# Charte eduroam (FR)

## 1. Introduction

eduroam (**edu**cation **roam**ing) 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 membres.

Tout établissement membre d'eduroam s'engage auprès de RENATER au respect des spécifications techniques de mise en œuvre (se référer au document «eduroam Policy Service Definition» en vigueur sur le site www.eduroam.org).

Il existe deux types de membres pour eduroam :

- Établissement de rattachement (fournisseur d'identités) : établissement gérant les ressources informatiques mises à disposition des utilisateurs dans le cadre de leurs activités professionnelles ou académiques. Ces ressources sont généralement accessibles nominativement via un identifiant et un mot de passe.

  Seuls les établissements ayant un agrément RENATER peuvent être fournisseurs d'identités.

- Établissement visité (fournisseur de services) : établissement, autre que l'établissement de rattachement, où se trouve l'utilisateur du service eduroam. Le rôle des fournisseurs de service eduroam est de fournir un accès Internet sécurisé aux utilisateurs.

  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 la charte eduroam et de l'acceptation par RENATER.

## 2. Engagement 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 visiteurs 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.

## 3. Engagement 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) eduroam ;
- 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 RENATER et celle du réseau étranger les accueillant ;
- offrir un service d'assistance à ses utilisateurs.

## 4. Engagements communs sur la sécurisation du service

Les participants à 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 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 de rattachement (fournisseurs d'identités) et les 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 charte eduroam.

### Obligations légales

Les obligations relatives à la loi informatiques et liberté doivent être remplies par les fournisseurs de services et les fournisseurs d'identité. Notamment :

- pour les établissements visités :
  - la déclaration des journaux d'utilisation d'eduroam auprès de la CNIL ;
  - la sécurisation de ces journaux ;
  - l'information des utilisateurs ;
  - la conservation de ces journaux pour une durée raisonnable.
- pour les établissements de rattachement :
  - la déclaration des journaux de connexion auprès de la CNIL ;
  - la sécurisation de ces journaux ;
  - la conservation de ces journaux pour une durée raisonnable ;
  - la sécurisation des identifiants de leurs utilisateurs ;

- l'information des utilisateurs ;

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 spécifique auprès de la CNIL.

## 5. 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 du service (établissement visité) soit en tant que fournisseur d'identité (établissement de rattachement) et pour lequel l'infrastructure organisationnelle et technique permettant l'accès à eduroam pour ses utilisateurs ou les utilisateurs visiteurs est en place.

### Participant

Un participant à eduroam est un établissement membre de la fédération eduroam.

### Utilisateur

Un utilisateur est :

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

### Établissement de rattachement

Un établissement de rattachement est un établissement de la communauté Éducation-Recherche ayant un agrément RENATER. Cet établissement propose l'accès à eduroam à ses utilisateurs au sein de l'établissement ou lorsque ceux-ci sont en déplacement dans un établissement visité. Il s'engage à respecter les « engagements en tant qu'établissement de rattachement » (cf. chapitre 3).

### Établissement visité

Un établissement visité est un établissement permettant aux utilisateurs provenant d'établissements participants l'accès à eduroam.