



[Créer un compte](#)  
[Se connecter](#)

# Extensible Authentication Protocol

20 langues

Article [Discussion](#) Lire [Modifier](#) [Modifier le code](#) [Voir l'historique](#) Outils

☐ Pour les articles homonymes, voir [EAP](#).

**Extensible Authentication Protocol** ou **EAP** est un protocole de communication réseau embarquant de multiples méthodes d'authentification, pouvant être utilisé sur les liaisons [point à point](#) (RFC 2284 <sup>1</sup>), les [réseaux filaires](#) et les [réseaux sans fil](#) (RFC 3748 <sup>2</sup>, RFC 5247 <sup>3</sup>) tels que les réseaux [Wi-Fi](#).

Plusieurs méthodes d'authentification sont prédéfinies ([MD5](#), [OTP](#), Generic Token Card, etc.) mais il est possible d'en rajouter sans qu'il soit nécessaire de changer ou de créer un nouveau [protocole réseau](#) .

## Le protocole EAP [ [modifier](#) | [modifier le code](#) ]

Le protocole EAP est :

- Un **protocole de communication réseau** : il est constitué d'un échange de trames dans un format spécifique à EAP pour réaliser l'authentification d'un partenaire <sup>RFC 1</sup>
- Un **protocole extensible** : quelques méthodes d'authentification sont prédéfinies ([MD5](#), [OTP](#), Generic Token Card, etc.) mais d'autres peuvent être ajoutées sans qu'il soit nécessaire de changer le protocole réseau ou d'en définir un nouveau <sup>RFC 2</sup>

Le protocole EAP a été proposé en **mars 1998** dans la RFC 2284 <sup>4</sup> et **proposé comme standard Internet** auprès de l'IETF.

Il est conçu pour fournir un mécanisme d'authentification pour les liaisons [PPP](#) ([couche 2 du modèle OSI](#)) afin d'autoriser ou interdire l'établissement de la [couche réseau](#) ([couche 3 du modèle OSI](#)) <sup>RFC 1</sup>. Ce protocole ne s'appuie donc pas sur le protocole [IP](#) ([couche 3 du modèle OSI](#)) <sup>RFC 3</sup>.

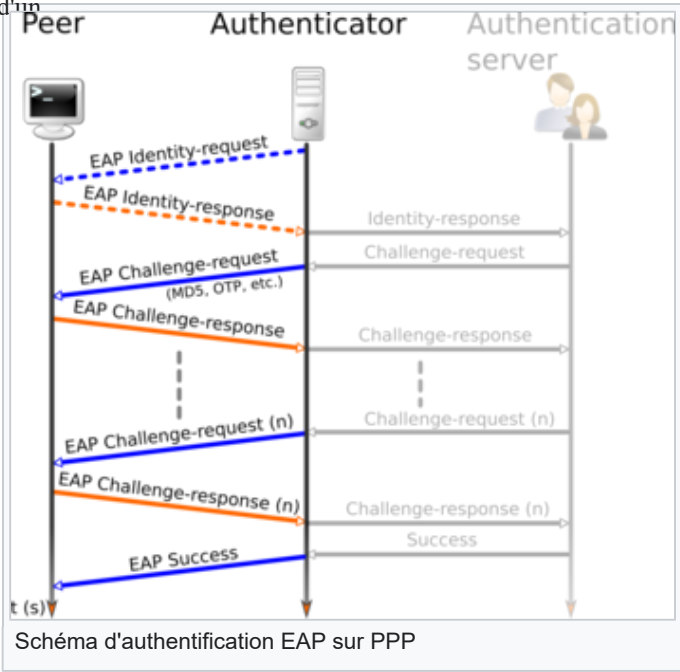
La liaison [PPP](#) est définie entre un *peer* <sup>note 1</sup> et un *authenticator* <sup>note 2, RFC 1</sup>.

L'*authenticator* peut envoyer une requête au *peer* pour connaître son identité ou alors de déterminer son identité par l'interface de communication ([Liaisons louées](#) , [Ligne dédiée](#) , etc.) <sup>RFC 1</sup>.

Cette identification est suivie d'une ou plusieurs requêtes envoyées par l'*authenticator* (obligatoire) avec un paramètre contenant la méthode d'authentification souhaitée <sup>RFC 1</sup> :

- [MD5-challenge](#)
- [One-Time Passwords](#)

Extensible Authentication Protocol 	
Informations	
<b>Fonction</b>	Authentification
<b>Sigle</b>	EAP
<b>Date de création</b>	1998
<b>RFC</b>	1998 <span> </span> : <a href="#">RFC 2284</a> <div>2004<span> </span>: <a href="#">RFC 3748</a><div>2008<span> </span>: <a href="#">RFC 5247</a></div></div>
<div><div>modifier</div><div><input type="checkbox"/></div></div>	



Generic Token Card

- SIM
- etc.

Le **peer** doit répondre à ce challenge et aura en fonction du résultat, un message envoyé par l'*authenticator* contenant un code<sup>RFC 4</sup> :

- Code 3 : Succès (Établissement de la couche réseau)
- Code 4 : Échec (Impossible d'établir la couche réseau)

Cette authentification peut être réalisée par l' *authenticator* lui-même ou déléguée à un **service tiers** (*authentication server*)<sup>RFC 5</sup>.

L'authentification peut être demandée par chaque extrémité <sup>[réf. nécessaire]</sup>

En **juin 2004**, la RFC 3748<sup>5</sup> vient étendre le fonctionnement du protocole EAP aux réseaux définis dans le standard **IEEE 802** rendant **obsolète** la RFC 2284<sup>4</sup><sup>RFC 6</sup> :

- Les **réseaux filaires** : Standard **IEEE 802.1X**
- Les **réseaux sans fil** : Standard **IEEE 802.11i**

Le protocole EAP sur ces réseaux est aussi connu sous le nom **EAPOL** <sup>note 3, RFC 7</sup>.

Bien que le protocole EAP possède un mécanisme de suppression de requêtes dupliquées et de retransmission de requêtes, il reste tributaire de la **couche de liaison de données**<sup>RFC 8</sup>. Par conséquent, des erreurs sur cette couche peuvent entraîner des erreurs d'authentification EAP<sup>RFC 9</sup>.

Le protocole EAP ne supporte pas nativement la **fragmentation des paquets réseau**<sup>RFC 10</sup> mais ce comportement peut être modifié avec certaines méthodes :

- **EAP-TLS** <sup>RFC 11</sup>

Quand le protocole EAP est utilisé en conjonction avec un point d'accès réseau compatible **802.1X** (sans-fil ou filaire), certaines méthodes EAP permettent de négocier une clé PMK (Pair-wise Master Key) entre le client et le point d'accès. Cette clé PMK peut ensuite être utilisée pour chiffrer les sessions **TKIP** ou **CCMP**.

Les standards **WPA** et **WPA2** ont adopté 5 types d'EAP comme mécanismes officiels d'identification<sup>[réf. nécessaire]</sup> :

- **EAP-TLS**
- **EAP-TTLS/MSCHAPv2**
- **PEAPv0/EAP-MS-CHAPv2**
- **PEAPv1/EAP-GTC**
- **EAP-SIM**

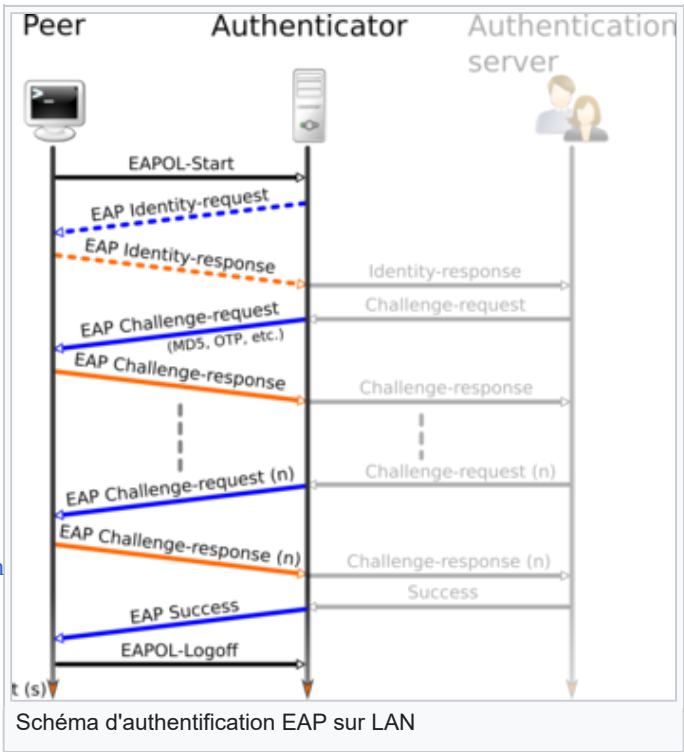
Mais EAP ne se limite pas à ces méthodes d'authentification. On présente ci-dessous des informations sur les EAP les plus connus.

Méthodes [ modifier | modifier le code ]

LEAP [ modifier | modifier le code ]

**Lightweight Extensible Authentication Protocol (LEAP)** est une implémentation propriétaire de EAP conçue par Cisco Systems.

Cisco a fait beaucoup d'efforts pour promouvoir ce protocole. Il a permis à d'autres fabricants de réaliser des produits « LEAP



Compatible » au travers du programme CCX (Cisco Certified Extensions). Ce protocole n'est pas présent nativement sous Windows. Il était connu pour être vulnérable aux attaques par dictionnaire comme EAP-MD5. Mais il ne l'est plus depuis la version ASLEAP (2003) de Joshua Wright. Cisco continue de soutenir que LEAP est une solution sécurisée si l'on utilise des mots de passe suffisamment complexes. Mais tout le monde sait bien que dans la réalité, les mots de passe complexes sont rarement utilisés<sup>[non neutre]</sup>. De nouveaux protocoles comme EAP-TTLS ou **PEAP** ne rencontrent pas ce type de fragilité car ils créent un tunnel TLS pour sécuriser l'identification. De plus ces nouveaux protocoles étant plus ouverts, ils peuvent être utilisés sur des points d'accès de marque Cisco ou non.

**EAP-TLS** [ [modifier](#) | [modifier le code](#) ]

EAP-TLS est un standard ouvert **IETF**. On le retrouve utilisé chez de nombreux fabricants de matériel sans fil. C’est le seul protocole EAP qui doit obligatoirement être implanté sur un matériel pour que ce dernier puisse porter le logo **WPA** ou **WPA2**. Il offre une bonne sécurité. En effet il utilise deux certificats pour la création d'un tunnel sécurisé qui permet ensuite l'identification : un côté serveur et un côté client. Cela signifie que même si le mot de passe est découvert, il ne sera d'aucune utilité sans le certificat client. Bien que EAP-TLS fournisse une excellente sécurité, l'obligation de disposer d'un certificat client est peut-être son talon d'Achille. En effet lorsque l'on dispose d'un grand parc de machines, il peut s'avérer difficile et coûteux de gérer un certificat par machine. C'est pour se passer du certificat client que les protocoles PEAP et EAP-TTLS ont été créés.

**TLS** est considéré comme le successeur du standard SSL. Il utilise une **Infrastructure à clés publiques** pour sécuriser les communications d'identification entre les clients et le serveur RADIUS.

Il existe des implémentations client ou serveur pour : Microsoft, Cisco, Apple, Linux... EAP-TLS est présent nativement dans MAC OS 10.3 et supérieur, Windows 2000 SP4, Windows XP, Windows Mobile 2003 et supérieur, et Windows CE 4.2.

**EAP-MD5** [ [modifier](#) | [modifier le code](#) ]

EAP-MD5 est un autre standard ouvert IETF, mais il offre un niveau de sécurité faible. La fonction de hachage MD5 utilisée est vulnérable aux attaques par dictionnaire, et elle ne supporte pas les clefs WEP dynamiques.

**EAP-TTLS** [ [modifier](#) | [modifier le code](#) ]

EAP-Tunneled Transport Layer Security, a été codéveloppé par Funk Software et Certicom ; c'est également un standard ouvert IETF. Il est supporté sur de nombreuses plates-formes, et offre un très bon niveau de sécurité. Il utilise des certificats X-509 uniquement sur le serveur d'identification. Le certificat est optionnel du côté client. Le défaut de **EAP-TTLS** par rapport à PEAP est de ne pas être présent nativement sur les systèmes Microsoft et Cisco. En revanche, il est légèrement plus sécurisé que PEAP car il ne diffuse pas le nom de l'utilisateur en clair.

**EAP-FAST** [ [modifier](#) | [modifier le code](#) ]

EAP-Flexible Authentication via Secure Tunneling est une proposition de Cisco Systems pour pallier les faiblesses de LEAP. L'utilisation de certificats serveur est optionnelle dans EAP-FAST. Il utilise Protected Access Credential (PAC). EAP-FAST dispose de trois phases.

- Phase 0 : Elle est optionnelle et permet de renseigner dynamiquement PAC. PAC peut être complété manuellement, auquel cas il n'y aura pas de phase 0.
- Phase 1 : Le client et le serveur **AAA**(Authentication Authorization Accounting) utilisent PAC pour établir un tunnel TLS.
- Phase 2 : Le client envoie les informations utilisateur à travers le tunnel.

EAP-FAST est défini dans un brouillon Internet IETF « draft-com-winget-eap-fast-03 ».

Actuellement il est proposé comme **RFC 4851**<sup>6</sup>.

**EAP-SIM** [ [modifier](#) | [modifier le code](#) ]

EAP-SIM est une méthode EAP pour les clients des réseaux **Wi-Fi** et des **réseaux de téléphonie mobile GSM**, **UMTS** et **LTE**. Il est utilisé pour l'identification et la distribution de clefs au travers des réseaux ; **SIM** signifie « Subscriber Identity Module ». EAP-SIM est décrit dans la RFC 4186<sup>7</sup>.

**Free Mobile** a été le premier opérateur français à mettre en service ce protocole d'authentification en avril 2012 pour ses clients détenteurs du **forfait illimité**<sup>8</sup>. Cela permet aux abonnés d'accéder au réseau **Free Wifi**. **SFR** a activé mi- juin 2012 , sur l'ensemble de son réseau, ce service déployé depuis mars 2012 , d'abord en phase d'expérimentation limitée<sup>9</sup>, sous le nom « Auto-connect ».

**EAP-AKA** [ [modifier](#) | [modifier le code](#) ]

EAP-AKA (Authentication and Key Agreement) est une méthode EAP pour les clients des réseaux de téléphonie mobile de 3<sup>e</sup> génération (UMTS et CDMA2000). Elle est décrite dans la RFC 4187<sup>10</sup>.

Contrairement à EAP-SIM, EAP-AKA permet de réaliser une authentification mutuelle de l'équipement utilisateur et du réseau. La longueur de la clé générée par accord mutuel est plus longue (128 bits) qu'avec EAP-SIM (64 bits)<sup>11</sup>.

Ce protocole est principalement employé dans les cadres suivants<sup>12</sup>:

- Authentification lors de l'attachement à un réseau de téléphonie mobile de 3<sup>e</sup> génération.
- Réutilisation des éléments d'authentification du réseau mobile lors de l'attachement à un réseau sans fil [Wifi] qui appartient à l'opérateur.

**EAP-AKA'** [ [modifier](#) | [modifier le code](#) ]

☐


Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue ! [Comment faire ?](#)

**Encapsulation** [ [modifier](#) | [modifier le code](#) ]

☐

Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue ! [Comment faire ?](#)

**PEAP** [ [modifier](#) | [modifier le code](#) ]



Pour un article plus général, voir [PEAP](#).

**Protected Extensible Authentication Protocol**, **Protected EAP**, ou plus simplement **PEAP**, est une méthode de transfert sécurisée d'informations d'identification, pour les réseaux filaires et sans fil. Ce protocole a été développé conjointement par Microsoft, RSA Security et Cisco Systems. C’est un standard ouvert de l'**IETF** (Internet Engineering Task Force). PEAP n'est pas une méthode de chiffrement, c'est une procédure pour identifier un client sur un réseau.

PEAP est très similaire à une autre méthode EAP : EAP-TTLS. Protected EAP a été créé pour contrer EAP-TTLS qui était jusque-là la seule méthode EAP à utiliser une **Infrastructure à clés publiques** (Public Key Infrastructure, PKI) **que** du côté serveur, pour la création d'un tunnel **TLS** protégeant l'identification. Dans ces deux standards, l'utilisation d'une clef publique côté client est optionnelle.


Il existe deux versions de PEAP certifiées [WPA](#) (mise à jour) et [WPA2](#) :

- PEAPv0/EAP- [MS-CHAPv2](#)
- PEAPv1/EAP-GTC

PEAP se déroule en deux phases :


1. La phase 1 permet l'identification du serveur grâce à une Infrastructure à clés publiques. Une fois le serveur identifié, il y a la création d'un tunnel sécurisé qui permettra à la phase 2 d'être chiffrée.
2. La phase 2 permet l'identification du client au travers du tunnel chiffré.

**Radius** [ [modifier](#) | [modifier le code](#) ]



Pour un article plus général, voir [Remote Authentication Dial-In User Service](#).

**Diameter** [ [modifier](#) | [modifier le code](#) ]



Pour un article plus général, voir [Diameter](#).

**Sécurité** [ [modifier](#) | [modifier le code](#) ]



Cette section est vide, insuffisamment détaillée ou incomplète. [Votre aide](#) est la bienvenue ! [Comment faire ?](#)

## Notes et références

### Notes

- ↑ que l'on pourrait traduire par : *Pair*.
- ↑ que l'on pourrait traduire par : *Authentificateur*.
- ↑ *Extensible Authentication Protocol Over LAN*

### Références

#### RFC

- ↑ <sup>a</sup> <sup>b</sup> <sup>c</sup> <sup>d</sup> <sup>e</sup> (en) RFC 2284 p. 2
- ↑ (en) RFC 3748 p. 2
- ↑ (en) RFC 3748 p. 5
- ↑ (en) RFC 2284 p. 6-7
- ↑ (en) RFC 2284 p. 2-3
- ↑ (en) RFC 3748 p. 3
- ↑ (en) RFC 3748 p. 54
- ↑ (en) RFC 3748 p. 15-16
- ↑ (en) RFC 3748 p. 16
- ↑ (en) RFC 3748 p. 16-17
- ↑ (en) RFC 5216 p. 14

#### Autres

- ↑ (en) L. Blunk et J. Vollbrecht, « PPP Extensible Authentication Protocol (EAP) » [archive], Request for comments n° 2284, mars 1998
- ↑ (en) B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., « Extensible Authentication Protocol (EAP) » [archive], Request for comments n° 3748, juin 2004
- ↑ (en) B. Aboba, D. Simon, P. Eronen, « Extensible Authentication Protocol (EAP) Key Management Framework » [archive], Request for comments n° 5247, août 2008
- ↑ <sup>a</sup> <sup>et</sup> <sup>b</sup> (en) Request for comments n° 2284 [archive]
- ↑ (en) Request for comments n° 3748 [archive]
- ↑ (en) Request for comments n° 4851 [archive]
- ↑ (en) Request for comments n° 4186 [archive]
- ↑ « Article d'annonce de l'activation de l'EAP-SIM chez Free » [archive] (consulté le 19 avril 2012)
- ↑ « EAP-SIM : SFR était là avant Free Mobile, et veut le faire savoir ! » [archive] (consulté le 19 avril 2012)
- ↑ (en) Request for comments n° 4187 [archive]
- ↑ « Authentication, Authorization, Accounting (AAA) » [archive du 6 septembre 2008] (consulté le 16 mai 2013), diapositives 29 à 32.

Consulté le 16 mai 2013.
- ↑ RFC 4187, §1: Introduction and Motivation. Consulté le 16 mai 2013.

## Bibliographie

### Articles

### Ouvrages

## Voir aussi

### Articles connexes

- IEEE 802.1X
- IEEE 802.11i

Authentication

- [Serveur d'authentification](#)
- [Protected Extensible Authentication Protocol](#)
- [Protocole AAA](#)
- [Remote Authentication Dial-In User Service](#)
- [FreeRADIUS](#)
- [Diameter](#)
- [Wi-Fi Protected Access](#)
- [wpa\\_supplicant](#)

Liens externes [ modifier | modifier le code ]

- (en) [RFC 2284](#) : (Obsolète) PPP Extensible Authentication Protocol (EAP)
- (en) [RFC 3748](#) : Extensible Authentication Protocol (EAP)
- (en) [RFC 3579](#) : RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
- (en) [RFC 4017](#) : EAP Method Requirements for Wireless LANs
- (en) « [protocol/EAP](#) » [archive], sur *freeradius.org* (consulté le 25 mars 2015)
- (en) « [Configure RADIUS for secure 802.1x wireless LAN](#) » [archive], sur *techrepublic.com*
- (en) « [How to self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication](#) » [archive], sur *techrepublic.com*
- (en) « [Extensible Authentication Protocol](#) » [archive], sur *technet.microsoft.com*
- (en) « [WIRE1x](#) » [archive], sur *wire.cs.nctu.edu.tw*
- (en) « [IETF EAP Method Update \(emu\) Working Group](#) » [archive], sur *ietf.org*

 [Portail de la cryptologie](#)

 [Portail de la sécurité informatique](#)

 [Portail des télécommunications](#)

Catégories : [Protocole réseau](#) | [Sécurité du réseau sans fil](#) | [Protocole d'authentification](#) | [Protocole cryptographique](#)  [+]

La dernière modification de cette page a été faite le 5 décembre 2019 à 12:22.

**Droit d'auteur** : les textes sont disponibles sous [licence Creative Commons attribution, partage dans les mêmes conditions](#) ; d'autres conditions peuvent s'appliquer. Voyez les [conditions d'utilisation](#) pour plus de détails, ainsi que les [crédits graphiques](#). En cas de réutilisation des textes de cette page, voyez [comment citer les auteurs et mentionner la licence](#).  
Wikipedia® est une marque déposée de la [Wikimedia Foundation, Inc.](#), organisation de bienfaisance régie par le paragraphe [501\(c\)\(3\)](#) du code fiscal des États-Unis.

[Politique de confidentialité](#)  [À propos de Wikipédia](#)  [Avertissements](#)  [Contact](#)  [Code de conduite](#)  [Version mobile](#)  [Développeurs](#)

[Statistiques](#)  [Déclaration sur les témoins \(cookies\)](#)

