글로벌무선로밍서비스(eduroam) 가입 신청서

본 기관(대학)은 'eduroam 규정'에 동의하고 준수 할것을 약속하며 아래와 같이 가입 신청합니다.

IdP/SP		대학은 IdP+SP로 신청
기관명(직책)		
서명		날짜 :

※ 이 문서에 서명함으로써 eduroam IdP와 eduroam SP는 'eduroam 규정' 기술된 규칙을 지켜야 하며, 규칙을 지키지 않을 때는 무선랜을 공동 활용할 수 없고 'eduroam' 이라는 이름 등을 사용할 수 없음을 의미합니다.

※ 일반적으로 각 대학은 Idp/SP 역할을 동시에 수행합니다.

※ 교육 및 연구기관을 제외한 타 기관(ISP, 지방자치단체 등)에서 eduroam 사용자를 위해 망을 개방하였을 때 이들 기관은 SP 역할로 가입합니다.

※ 정보서비스를 담당하는 기관장 서명 후 스캔하여 홈페이지(www.eduroam.kr)에 기관관리자 아이디로 등록하면, 운영센터 검토 과정을 거쳐 승인됩니다.

eduroam 운영 규정 문 v.2.0

2024년 11월 1일

한국교육정보화재단(KREN) IAM 센터에서 eduroam 로밍서비스를 제공하기 위해 방문 기관 서비스제공자(SP)와 소속기관 계정관리자(IdP)가 지켜야 할 최소한의 기술적, 조직적 표준을 기술한다.

원활한 운영을 위해 아래 표1과 같은 조직을 구성하여 운영한다.

주요 기관		주요 역할
운영센터		▪ 안전하고 신뢰성 있는 운영관리 ▪ 정책에 명시된 내용을 준수하는 서비스 제공 ▪ 참여기관의 운영 담당자에 대한 기술지원 ▪ 소프트웨어의 시험, 솔루션의 추천 및 문서화, 매뉴얼 제공 등 ▪ 국내외 관계기관 및 타 ID 연합 간 협력 ▪ 잠재적 참여기관에 대한 홍보 ▪ 정책 개정의 발의 ▪ 참여기관의 회원 승인을 위한 발의 ▪ 안전하고 신뢰성 있는 운영을 방해하는 참여기관에 대해 제명 발의 ▪ 참여기관의 목록 및 적용된 기술 프로파일에 대한 정보 공개 ▪ 특정 기술 프로파일을 이용하는 참여기관에 대한 정보 공개
위원회	정책위원회	▪ 정책 개정의 승인 ▪ 참여기관 가입 자격에 대한 심의 및 가부 결정 ▪ 참여기관의 제명 승인 ▪ 타 ID 연합과의 연계에 대한 심의 및 승인 ▪ 추진 업무 및 발전 방향에 대한 자문 ▪ 기타 사항의 심의 및 승인
	기술분과 위원회	▪ 구체적인 사안의 조사·검토 및 작업 등을 실시 ▪ 정책위원회 위원장의 요구에 응하여 작업 등을 실시하고, 그 결과에 대해 정책위원회에 보고 또는 심의 사항 제안
	실무분과위원회	▪ 참여하는 기관들의 운영 요원으로 구성하며, 서비스의 기술적, 운영적 문제들을 협의하고 해결

1. 용어

1.1 eduroam

eduroam은 사용자가 속한 IdP에 의해 발행된 사용자 본인의 신임장에 의한 신원확인을 통해 안전한 네트워크 접근 서비스를 제공한다.

1.2 eduroam Identity Provider (eduroam IdP)
사용자 Id 관리와 해당 사용자의 eduroam 접근을 위한 인증 서버 제공자이다. IdP는 "소속기관"이라고도 부른다.

1.3 eduroam Service Provider (eduroam SP)
소속 eduraom에 의해 인증이 된 사용자들에게 Internet 서비스를 사용할 수 있도록 접근망을 운영하는 기관이다. "방문 기관"이라고도 부른다.

1.4 Roaming Operator (RO)
RO는 'eduroam 운영자'라고 불리기도 한다. 한국교육정보화재단 IAM센터

1.5 RADIUS Proxy Server (RPS)
RPS는 eduroam 서비스를 제공하기 위해 기술적인 하부 시스템 (RADIUS 계층구조 서버) 을 제공하기 위해 수립되고 유지된다.

2. 사용자 확인 절차
2.1 eduroam은 eduroam SP의 망에 접속한 각 사용자의 신원확인을 위한 기술들을 사용한다. 사용자 확인 절차는 eduroam SP와 사용자의 eduroam IdP 사이에 사용자의 내부 EAP 신원을 확인하기 위해 eduroam 통신 외적인 방법으로 정의된다. 사용자 신원확인을 위해 충분한 로깅 정보를 eduroam SP 및 eduroam IdP에 기록해야 한다. eduroam IdP는 사용자를 분명하게 확인할 책임이 있다. 사용자 확인 절차는 이 사용자 확인이 eduroam SP에게 전달되는 것을 명시적으로 포함하고 있지는 않다.

3. eduroam EAP 패킷 전송을 위한 기술
3.1 RO 또는 SP에 의해 운영되는 RPS는 반드시 자신이 받은, eduroam 참여자에게 전달되어야 할 EAP 메시지를 수정하지 않고 eduroam 라우팅 방식에 따라 전달되어야 한다.

4. RO가 지켜야 할 관리적 기술적 요건들
4.1 RO는 eduroam 서비스가 잘 동작하게 하는 책임이 있다.
4.2 RO는 eduroam IdP가 해당 국가의 교육과 연구기관에 속한 기관인지 에 대한 적격성을 판단할 권한을 갖는다.
4.3 RO는 eduroam SP의 적격성을 판단할 권한을 갖는다. 해당 eduroam

SP가 기술적 요구조건을 만족하고 모든 eduroam 사용자에게 차별 없이 무료로 서비스를 제공한다면 적격성에 문제가 없다.

4.4 RO는 사용할 수 있는 eduroam SP 정보를 홈페이지에 게시한다.

4.5 RO는 요구조건이나 문제 해결 방식 등의 변화를 소통할 수 있도록 eduroam SP 들과 대화 채널을 반드시 수립하여야 한다.

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

4.6.1 IdP 리스트와 eduroam 사용 가능 지역을 나타내는 목록이나 지도 및 각 SP의 웹 페이지 접근 URL

4.6.2 eduroam 서비스 및 메일링 리스트 관리 책임이 있는 적절한 기술 지원팀과 상세 연락 정보

4.7 RO는 eduroam IdP와 eduroam SP가 사용자의 신원확인 절차가 성공적으로 종료될 수 있도록 충분한 로그 정보를 유지해야 한다. 이 목표를 성취하기 위한 수단들은 eduroam 설명문 부록 A, B에 기술되어 있다.

5. eduroam IdP 및 SP의 관리적, 기술적 조건

5.1 eduroam IdP 및 SP의 요구조건은 이 문서의 부록 A와 B에 나열되어 있다. 이러한 요구조건들은 기술변화나 RO 그리고 각 eduroam 사용자로부터의 의견 수렴으로 변경될 수 있다. 변경 사항은 버전 관리를 통해 관리되며, 이 문서의 선행 버전에 동의한 단체에 영향을 미친다.

이 문서에 서명함으로써 eduroam IdP와 eduroam SP는 여기에 기술된 규칙을 지킨다.

이런 규칙을 지키지 않을 때는 무선랜을 공동 활용할 수 없으며, 이는 eduroam 이름 등을 사용할 수 없음을 의미한다.

eduroam 설명문 부록

A. eduroam Identity 제공자를 위한 관리적 기술적 조건들

A.1 eduroam IdP는 반드시 eduroam 라우팅 체제에 연결하기 위해 RADIUS 인터페이스를 구현해야 한다.

A.2 eduroam IdP는 반드시 관할 사용자들을 위해 무선과 유선망에 적합한 EAP 방식을 구현하여 상호 인증 및 단대단 인증서를 암호화해야 한다.

A.3 eduroam IdP는 반드시 접근 요청을 받은 이용 자격이 있는 담당 지역 사용자들을 위해 'RADIUS 승인' 메시지를 보내야 한다.

A.4 eduroam IdP는 인증되지 않는 불법 사용자에 대해서는 반드시 'RADIUS 승인' 메시지를 보내지 않아야 한다.

A.5 eduroam IdP들은 자신의 사용자들에게 필요한 지원을 해야 한다. 어떤 지원은 협력과 해결을 위해 RO 수준에서 지원될 수 있다.

A.6 eduroam IdP 들은 모든 인증 시도에 대해 로그 정보를 저장해야 한다; 그리고 로그 정보에는 다음과 같은 내용들이 포함되어야 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)

달리 규정이 없는 한 최소 6개월은 저장하여야 한다.

B. eduroam 서비스제공자(SP)를 위한 관리적 기술적 조건들

B.1 eduroam SP는 반드시 eduroam 시스템에 연결하기 위해 802.1X를 사용한 RADIUS 인터페이스를 구현해야 한다.

B.2 IEEE 802.11 무선망을 제공하는 SP는 반드시 SSID로 'eduroam'을 broadcast 해야 한다. 만일 동일 장소에 하나 이상의 eduroam SP가 존재한다면 'eduroam-'형태의 SSID를 사용할 수 있다.

B.3 IEEE 802.11 무선망 SP는 반드시 WPA2+AES를 지원해야 한다.

B.4 eduroam SP는 라우팅할 수 있는 IP주소를 제공해야 하며, NAT를 제공할
수 있다.

B.5 eduroam SP는 eduroam 참여자가 목적지인 EAP 메시지를 수정 없이 eduroam 하부구조에 전달해야 한다.

B.6 eduroam SP는 eduroam 사용자에게 접근망 사용에 대한 요금을 청구해서는 안된다.

B.7 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 안 되며, 이런 일이 필요한 경우에는 해당 RO에 반드시 보고하여야 한다.

B.8 eduroam SP는 책임 있는 Id 제공자를 인식할 수 있도록 로그인 한 사용자에 대해 다음과 같은 정보를 기록함으로써 충분한 로그 정보를 저장해야 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 사용되었으면 로그인 후 발행된 3계층의 IP주소와 2계층의 MAC 주소 사이의 상관관계 정보 (예, ARP 스니 핑 로그나 DHCP 로그)

달리 규정이 없는 한 최소 6개월은 저장하여야 한다.