

# Charte eduroam (FR)

---

## 1. Introduction

eduroam (**education roaming**) a pour objectif d'offrir des accès réseaux sécurisés aux utilisateurs de la communauté Éducation-Recherche internationale.

Le service eduroam en France est géré par RENATER, qui veille à la mise en place d'une infrastructure d'authentification répartie pour la communauté Éducation-Recherche. Cette infrastructure s'appuie sur le protocole RADIUS et permet l'accès au réseau avec un identifiant unique sur tous les sites des établissements qui sont membres d'eduroam.

Tout établissement membre d'eduroam s'engage auprès de RENATER au respect des spécifications techniques de mise en œuvre (se référer à la présente Charte et au document «eduroam Policy Service Definition» en vigueur sur le site [www.eduroam.org](http://www.eduroam.org)).

## 2. Définitions

### Établissement membre

Un établissement membre de la Fédération eduroam est un établissement ayant demandé à RENATER l'accès au service eduroam, soit en tant que fournisseur d'identités (établissement de rattachement), soit en tant que fournisseur du service (établissement visité) et pour lequel l'infrastructure organisationnelle et technique permettant l'accès à eduroam pour ses Utilisateurs ou les Utilisateurs visiteurs est en place.

Il existe deux types d'Établissements membres pour eduroam :

- **Établissement de rattachement (fournisseur d'identités)** : établissement de la communauté Éducation-Recherche proposant l'accès à eduroam à ses Utilisateurs au sein de l'Établissement ou lorsque ceux-ci sont en déplacement dans un Établissement visité. L'Établissement de rattachement gère les ressources informatiques mises à disposition de ses Utilisateurs. Ces ressources sont généralement accessibles nominativement via un identifiant et un mot de passe. L'Établissement de rattachement est fournisseur d'identités.
- **Établissement visité (fournisseur de service)** : établissement, autre que l'établissement de rattachement, où se trouve l'Utilisateur visiteur du service eduroam. Son rôle est de permettre l'accès à eduroam aux Utilisateurs provenant d'Établissements de rattachement membres d'eduroam en fournissant un accès Internet sécurisé aux Utilisateurs.  
Un Établissement de rattachement est un Établissement visité lorsqu'il donne accès au Service eduroam à un Utilisateur d'un autre Établissement de rattachement.

## Fédération eduroam

Ensemble des Établissements ayant souscrit au Service eduroam, soit en tant que fournisseur d'identité, soit en tant que fournisseur de services.

## Service eduroam

Infrastructure technique d'authentification répartie pour la communauté Éducation-Recherche permettant d'offrir aux Utilisateurs la possibilité d'utiliser, lors de leurs déplacements, les infrastructures réseau des autres Établissements membres en utilisant l'identité numérique professionnelle qui est authentifiée par son Établissement de rattachement.

## Utilisateur / Utilisateur visiteur

Un utilisateur du Service eduroam est :

- soit un personnel administratif, technique, chercheur, enseignant, appartenant à un établissement de la communauté Éducation-Recherche ayant un agrément RENATER ;
- soit un étudiant appartenant à un établissement de la communauté Éducation-Recherche ayant un agrément RENATER.

### 3. Conditions d'accès à eduroam

- Pour l'Établissement de rattachement (fournisseur d'identités) :

Seuls les établissements ayant un agrément RENATER peuvent être fournisseurs d'identités. L'Établissement de rattachement s'engage à respecter les « engagements en tant qu'établissement de rattachement » (cf. article 4) et à faire respecter la charte déontologique de RENATER par ses Utilisateurs.

- Pour l'Établissement visité (fournisseur de services) :

Les établissements n'appartenant pas à la communauté Éducation-Recherche ou n'ayant pas d'agrément RENATER peuvent être fournisseurs de services, sous réserve de la signature de présente la charte eduroam et de l'acceptation par RENATER.

### 4. Engagements en tant qu'Établissement de rattachement (fournisseur d'identités) :

En tant qu'Établissement de rattachement, celui-ci s'engage à :

- être également un Établissement visité (fournisseur de service), c'est à dire permettre l'accès à eduroam aux Utilisateurs d'un autre Établissement de rattachement ;
- mettre en œuvre un service d'authentification de ses Utilisateurs via un serveur RADIUS ;
- mettre en œuvre une méthode d'authentification conforme au niveau de sécurité demandé ;
- informer ses Utilisateurs sur l'existence du service et la façon d'y accéder ;

- informer ses Utilisateurs sur l'obligation, lors de leurs déplacements, de respecter la charte déontologique RENATER et la charte informatique du réseau de l'Établissement visité ;
- offrir un service d'assistance à ses Utilisateurs.
- Concernant la protection des données à caractère personnel, RENATER attire l'attention sur le fait que les journaux d'activités sont assimilés à de la cybersurveillance et que celle-ci nécessite une déclaration au registre de l'Établissement. L'Établissement de rattachement doit remplir les obligations suivantes :
  - la déclaration des journaux de connexion au registre des traitements de l'Établissement ;
  - la sécurisation de ces journaux ;
  - la conservation de ces journaux pour une durée raisonnable (1 an maximum) ;
  - la sécurisation des identifiants de ses Utilisateurs ;
  - l'information des Utilisateurs de la collecte de leurs données à caractère personnelle.

## 5. Engagements en tant qu'Établissement visité (fournisseur de services)

En tant qu'Établissement visité, celui-ci s'engage à :

- offrir le service eduroam à travers des points d'accès sans fil et une infrastructure conforme aux spécifications techniques de mise en œuvre ;
- mettre à disposition des Utilisateurs d'eduroam de l'information sur le service et sur ses conditions d'utilisation ;
- lorsque l'activité de l'Utilisateur est surveillée par l'Établissement visité, celui-ci doit annoncer clairement ce fait, en incluant comment cela est surveillé, stocké et accessible ;
- coopérer avec RENATER pour tout ce qui concerne la mise en œuvre et l'exploitation du service eduroam.
- Concernant la protection des données à caractère personnel, RENATER attire l'attention sur le fait que les journaux d'activités sont assimilés à de la cybersurveillance et que celle-ci nécessite une déclaration au registre de l'Établissement. L'Établissement visité doit remplir les obligations suivantes :
  - la déclaration des journaux d'utilisation d'eduroam au registre de l'Établissement ;
  - la sécurisation de ces journaux ;
  - la conservation de ces journaux pour une durée raisonnable (1 an maximum) ;
  - l'information des Utilisateurs de la collecte de leurs données à caractère personnelle.

## 6. Engagements communs sur la sécurisation du service

### Signalisation des incidents

Les membres d'eduroam doivent aviser RENATER de tout incident de sécurité lié à eduroam.

### Protection des données d'authentification des utilisateurs

Les identifiants et mots de passe des utilisateurs, transitant via l'infrastructure eduroam, doivent être chiffrés de bout en bout, c'est à dire entre leur poste de travail et le serveur d'authentification de leur établissement de rattachement.

### Protection du trafic des Utilisateurs

Les Établissements membres doivent mettre en œuvre des méthodes de chiffrement efficaces sur les points d'accès sans fil donnant accès au service eduroam, conformément au document «eduroam Policy Service Definition» en vigueur.

### Serveurs RADIUS

Les serveurs RADIUS doivent être installés et gérés suivant les règles de bonnes pratiques en matière d'installation, de configuration, d'administration et de sécurité afin d'offrir le niveau de sécurité et de confiance nécessaire à l'infrastructure.

Il est souhaitable d'avoir une infrastructure redondante protégée par des pare-feu ou routeurs filtrants.

### Traçabilité

Les mesures appropriées doivent être mises en œuvre pour pouvoir identifier l'utilisateur d'une adresse IP (IPv4 ou IPv6) à un moment donné.

### Informations

Les établissements membres d'eduroam qu'il soit Établissement de rattachement (fournisseurs d'identités) ou Établissements visités (fournisseur de services) doivent communiquer à RENATER au moins un contact technique.

Toute modification de coordonnées doit être notifiée à RENATER.

### Suspension du service

RENATER se réserve le droit de suspendre l'accès au service aux membres d'eduroam enfreignant les règles énoncées dans la présente charte eduroam.