Déclaration de conformité d'eduroam

Introduction

1.1 Ce document énonce les normes techniques et organisationnelles minimales que les exploitants (RO) et les confédérations (RC) du service d'itinérance doivent respecter pour offrir le service mondial d'itinérance eduroam. Les RO et les RC devront se coordonner pour appliquer ces normes.

1.2 Le GeGC (*Global eduroam Governance Committee*) peut modifier en tout temps ce document en fonction des commentaires formulés par les RO, les RC ou les utilisateurs du service. Les modifications seront apportées selon le processus du versionnage et les méthodes employées par GÉANT pour vérifier les modifications. Ce document pourrait être enrichi ou être remplacé par une entente plus précise.

1.3 Le GeGC, que coordonne GÉANT, se compose de représentants des RO et des RC qui ont rédigé le document. Les commentaires sur le document devraient être envoyés à <gegc@lists.geant.org> afin d'être examinés. La charte du GeGC décrit de façon plus détaillée les liens entre le GeGC et GÉANT.

1.4 Si le statut d'une entité (IdP, SP, RO) du service eduroam engendre un litige que le RO ou le RC concerné ne peut résoudre, la décision finale sera rendue par le GeGC.

1.5 PARFOIS, il arrive qu'on doive retrancher un IdP, SP, RO ou RC afin de se conformer aux lois ou aux exigences légales auxquelles l'équipe d'exploitation principale d'eduroam ou les exploitants du service doivent se plier. La communauté eduroam sera mise au courant de telles décisions.

1.6 Les SP, IdP, RO et RC d'eduroam DOIVENT tous se conformer aux règles applicables à la protection des données.

1.7 Les termes et expressions « DOIT », « NE DOIT PAS », « EST TENU » « DEVRA », « NE DEVRA PAS », « DEVRAIT », « NE DEVRAIT PAS », « IL EST RECOMMANDÉ », « POURRA », « FACULTATIF » et autres expressions similaires qui figurent dans ce document seront interprétées de la façon indiquée dans le document RFC 2119 [RFC2119].

1.8 Définitions

eduroam	Service fédéré d'itinérance garantissant un accès sécurisé au réseau grâce à l'authentification de l'utilisateur au moyen des identifiants qui lui ont été attribués par son IdP.
Équipe d'exploitation principale d'eduroam	Équipe qui s'occupe des différents aspects du service eduroam au nom des exploitants du service (RO). Les membres de l'équipe sont nommés par GEANT.

Fournisseur d'identités eduroam {ldP)	Entité responsable des identifiants de l'utilisateur et de l'usage d'eduroam par ce dernier. Dans certaines régions, on parle aussi d'« institutions d'accueil ».
Fournisseur de service eduroam (SP)	Entité qui exploite un réseau auquel les utilisateurs d'eduroam peuvent accéder afin de parcourir l'internet après avoir été authentifiés par leur ldP. Dans certaines régions, on parle aussi d'« institutions visitées ».
Exploitant du service d'itinérance (RO)	Entité qui exploite le service eduroam dans un pays ou une zone économique et que reconnaît la RC à laquelle elle est affiliée ou le GeGC, si le pays ou la zone économique en question se trouve dans une zone géographique où aucune RC n'a été établie. Le RO pourrait, par exemple, être l'exploitant d'un réseau zone économiqueal de la recherche et de l'éducation. On parle aussi parfois d'« exploitant d'eduroam ».
Serveur de procuration RADIUS (RPS)	Les RPS sont mis en place et entretenus pour servir d'infrastructure technique (hiérarchie des serveurs RADIUS) au service eduroam mondial. La RC d'une région donnée exploite les RPS du niveau supérieur. En l'absence de RC dans une région, c'est le GeGC, conseillé par les RO locaux, qui désigne les RO chargés d'exploiter les RPS de la région en question.
Confédération du service d'itinérance (RC)	Entité formée d'un regroupement de RO desservant une région et reconnue comme telle par le GeGC. La « confédération européenne d'eduroam » en est un exemple.

2. Conformité administrative et technique des RO, RC, ldP et SP

2.1. eduroam utilise des technologies permettant d'identifier chaque utilisateur qui accède au réseau des SP. Le RO a pour responsabilité de s'assurer que l'identification de chaque utilisateur est unique.

2.2 L'utilisateur et l'IdP eduroam déterminent par quel mécanisme d'authentification réciproque on vérifiera l'identité de l'utilisateur. L'IdP eduroam doit remettre les identifiants d'une façon sécurisée (de préférence hors bande) afin que l'utilisateur dispose d'une identité unique et puisse vérifier l'authenticité de l'IdP par authentification réciproque.

2.3 Le processus d'identification a besoin d'informations suffisantes pour identifier l'utilisateur. Ces informations seront conservées par l'exploitant du service d'itinérance, le SP eduroam et l'IdP eduroam. Ce processus n'exige pas nécessairement la divulgation de l'identité de l'utilisateur ni la transmission de cette identité par le SP eduroam (on préconise l'usage d'un protocole externe d'identification anonyme ou EAP pour protéger les renseignements personnels).

2.4. Le RPS exploité par la RC, le RO, l'ldP ou le SP eduroam DOIT relayer les messages EAP (identité externe comprise) qu'ils reçoivent et sont destinés aux utilisateurs d'eduroam sans les modifier au serveur RADIUS approprié (de la RC, du RO ou de l'ldP), tel que déterminé par le système de routage d'eduroam établi et approuvé par le GeGC.

3. Conformité administrative et technique des RO

3.1. Le RO veille au bon fonctionnement du service eduroam dans un pays ou une zone économique donnés.

3.2. Parfois, il arrive que le RO veille aussi au bon fonctionnement du service dans une autre pays ou une autre zone économique s'il n'y existe aucune entité appropriée pour cela. La RC de la zone géographique concernée devra donner une autorisation explicite en ce sens ou on devra obtenir cette autorisation du GeGC, si le pays ou la zone économique se trouve dans une région où aucune RC n'a été établie.

3.3. Le RO a le pouvoir d'établir l'admissibilité des IdP eduroam, c'est-à-dire des organisations du pays ou de la zone économique qui poursuivent des activités de recherche ou d'enseignement.

3.4. Le RO a le pouvoir d'établir l'admissibilité des SP eduroam dans le pays ou la zone économique concernés. Aucune restriction ne s'applique à l'admissibilité des SP eduroam pourvu que les exigences techniques aient été respectées et que les utilisateurs puissent tous accéder gratuitement à eduroam, peu importe leur origine.

3.5. Le RO DOIT établir des canaux de communication avec les autres RO. Il pourra le faire en passant par une RC ou en utilisant la liste des exploitants régionaux du service eduroam. Le RO DOIT s'assurer que les informations le concernant dans la base de données d'eduroam sont complètes et exactes (https://monitor.eduroam.org/). Le RO DOIT pouvoir être rejoint dans un délai raisonnable par les canaux appropriés.

3.6. Le RO DEVRAIT publier les informations relatives aux points de présence d'eduroam (sites des SP) disponibles dans le pays ou la zone économique concernés d'une manière adéquate, telle qu'établie par le GeGC.

3.7. Le RO DOIT établir des canaux de communication avec les SP eduroam dans son pays ou sa zone économique afin de leur signaler les modifications et de résoudre les problèmes éventuels.

3.8. Le RO DOIT afficher l'information concernant les services eduroam sur des pages web dédiées, soit au minimum ce qui suit.

3.8.1. Un énoncé confirmant l'adhésion à la politique de la RC (s'il y a lieu), avec un lien url.

3.8.2. La liste des ldP et une liste ou une carte indiquant les zones couvertes par le service eduroam avec des liens menant à la page web de chaque SP eduroam.

3.8.3. Les coordonnées des membres du personnel de soutien technique responsables du service eduroam et la ou les listes de distribution.

3.9. Le RO DOIT s'assurer que les ldP et SP eduroam de son pays ou de sa zone économique gardent suffisamment d'informations pour que les utilisateurs puissent être identifiés. Les annexes A et B proposent des moyens pour cela.

3.10. 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 ne l'ont pas déjà été comme une marche de commerce de GÉANT. Quand la RC d'une région, ou le GeGC s'il n'y a pas de RC dans cette région, ne reconnaît plus l'entité servant de RO dans un pays ou une zone économique faisant partie de ladite région, l'entité concernée DOIT céder la propriété des marques de commerce à GÉANT.

4. Conformité administrative et technique des ldP et des SP d'eduroam

4.1. Les annexes A et B du présent document énonce les exigences que doivent respecter les ldP et les SP eduroam. Ces exigences peuvent varier en fonction des progrès de la technologies et des commentaires formulés par les RO, les RC, les ldP, les SP ou les utilisateurs d'eduroam. Les modifications sanctionnées par une majorité des membres du GeGC seront gérées par versionnage et DOIVENT être signalées aux RO et aux RC par courriel dans les dix (10) jours qui précèdent leur entrée en vigueur. Ces modifications s'appliqueront à toutes les parties qui utilisent eduroam (à savoir, les RO, les RC, les ldP et les SP).

4.2 En ratifiant ce document, le RO ou la RC déclare unilatéralement appliquer et respecter les règles qui y sont énoncées. En ratifiant ce document, la RC s'engage à faire en sorte que les RO qu'elle regroupe appliquent et respectent les règles qui y sont énoncées. En ratifiant ce document, le RO s'engage à faire en sorte que les ldP et les SP eduroam de son pays ou de sa zone économique appliquent et respectent les règles qui y sont énoncées. En ratifiant ce document, le RO ou la RC convient que cette Déclaration de conformité à eduroam remplace les déclarations antérieures ratifiées par le RO ou la RC.

4.3 Ne pas adhérer aux règles du présent document pourrait entraîner la non-reconnaissance de l'entité comme RC ou RO et l'empêcher d'utiliser le nom, le logo et la marque de commerce d'eduroam.

RC/RO pour : (pays, zone économique, multiple de)

Signé par : (nom du RO ou de la RC)

Signature : Date:

Annexes à la Déclaration de conformité d'eduroam

A. Conformité administrative et technique des fournisseurs d'identités (IdP) eduroam

A.1. L'IdP eduroam DOIT installer une interface RADIUS pour se connecter à l'Infrastructure d'eduroam.

A.2. L'IdP eduroam DOIT appliquer à l'ensemble des utilisateurs qui lui sont affiliés un protocole EAP qui convient aux réseaux sans fil et filaires, et permet l'authentification réciproque ainsi que l'encryptage des identifiants de bout en bout.

A.3. L'IdP eduroam DOIT envoyer un message RADIUS de confirmation aux utilisateurs qui ont demandé à accéder au réseau et dont l'identité a été authentifiée.

A.4. L'IdP eduroam DOIT envoyer un message RADIUS de refus aux utilisateurs qui n'ont pas le droit d'accéder au réseau ou dont l'identité n'a pu être authentifiée.

A.5. L'IdP eduroam DOIT procurer un soutien technique à ses utilisateurs. Les questions relatives au soutien technique peuvent être relayées au RO ou à la RC afin qu'ils les coordonnent ou y répondent.

A.6. L'IdP eduroam DOIT enregistrer toutes les tentatives d'authentification en consignant TOUTES les informations que voici :

- horodatage de la demande d'authentification et réponse à la demande;
- identité EAP externe de la demande d'authentification (attribut User-Name);
- identité EAP interne (identifiant réel de l'utilisateur);
- adresse MAC du client qui se connecte (attribut Calling-Station-Id);
- SP visité par l'utilisateur grâce à l'attribut Operator-Name, s'il existe;
- pays visité de la demande au moyen de l'attribut eduroam-SP-country, s'il existe;
- nature de la réponse à l'authentification (à savoir, authentification acceptée ou refusée).

Ces informations doivent être conservées au moins trois mois, à moins que la réglementation de la zone économique n'ait d'autres exigences.
L'IdP eduroam DEVRAIT fournir un attribut Chargeable-User-Identity (attribut CUI de RADIUS) pour faciliter l'identification de l'utilisateur par le réseau SP visité.

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

B.1. Le réseau du SP eduroam DOIT se connecter à l'infrastructure eduroam avec une infrastructure RADIUS respectant la norme 802.lX de l'IEEE.

B.2. Le réseau sans fil IEEE 802.11 du SP DOIT diffuser le SSID « eduroam ». S'il y a plus d'un SP eduroam au même endroit, on POURRA se servir d'un autre SSID, pourvu qu'il débute par « eduroam ».

Si le SP eduroam n'est pas le réseau d'origine d'un IdP (à savoir, s'il fait partie d'une autre infrastructure d'itinérance), on POURRA y accéder par Passpoint / Hotspot 2.0 en recourant à un identifiant RCOI (*Roaming Consortium Organisation Identifier*) de GÉANT dans 001BC50460 ou à l'identifiant spécifiquement attribué au réseau d'itinérance par GÉANT.

B.3. Le SP eduroam DEVRAIT diriger l'authentification des clients du réseau Passpoint / Hotspot 2.0 eduroam vers l'infrastructure, mais il POURRAIT choisir de recourir à la découverte dynamique des pairs (au moyen des enregistrements NAPTR) pour chercher l'infrastructure.

B.4. Le réseau sans fil IEEE 802.11 du SP eduroam DOIT accepter la norme WPA2+Enterprise (éventuellement par compatibilité).

B.5. Le réseau du SP eduroam DOIT diffuser l'adresse IP et l'infrastructure de configuration automatique du résolveur DNS.

B.6. Le réseau du SP eduroam DEVRAIT fournir des adresses IP routables et POURRAIT en donner la traduction NAT.

B.7. Le SP eduroam DOIT relayer tous les messages EAP destinés aux participants d'eduroam à l'infrastructure eduroam sans les modifier, identification externe comprise.

B.8. Le SP eduroam NE DOIT PAS facturer l'utilisateur ni son IdP eduroam pour avoir accès à son réseau.

B.9. Le SP eduroam applique les politiques locales. Cependant, on décourage vivement la modification du contenu des connexions (à savoir, listes d'accès ou règles de filtrage du pare-feu en vue d'interdire arbitrairement certaines publications ou procurations de la couche applications) et toute modification de ce genre DOIT être signalée au RO concerné.

8.10. Le SP eduroam DEVRAIT garder suffisamment d'informations pour qu'on puisse identifier le fournisseur d'identités de l'utilisateur qui s'est connecté en les consignant ou en les relayant. Ces informations comprennent les suivantes :

- horodatage de la demande d'authentification et réponse correspondante;
- identité EAP externe dans la demande d'authentification (attribut User-Name);
- adresse MAC du client qui se connecte (attribut Calling-Station-Id);
- adresse MAC et SSID du point d'accès auquel l'utilisateur s'est connecté (attribut Called-Station-Id, mais il n'est pas toujours disponible);
- identifiant du SP dans l'attribut Operator-Name (le RO POURRAIT le fournir);
- nature de la réponse à la demande d'authentification (acceptation ou rejet);
- attribut CUI (Chargeable-User-Identity) si l'IdP le diffuse;
- précisions sur la corrélation entre l'adresse de la couche clients (MAC) et l'adresse de la couche 3 (IP) diffusées après la connexion quand on se sert d'une adresse publique (p. ex., journaux DHCP).

Ces informations seront conservées au moins trois mois, à moins que la règlementation de la zone économique n'ait d'autres exigences.