-Name 속성)
 - 내부 EAP 아이덴티티 (실 사용자 식별자)
 - 연결한 클라이언트 MAC 주소 (Calling-Station-Id 속성)
 - 인증 응답 종류 (즉, 수락 또는 거절)

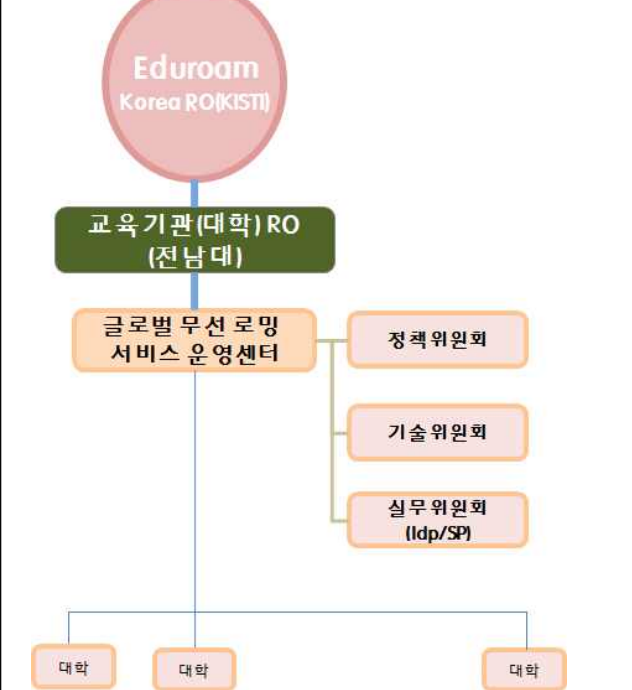
6. eduroam SP의 관리적, 기술적 조건

- 가. eduroam SP는 반드시 eduroam 시스템에 연결하기 위해 802.1X를 사용한 RADIUS 인터페이스를 구현해야 한다.
- 나. IEEE 802.11 무선망을 제공하는 SP는 반드시 SSID로 'eduroam'을 broadcast해야 한다. 만일 동일 장소에 하나 이상의 eduroam SP가 존재한다면 'eduroam-'형태의 SSID를 사용할 수 있다.
- 다. IEEE 802.11 무선망 SP는 반드시 WPA2+AES를 지원해야 한다.
- 라. eduroam SP는 라우팅 가능한 IP주소를 공급해야하며, NAT를 제공할 수 있다.
- 마. eduroam SP는 eduroam 참여자가 목적지인 EAP 메시지를 수정없이 eduroam 하부구조에 전달해야 한다.
- 바. eduroam SP는 eduroam 사용자에게 접근망 사용에 대한 요금을 청구해서는 안된다.
- 사. eduroam SP의 서비스는 각자의 정책에 의해 제공된다. 그러나, 사용자 접근 정보 (예, 임의의 포트나 응용 계층의 프락시를 거절하기 위한 접근 목록이나 방화벽 필터 규칙) 등은 수정해서는 안되며, 이런 일이 필요한 경우에는 해당 RO에게 반드시 보고하여야 한다.
- 아. eduroam SP는 책임 있는 Id 제공자를 인식할 수 있도록 로그인 한 사용자에게 대해 다음과 같은 정보를 기록함으로써 충분한 로그 정보를 저장해야 한다. 이 정보는

달리 규정이 없는 한 최소 6개월은 저장하여야 한다.

- 인증 요청 및 응답에 대한 타임스탬프
- 인증 요청의 외부 EAP 아이덴티티 (User-Name 속성)
- 연결한 클라이언트 MAC 주소 (Calling-Station-Id 속성)
- 인증 응답 종류 (즉, 수락 또는 거절)
- 만일 public 주소가 사용된 경우 로그인 후 발행된 3계층의 IP주소와 2계층의 MAC 주소 사이의 상관관계 정보 (예, ARP 스니핑 로그나 DHCP 로그)

교육(대학)기관 글로벌무선로밍서비스(eduroam) 조직도

조직도	역할	
	구분	주요 업무
 <p>The diagram shows the organizational structure of Eduroam. At the top is a red circle labeled 'Eduroam Korea RO(KISTI)'. Below it is a green rectangle labeled '교육기관(대학) RO (전남대)'. This is connected to an orange rectangle labeled '글로벌 무선 로밍 서비스 운영센터'. To the right of this center are three stacked orange rectangles: '정책위원회', '기술위원회', and '실무위원회 (ldp/SP)'. At the bottom, three orange rectangles labeled '대학' are connected to the '글로벌 무선 로밍 서비스 운영센터'.</p>	정책위원회	-운영규정 재개정 -정책방향 등 주요의사결정 -적용 기술 검토 자문
	기술위원회	-관리에 따른 운영 규정 조정 -실무위원회 이슈 사항 조정 -대외협력
	실무위원회	-각 대학 인증 서버 운영 -무선랜과 관련 네트워크 운영 -운영센터 Contact Point
	글로벌로밍서비스운영센터	-NRO와 협력 -Radius Proxy 서버 운영 -회원 대학 연동 기술 지원 및자문 -관리시스템 운영 -위원회 활동 지원