Énoncé de conformité d'eduroam

Ce document énonce les normes techniques et organisationnelles minimales s'appliquant aux exploitants de services d'itinérance (RO) et aux confédérations de services d'itinérance (RC) qui souhaitent dispenser le service d'itinérance mondial eduroam. L'application de ces normes nécessite une coordination de la part des RO et des RC.

Le Global eduroam Governance Committee (GeGC) pourra modifier ce document d'après les commentaires formulés par les RO, les RC ou les utilisateurs d'eduroam. Les modifications éventuelles seront gérées par versionnage et par les méthodes de gestion du changement pertinentes de la TERENA.

Le GeGC, que coordonne la TERENA, se compose de représentants des RO et des RC. Ce sont ses membres qui ont rédigé le présent document. Tout commentaire s'y rapportant devrait être envoyé à <gegc@terena.org> afin que le GeGC puisse en prendre connaissance.

Les litiges concernant le statut d'une entité (fournisseur d'identités, fournisseur de services, exploitant de service d'itinérance) que le RO ou la RC responsable du service eduroam ne peut résoudre seront transmis au GeGC, qui rendra la décision finale.

1. Terminologie

1.1. eduroam

eduroam est un service fédéré d'itinérance garantissant un accès sécurisé à un réseau par authentification de l'utilisateur au moyen des identifiants que lui a attribués son fournisseur d'identités.

1.2. Fournisseur d'identités eduroam (IdP eduroam)

Entité chargée de fournir les identifiants à l'utilisateur et exploitant un serveur d'authentification avec lequel ledit utilisateur pourra accéder au service eduroam. Dans certaines régions, on appelle les IdP « institutions d'origine ».

1.3. Fournisseur de services eduroam (SP eduroam)

Entité qui exploite un réseau au moyen duquel l'utilisateur d'eduroam peut accéder à l'internet après avoir été authentifié par son IdP. Dans certaines régions, les SP portent le nom d'« institutions d'accueil ».

1.4. Exploitant de service d'itinérance (RO)

Entité qui exploite le service eduroam, reconnue par la RC à laquelle elle appartient ou par le GeGC, si la zone économique ou le pays dans lequel se trouve l'entité en question ne compte pas de RC locale. Il pourrait s'agir, par exemple, de l'exploitant du Réseau national de la recherche et de l'éducation. On appelle parfois le RO « exploitant du service eduroam ».

1.5. Serveur de procuration RADIUS (RPS)

Les RPS servent d'infrastructure technique (à savoir, la hiérarchie de serveurs RADIUS) au service eduroam mondial.

La RC locale exploite les RPS situés au sommet de la hiérarchie dans une région donnée. En l'absence de RC locale, c'est le GeGC, guidé par les RO locaux, qui désigne les RO responsables des principaux RPS de la région.

1.6. Confédération de services d'itinérance (RC)

Entité composée d'un ensemble cohérent de RO desservant une région et reconnue comme telle par le GeGC. La « confédération européenne des services eduroam » en est un exemple.

2. Identification de l'utilisateur

2.1. eduroam recourt à des technologies permettant d'identifier chaque utilisateur qui accède à un réseau de SP eduroam. Le SP eduroam et l'IdP eduroam de l'utilisateur communiquent hors bande pour établir l'identité interne de ce dernier au moyen du protocole EAP. Pour que cette méthode fonctionne, le SP eduroam et l'IdP eduroam doivent enregistrer des données suffisantes dans leurs journaux d'exploitation. Grâce à elle, l'IdP eduroam responsable est en mesure d'identifier sans erreur l'utilisateur qui souhaite accéder au réseau d'un SP eduroam. Ainsi, on évite expressément la transmission des identifiants de l'utilisateur au SP eduroam.

3. Conformité technique pour le transfert des paquets EAP d'eduroam

3.1. Le RPS qu'exploite une RC, un RO, un IdP eduroam ou un SP eduroam DOIT relayer, sans les modifier, les messages EAP qu'il reçoit et qui sont destinés aux participants du réseau eduroam au serveur RADIUS correspondant (de la RC, du RO ou de l'IdP) déterminé par le système de routage établi et validé par le GeGC.

4. Conformité administrative et technique des RO

4.1. Le RO garantit l'exploitation du service eduroam dans un pays ou une zone économique donnés.

4.2. Le RO peut aussi avoir pour responsabilité de veiller à l'exploitation du service eduroam dans un autre pays ou une autre zone économique si aucune entité adéquate n'est en mesure et n'accepte de le faire. Pareil cas nécessite une autorisation explicite de la RC de la région dont fait partie le pays ou la zone économique en question ou du GeGC, si aucune RC n'a été établie dans le pays ou la zone économique concernés.

4.3. Le RO peut établir l'admissibilité de l'IdP eduroam, donc des organisations qui poursuivent des activités de recherche ou d'enseignement, dans son pays ou sa zone économique.

4.4. Le RO peut établir l'admissibilité du SP eduroam dans son pays ou sa zone économique. Aucune restriction ne s'applique à l'admissibilité du SP eduroam pourvu que celui-ci respecte les exigences techniques d'eduroam et que les utilisateurs d'eduroam puissent tous accéder gratuitement à ses services, quelle que soit leur origine.

4.5. Le RO DOIT établir des canaux de communication avec les autres RO, soit par l'entremise d'une RC, soit en recourant à la liste des exploitants régionaux du service eduroam. Le RO DOIT pouvoir être rejoint par ce canal dans un délai raisonnable.

4.6. Le RO DEVRAIT publier l'information sur les points de présence eduroam disponibles (sites des SP) dans son pays ou sa zone économique de la manière adéquate, telle qu'établie par le GeGC.

4.7. Le RO DOIT établir des canaux de communication avec les SP eduroam de son pays ou de sa zone économique afin de leur signaler les changements apportés aux exigences et de résoudre les problèmes.

4.8. Le RO DOIT afficher l'information concernant les services eduroam sur une page Web réservée à cela. Au strict minimum, cette page fournira les renseignements que voici :

4.8.1. une mention confirmant l'adhésion à une politique de la RC (s'il y a lieu), avec un lien url menant à cette politique;

4.8.2. la liste des IdP et une liste ou une carte indiquant l'étendue des zones que couvre le service eduroam, avec un lien vers la page Web de chaque SP eduroam;

4.8.3. les coordonnées du service de soutien technique pertinent, responsable du service eduroam et des listes de diffusion.

4.9. Le RO DOIT s'assurer que les IdP eduroam et les SP eduroam de son pays ou de sa zone économique conservent assez de données dans un journal pour que les utilisateurs puissent être correctement identifiés. Les annexes A et B indiquent comment y parvenir.

4.10. Le RO DOIT enregistrer le nom et le logo d'eduroam comme une marque de commerce dans son pays ou sa zone économique s'ils n'ont pas déjà été enregistrés en tant que marque de commerce de la TERENA. Quand la RC locale d'un pays ou d'une zone économique, ou le GeGC s'il n'y en a pas, ne reconnaît plus une entité comme RO, l'entité en question DOIT céder la propriété des marques de commerce à la TERENA.

5. Conformité administrative et technique des IDP eduroam et des SP eduroam

5.1. Les annexes A et B du présent document énumèrent les exigences applicables aux IdP eduroam et aux SP eduroam. Ces exigences peuvent être modifiées pour des raisons techniques ou à la suite des commentaires formulés par les RO, les RC ou les utilisateurs du service. Les modifications retenues par la majorité des membres du GeGC seront introduites par versionnage et devront être adoptées par toutes les parties qui ont ratifié une version antérieure du présent document.

En ratifiant ce document, le RO ou la RC déclare unilatéralement qu'elle appliquera et respectera les règles qu'il énumère. En ratifiant ce document, la RC s'engage à faire en sorte que les RO qui la composent appliquent et respectent les règles qu'on y trouve. En ratifiant ce document, le RO s'engage à faire en sorte que les IdP eduroam et les SP eduroam de son pays ou de sa zone économique appliquent et respectent les règles qui y sont décrites.

Une RC ou un RO qui déroge aux règles en question pourrait ne plus être reconnu comme tel et se voir priver du droit d'utiliser le nom, le logo et la marque de commerce d'eduroam.

La RC/le RO de : (pays, zone économique / plusieurs)

Ratifié par : (nom du RO / de la RC)

Signature : Date :

Annexes à l'énoncé de conformité d'eduroam

A. Conformité administrative et technique du fournisseur d'identités (IdP) eduroam

A.1. L'IdP eduroam DOIT mettre en place une interface RADIUS qui lui permettra de se connecter au système de routage d'eduroam.

A.2. L'IdP eduroam DOIT adopter une méthode reposant sur le protocole EAP pour l'ensemble des utilisateurs locaux. Cette méthode doit convenir aux réseaux sans fil et permettre une authentification mutuelle de même que l'encryptage intégral des identifiants.

A.3. L'IdP eduroam DOIT envoyer un message de confirmation RADIUS pour les utilisateurs locaux en règle qui ont été authentifiés et souhaitent accéder à son réseau.

A.4. L'IdP eduroam NE DOIT PAS envoyer de message de confirmation RADIUS pour les utilisateurs qui ne sont pas en règle ou qui n'ont pas été authentifiés.

A.5. L'IdP eduroam DOIT dispenser du soutien technique à ses utilisateurs. Les problèmes techniques peuvent être relayés au RO ou à la RC aux fins de coordination et de résolution.

A.6. L'IdP eduroam DOIT consigner toutes les tentatives d'authentification dans un journal. Les informations qui suivent DOIVENT être enregistrées :

- référence temporelle de la demande d'authentification et de la réponse fournie;
- identité externe du protocole EAP dans la demande d'authentification (attribut User-Name);
- identité interne du protocole EAP (identifiant de l'utilisateur réel);
- adresse MAC du client se connectant (attribut Calling-Station-Id);
- réponse à la demande d'authentification (à savoir, acceptation ou refus).

Ces informations doivent être conservées au moins six mois, sauf exigence contraire dans la réglementation nationale.

B. Conformité administrative et technique des fournisseurs de services (SP) eduroam

B.1. Le réseau du SP eduroam DOIT respecter la norme 802.1X et disposer d'une interface RADIUS lui permettant de se connecter à l'infrastructure d'eduroam.

B.2. Le réseau sans fil IEEE 802.11 du SP eduroam DOIT diffuser le SSID « eduroam ». S'il y a plusieurs SP eduroam au même endroit, on POURRA utiliser un SSID qui commence par « eduroam ».

B.3. Le réseau sans fil IEEE 802.11 du SP eduroamp DOIT accepter le protocole de sécurité WPA2+AES et PEUT accepter le protocole WPA/TKIP à titre de courtoisie à l'endroit de ceux qui possèdent des appareils l'utilisant encore. Exceptionnellement, un SP établi avant le 1er janvier 2012 PEUT n'accepter que le protocole WPA/TKIP, mais pas ceux établis après le 1er janvier 2013.

B.4. Le réseau du SP eduroam DOIT fournir l'adresse IP et une infrastructure à configuration automatique pour la résolution DNS.

B.5. Le réseau du SP eduroam DEVRAIT fournir des adresses IP pouvant être routées et PEUT offrir la traduction des adresses réseau.

B.6. Le SP eduroam DEVRAIT retransmettre les messages EAP-destinés aux participants d'eduroam à l'infrastructure d'eduroam sans les modifier.

B.7. Le SP eduroam NE DOIT PAS facturer l'utilisateur ni les IdP eduroam pour accéder à son réseau.

B.8. Les services du SP eduroam s'appuient sur les politiques locales. Toutefois, on décourage vivement d'apporter la moindre modification à la connexion de l'utilisateur (à savoir, listes d'accès ou règles de filtrage du pare-feu bloquant certains ports ou procurations pour la couche d'applications). Les modifications de cette nature DOIVENT être signalées au RO concerné.

B.9. Le SP eduroam DEVRAIT conserver suffisamment d'informations pour qu'on puisse identifier le fournisseur d'identités responsable de l'utilisateur qui s'est connecté. On enregistrera dans un journal les données qui suivent :

- référence temporelle de la demande d'authentification et de la réponse fournie;
- identité externe du protocole EAP dans la demande d'authentification (attribut User-Name);
- identité interne du protocole EAP (identifiant de l'utilisateur réel);
- adresse MAC du client se connectant (attribut Calling-Station-Id);
- réponse à la demande d'authentification (à savoir, acceptation ou refus);
- corrélation des informations entre l'adresse de couche 2 (MAC) du client et l'adresse de couche 3 (IP) attribuée après la connexion, si on utilise une adresse publique (p. ex., journaux de reniflage ARP ou journaux DHCP).

Ces informations doivent être conservées au moins six mois, sauf indication contraire dans la réglementation nationale.

FAQ sur l'énoncé de conformité

Q : Au point 3.1, on indique que les messages EAP DOIVENT être transférés sans modification. Cette exigence empêche-t-elle l'exploitant de retrancher les attributs du LAN virtuel ou de stopper les attaques par force brute?

R : Les paquets RADIUS contiennent le message EAP et d'autres attributs, comme les attributs d'affectation à un LAN virtuel. Seul le message EAP doit rester intact. Les attributs du LAN virtuel peuvent être modifiés ou supprimés, si besoin est.

Veuillez noter aussi que cette exigence ne s'applique qu'aux serveurs de procuration. Une attaque par force brute viendra d'un point d'accès sans fil (le réseau d'un SP eduroam, par exemple). Le SP eduroam pourra l'empêcher (exigence B.6, qui est conditionnelle). Si le SP décide de retransmettre la demande à un IdP, le serveur de procuration situé entre les deux ne devrait pas interférer.

Le but de cette exigence est de s'assurer qu'aucun serveur de procuration ne mette fin à une séance EAP (à savoir, ne retransmette pas la demande et coupe le canal de communication). Un tel comportement ne sera pas toléré.

Q : L'exigence 4.6 prescrit que les informations sur le point d'accès soient formatées d'une certaine manière. Pourquoi doit-on choisir un format aussi commun?

R : L'information sert à compiler plusieurs documents sur les utilisateurs (une carte mondiale des points d'accès sans fil, par exemple). Créer une carte cohérente de la planète serait impossible – ou alors techniquement très difficile – si l'information concernant les points d'accès sans fil était fragmentée ou formatée de différentes façons.

Q : L'exigence 5.1 dit « En ratifiant ce document, le RO s'engage à faire en sorte que les IdP eduroam et les SP eduroam de son pays ou de sa zone économique appliquent et respectent les règles qui y sont décrites. » Comment le RO peut-il respecter une telle exigence?

R : Une bonne façon de le faire serait que faire signer aux IdP eduroam et aux SP eduroam du pays ou de la zone économique une déclaration qui les engage à appliquer et à respecter les règles établies. S'il constate qu'un IdP eduroam ou un SP eduroam enfreint les règles en question par la suite, le RO prendrait les mesures nécessaires pour y remédier.