Groupe de travail Réseau
Request for Comments : 3748
RFC rendue obsolète : 2284

Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
L. Blunk, Merit Network
J. Carlson, Sun
H. Levkovetz, ipUnplugged
J. Vollbrecht, Vollbrecht Consulting LLC
juin 2004

Protocole d'authentification extensible (EAP)

Résumé
Le présent document définit le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*), un cadre d'authentification qui prend en charge plusieurs méthodes d'authentification. EAP fonctionne normalement directement sur les couches de liaison des données comme le protocole de point à point (PPP, *Point-to-Point Protocol*) ou IEEE 802, sans exiger IP. EAP fournit sa propre prise en charge de l'élimination des dupliqués et de la retransmission, mais il s'appuie sur des garanties d'ordre de couche inférieure. La fragmentation n'est pas prise ne charge par EAP lui-même ; cependant des méthodes d'EAP individuelles peuvent le faire.

Le présent document rend obsolète la RFC 2284. Un résumé des changements apportés par le présent document à la RFC 2284 figure en Appendice A.

Table des Matières

1. Introduction

Le présent document définit le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*), un cadre d'authentification qui prend en charge plusieurs méthodes d'authentification. EAP fonctionne normalement directement sur des couches de liaison des données telles que le protocole de point à point (PPP, *Point-to-Point Protocol*) ou IEEE 802, sans avoir besoin d'IP. EAP fournit son propre support pour l'élimination des dupliqués et la retransmission, mais il s'appuie sur les garanties d'ordre des couches inférieures. La fragmentation n'est pas prise en charge au sein d'EAP lui-même, cependant, les méthodes EAP individuelles peuvent le faire.

EAP peut être utilisé sur des liaison dédiés, aussi bien que sur des circuits commutés, et sur des liaisons filaires aussi bien que sans fil. Aujourd'hui, EAP a été mis en œuvre avec des hôtes et des routeurs qui se connectent via des circuits commutés ou des lignes numérotées en utilisant PPP [RFC1661]. Il a aussi été mis en œuvre avec des commutateurs et des points d'accès utilisant [IEEE-802]. L'encapsulation d'EAP sur des supports filaires IEEE 802 est décrite dans [IEEE-802.1X], et l'encapsulation sur des LAN sans fil IEEE dans [IEEE-802.11i].

Un des avantages de l'architecture EAP est sa souplesse. EAP est utilisé pour choisir un mécanisme d'authentification spécifique, normalement après que l'authentificateur a demandé plus d'informations pour déterminer la méthode d'authentification spécifique à utiliser. Plutôt que d'exiger que l'authentificateur soit mis à jour pour prendre an charge chaque nouvelle méthode d'authentification, EAP permet l'utilisation d'un serveur d'authentification d'extrémité arrière, qui peut mettre en œuvre certaines méthodes d'authentification, ou toutes, l'authentificateur agissant comme un passeur pour certaines ou toutes les méthodes et les homologues.

Dans le présent document, les exigences de l'authentificateur s'appliquent sans considérer si l'authentificateur fonctionne comme passeur ou non. Lorsque l'exigence est destinée à s'appliquer à l'authentificateur ou au serveur d'authentification d'extrémité arrière, selon l'endroit où se termine l'authentification EAP, le terme "serveur EAP" sera utilisé.

1.1 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1.2 Terminologie

Le présent document utilise fréquemment les termes suivants :

Authentificateur : c'est l'extrémité de la liaison qui initie l'authentification EAP. Le terme authentificateur est utilisé dans [IEEE-802.1X], et a la même signification dans le présent document.

Homologue : extrémité de la liaison qui répond à l'authentificateur. Dans [IEEE-802.1X], cette extrémité est connue sous le nom de solliciteur *(Supplicant)*.

Solliciteur : extrémité de la liaison qui répond à l'authentificateur dans [IEEE-802.1X]. Dans le présent document, cette extrémité de la liaison est appelée l'homologue.

Serveur d'authentification d'extrémité arrière : c'est une entité qui fournit un service d'authentification à un authentificateur. Lorsque utilisé, ce serveur exécute normalement les méthodes EAP pour l'authentificateur. Cette terminologie est aussi utilisée dans [IEEE-802.1X].

AAA : Authentification, Autorisation, et comptabilité. Les protocoles AAA avec soutien EAP incluent RADIUS [RFC3579] et Diameter [RFC4072]. Dans le présent document, les termes "serveur AAA" et "serveur d'authentification d'extrémité arrière" sont utilisés de façon interchangeable.

Message affichable : c'est interprété comme étant une chaîne de caractères lisible par l'homme. Le codage du message DOIT suivre le format de transformation UTF-8 [RFC2279].

Serveur EAP : entité qui termine la méthode d'authentification EAP avec l'homologue. Dans le cas où aucun serveur d'authentification d'extrémité arrière n'est utilisé, le serveur EAP fait partie de l'authentificateur. Dans le cas où l'authentificateur opère en mode passeur, le serveur EAP est situé chez le serveur d'authentification d'extrémité arrière.

Éliminer en silence : cela signifie que la mise en œuvre élimine le paquet sans autre traitement. La mise en œuvre DEVRAIT avoir la capacité d'inscrire l'événement dans un journal, incluant le contenu du paquet éliminé en silence, et DEVRAIT enregistrer l'événement dans un compteur de statistiques.

Authentification réussie : dans le contexte du présent document, "authentification réussie" est un échange de messages EAP, par suite duquel l'authentificateur décide de permettre l'accès à l'homologue, et l'homologue décide d'utiliser cet accès. La décision de l'authentificateur implique normalement les deux aspects d'authentification et d'autorisation ; l'homologue peut réussi à s'authentifier auprès de l'authentificateur, mais l'accès peut être refusé par l'authentificateur pour des raisons de politique.

Vérification d'intégrité de message (MIC, *Message Integrity Check*) : fonction de hachage chiffré utilisée pour l'authentification et la protection d'intégrité des données. C'est souvent appelé un code d'authentification de message (MAC), mais les spécifications IEEE 802 (et le présent document) utilisent l'acronyme MIC pour éviter la confusion avec le contrôle d'accès au support *(Medium Access Control)*.

Séparation cryptographique :deux clés (x et y) sont "cryptographiquement séparées" si un adversaire qui connaît tous les messages échangés dans le protocole ne peut pas calculer x à partir de y ou y à partir de x sans "casser" certaines hypothèses cryptographiques. En particulier, cette définition permet que l'adversaire ait la connaissance de tous les noms occasionnels envoyés en clair, ainsi que toutes les contre valeurs prévisibles utilisées dans le protocole. Casser une hypothèse cryptographique exigerait normalement d'inverser une fonction unidirectionnelle ou de prédire le résultat d'un générateur de nombres cryptographiques pseudo aléatoires sans connaissance de l'état secret. En d'autres termes, si les clé sont cryptographiquement séparées, il n'y a pas de raccourci pour calculer x à partir de y ou y à partir de x, mais le travail qu'un adversaire doit effectuer pour réaliser ce calcul est équivalent à effectuer une recherche exhaustive de la valeur de l'état secret.

Clé de session maîtresse (MSK, *Master Session Key*) : matériel de chiffrement qui est déduit entre l'homologue et le serveur EAP et exporté par la méthode EAP. La MSK est d'au moins 64 octets. Dans les mises en œuvre existantes, un serveur AAA agissant comme serveur EAP transporte la MSK à l'authentificateur.

Clé de session maîtresse étendue (EMSK, *Extended Master Session Key*) : matériel de chiffrement supplémentaire déduit entre client et serveur EAP qui est exporté par la méthode EAP. La EMSK fait au moins 64 octets. La EMSK n'est pas partagée avec l'authentificateur ni aucun autre tiers. La EMSK est réservée pour de futures utilisations qui ne sont pas encore définies.

Indications de résultat : une méthode fournit des indications de résultats si après l'envoi et la réception du dernier message de la méthode :

1) l'homologue sait si il a authentifié le serveur, ainsi que si le serveur l'a authentifié,
2) le serveur sait si il a authentifié l'homologue, ainsi que si l'homologue l'a authentifié.

Dans le cas où la réussite de l'authentification est suffisante pour autoriser l'accès, l'homologue et l'authentificateur vont alors aussi savoir si l'autre partie veut fournir ou accepter l'accès. Cela peut n'être pas toujours le cas. Un homologue authentifié peut être refusé d'accès par manque d'autorisation (par exemple, limite de session) ou pour d'autres raisons. Comme l'échange EAP fonctionne entre l'homologue et le serveur, d'autres nœuds (comme des mandataires AAA) peuvent aussi affecter la décision d'autorisation. Ceci est discuté plus en détails au paragraphe 7.16.

1.3 Applicabilité

EAP a été conçu pour être utilisé dans l'authentification d'accès réseau, où la connexité de la couche IP peut n'être pas disponible. L'utilisation de EAP pour d'autres objets, comme le transport de données en vrac, N'EST PAS RECOMMANDÉE.

Comme EAP n'exige pas la connexité IP, il fournit juste assez de soutien pour le transport fiable des protocoles d'authentification, et rien de plus.

EAP est un protocole en mode rigide qui ne prend en charge qu'un seul paquet à la fois. Par suite, EAP ne peut pas transporter efficacement des données en vrac, à la différence des protocoles de transport comme TCP [RFC0793] ou SCTP [RFC2960].

Bien que EAP fournisse la prise en charge de la retransmission, il suppose des garanties d'ordre fournies par la couche inférieure, de sorte que la réception déclassée n'est pas acceptée.

Comme EAP ne prend pas en charge la fragmentation et le réassemblage, les méthodes d'authentification EAP qui génèrent des charges utiles plus grandes que la MTU EAP minimum doivent assurer la prise en charge de la fragmentation.

Bien que les méthodes d'authentification telles que EAP-TLS [RFC2716] fournissent la prise en charge de la fragmentation et du réassemblage, les méthodes EAP définies dans le présent document ne le font pas. Par suite, si la taille du paquet EAP excède la MTU EAP de la liaison, ces méthodes rencontreront des difficultés.

L'authentification EAP est initiée par le serveur (authentificateur) alors que de nombreux protocoles d'authentification sont initiés par le client (homologue). Par suite, il peut être nécessaire qu'un algorithme d'authentification ajoute un ou deux messages supplémentaires (au plus un aller retour) afin de fonctionner sur EAP.

Lorsque l'authentification fondée sur le certificat est prise en charge, le nombre d'allers retours supplémentaires peut être beaucoup plus grand à cause de la fragmentation des chaînes de certificats. En général, un paquet EAP fragmenté va exiger autant d'allers retours qu'il y a de fragments à envoyer. Par exemple, une chaîne de certificats de 14 960 octets va exiger dix allers retours à l'envoi avec une MTU EAP de 1496 octets.

Lorsque EAP fonctionne sur une couche inférieure dans laquelle se rencontre une perte de paquets significative, ou lorsque la connexion entre l'authentificateur et le serveur d'authentification subit des pertes significatives de paquets, les méthodes EAP qui exigent de nombreux allers retours peuvent subir des difficultés. Dans ces situations, l'utilisation de méthodes EAP avec moins d'allers retours est conseillée.

2. Protocole d'authentification extensible (EAP)

L'échange d'authentification EAP se déroule comme suit :

(1) L'authentificateur envoie une demande pour authentifier l'homologue. La demande a un champ Type pour indiquer ce qui est demandé. Des exemples de types de demandes incluent Identité, Défi MD5, etc. Le type Défi MD5correspond étroitement au protocole d'authentification CHAP [RFC1994]. Normalement, l'authentificateur envoie une demande initiale Identité ; cependant, une demande initiale Identité n'est pas obligée, et PEUT être sautée. Par exemple, l'identité peut n'être pas exigée lorsque elle est déterminée par l'accès auquel l'homologue s'est connecté (liaisons louées, commutateur dédié ou accès commutés) ou lorsque l'identité est obtenue d'une autre façon (via l'appel de l'identité de la station ou son adresse MAC, dans le champ Nom de la réponse au défi MD5, etc.).

(2) L'homologue envoie un paquet Réponse en réponse à une Demande valide. Comme avec le paquet de demande, le paquet de réponse contient un champ Type, qui correspond au champ Type de la demande.

(3) L'authentificateur envoie un paquet de demande supplémentaire, et l'homologue réplique par une réponse. La séquence de demandes et réponses continue autant que nécessaire. EAP est un protocole "en mode rigide", de sorte qu'à part la demande initiale, une nouvelle demande ne peut pas être envoyée avant de recevoir une réponse valide. L'authentificateur est chargé de retransmettre les demandes comme décrit au paragraphe 4.1. Après un nombre convenable de retransmissions, l'authentificateur DEVRAIT terminer la conversation EAP. L'authentificateur NE DOIT PAS envoyer de paquet Succès ou Échec lors de la retransmission ou lorsque il échoue à obtenir une réponse de l'homologue.

(4) La conversation continue jusqu'à ce que l'authentificateur ne puisse pas authentifier l'homologue (des réponses inacceptables à une ou plusieurs demandes) auquel cas la mise en œuvre d'authentificateur DOIT transmettre un Échec EAP (code 4). Autrement, la conversation d'authentification peut continuer jusqu'à ce que l'authentificateur détermine qu'une authentification réussie s'est produite, auquel cas l'authentificateur DOIT transmettre un Succès EAP (code 3).

Avantages :
- o Le protocole EAP peut prendre en charge plusieurs mécanismes d'authentification sans avoir à en pré négocier un particulier.
- o Les appareils de serveur d'accès réseau (NAS, *Network Access Server*) (par exemple, un commutateur ou point d'accès) n'ont pas à comprendre chaque méthode d'authentification et PEUVENT agir comme agent passeur pour un serveur d'authentification d'extrémité arrière. La prise en charge du passeur est facultative. Un authentificateur PEUT authentifier les homologues locaux, tout en agissant en même temps comme passeur pour des homologues non locaux et les méthodes d'authentification qu'il ne met pas en œuvre localement.
- o La séparation de l'authentificateur du serveur d'authentification d'extrémité arrière simplifie la gestion des accréditifs et la prise de décisions de politique.

Inconvénients :
- o Utilisé dans PPP, EAP exige l'ajout d'un nouveau type d'authentification à PPP LCP et donc les mises en œuvre de PPP devront être modifiées pour l'utiliser. Il s'écarte aussi du précédent modèle d'authentification PPP de négociation d'un mécanisme d'authentification spécifique durant LCP. De même, les mises en œuvre de commutateurs ou de point d'accès devront prendre en charge [IEEE-802.1X] afin d'utiliser EAP.
- o Lorsque l'authentificateur est séparé du serveur d'authentification d'extrémité arrière, cela complique l'analyse de la sécurité et, si nécessaire, la distribution de clés.

2.1 Prise en charge de séquences

Une conversation EAP PEUT utiliser une séquence de méthodes. Un exemple courant en est une demande Identité suivie par une seule méthode d'authentification EAP comme un Défi MD5. Cependant, l'homologue et l'authentificateur DOIVENT utiliser une seule méthode d'authentification (Type 4 ou supérieur) au sein d'une conversation EAP, après quoi l'authentificateur DOIT envoyer un paquet Succès ou Échec.

Une fois qu'un homologue a envoyé une Réponse du même type que la demande initiale, un authentificateur NE DOIT PAS envoyer une Demande d'un type différent avant l'achèvement du tour final d'une méthode donnée (à l'exception d'une demande de notification) et NE DOIT PAS envoyer une demande pour une méthode supplémentaire de tout type après l'achèvement de la méthode d'authentification initiale ; un homologue qui reçoit une telle demande DOIT la traiter comme invalide, et l'éliminer en silence. Par suite, Identity Requery n'est pas pris en charge.

Un homologue NE DOIT PAS envoyer un accusé de réception négatif (Nak, *negative achnowledgement*) (traditionnel ou étendu) en réponse à une demande après l'envoi d'une réponse initiale non Nak. Comme des paquets de demande EAP fallacieux peuvent être envoyés par un attaquant, un authentificateur qui reçoit un Nak inattendu DEVRAIT l'éliminer et enregistrer l'événement.

Plusieurs méthodes d'authentification au sein d'une conversation EAP ne sont pas acceptées à cause de leur vulnérabilité aux attaques par interposition (voir au paragraphe 7.4) et de l'incompatibilité avec les mises en œuvre existantes.

Lorsque une seule méthode d'authentification EAP est utilisée, mais que d'autres méthodes fonctionnent en son sein (une méthode "tunnelée") la prohibition des méthodes d'authentification multiples ne s'applique pas. De telles méthodes "tunnelées" apparaissent comme une seule méthode d'authentification pour EAP. La rétro compatibilité peut être assurée, car un homologue qui ne supporte pas une méthode "tunnelée" peut répondre à la demande initiale EAP par un Nak (traditionnel ou étendu). Pour répondre aux faiblesses de la sécurité, les méthodes "tunnelées" DOIVENT prendre en charge la protection contre les attaques par interposition.

2.2 Modèle EAP de multiplexage

Conceptuellement, les mises en œuvre EAP comportent les composants suivants :

[a] Couche inférieure. Elle est chargée de la transmission et de la réception des trames EAP entre l'homologue et l'authentificateur. EAP a fonctionné sur diverses couches inférieures qui incluent PPP, les LAN filaires IEEE 802 [IEEE-802.1X], les LAN sans fil IEEE 802.11 [IEEE-802.11], UDP (L2TP [RFC2661] et IKEv2 [RFC4306]]), et TCP [PIC]. Le comportement de couche inférieure est exposé à la Section 3.

[b] Couche EAP. Elle reçoit et transmet les paquets EAP via la couche inférieure, met en œuvre la détection des dupliqués et la retransmission, et livre et reçoit les messages EAP de et vers les couches d'homologue EAP et d'authentificateur.

[c] Couches EAP d'homologue et d'authentificateur. Sur la base du champ Code, la couche EAP démultiplexe les paquets EAP entrants aux couches EAP d'homologue et d'authentificateur. Normalement, une mise en œuvre EAP sur un certain hôte va prendre en charge la fonction d'homologue ou d'authentificateur, mais il est possible à un hôte d'agir à la fois comme homologue et authentificateur EAP. Dans une telle mise en œuvre les deux couches EAP homologue et authentificateur seront présentes.

[d] Couches de méthode EAP. Les méthodes EAP mettent en œuvre les algorithmes d'authentification et reçoivent et transmettent les messages EAP via les couches EAP d'homologue et d'authentificateur. Comme la prise en charge de la fragmentation n'est pas fournie par EAP lui-même, c'est de la responsabilité des méthodes EAP, qui est exposée à la Section 5.

Le modèle de multiplexage EAP est illustré ci-dessous à la Figure 1. Noter qu'il n'est pas exigé qu'une mise en œuvre se conforme à ce modèle, pour autant que le comportement sur le réseau soit cohérent avec lui.

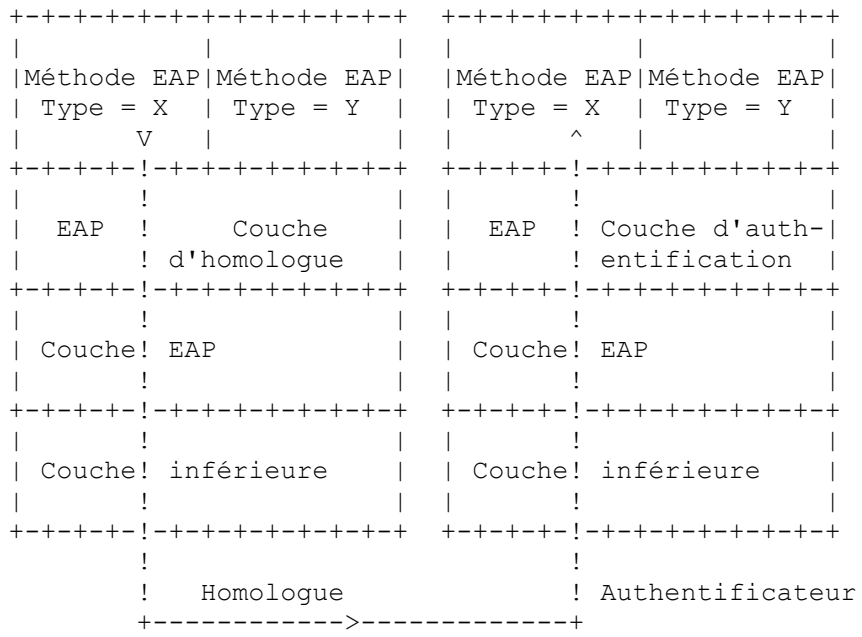


Figure 1 : Modèle EAP de multiplexage

Au sein d'EAP, le champ Code fonctionne un peu comme un numéro de protocole dans IP. On suppose que la couche EAP démultiplexe les paquets EAP entrants conformément au champ Code. Les paquets EAP reçus avec le code 1 (demande), 3 (Succès), et 4 (Échec) sont livrés par la couche EAP à la couche EAP homologue, si elle est mise en œuvre. Les paquets EAP avec le code 2 (Réponse) sont livrés à la couche authentificateur EAP, si elle est mise en œuvre.

Au sein d'EAP, le champ Type fonctionne un peu comme un numéro d'accès dans UDP ou TCP. On suppose que les couches EAP homologue et authentificateur démultiplexent les paquets EAP entrants conformément à leur Type, et les livrent seulement à la méthode EAP correspondant à ce type. Une mise en œuvre de méthode EAP sur un hôte peut s'enregistrer pour recevoir des paquets des couches homologue ou authentificateur, ou les deux, selon le ou les rôles qu'elle prend en charge.

Comme les méthodes d'authentification EAP peuvent souhaiter accéder à l'identité, les mises en œuvre DEVRAIENT rendre les demandes et réponses Identité accessibles aux méthodes d'authentification (Types 4 ou supérieur) en plus de la méthode Identité. Le type Identité est exposé au paragraphe 5.1. Une réponse Notification n'est utilisée que comme confirmation que l'homologue a reçu la demande Notification, et non qu'il l'a traitée, ou a affiché le message à l'utilisateur. On ne peut pas supposer que le contenu de la demande ou réponse Notification est disponible pour une autre méthode. Le type Notification est exposé au paragraphe 5.2.

Nak (Type 3) ou Nak étendu (Type 254) est utilisé pour les besoins de la négociation de méthode. Les homologues répondent à une demande initiale EAP pour un type inacceptable avec une réponse Nak (Type 3) ou Nak étendu (Type 254). On ne peut pas supposer que le contenu de la ou des réponses Nak soit disponible pour une autre méthode. Les types Nak sont exposés au paragraphe 5.3.

Les paquets EAP avec les codes de Succès ou Échec ne comportent pas de champ Type, et ne sont pas livrés à une méthode EAP. Succès et Échec sont exposés au paragraphe 4.2.

Avec ces considérations, les messages de demande/réponse de succès, échec, Nak , et Notification NE DOIVENT PAS être utilisés pour porter des données destinées à être livrées aux autres méthodes EAP.

2.3 Comportement de passeur

Lorsque il fonctionne comme "passeur authentificateur", un authentificateur effectue des vérifications sur les champs Code, Identifiant, et Longueur comme décrit au paragraphe 4.1. Il transmet les paquets EAP reçus de l'homologue et destinés à sa couche authentificateur au serveur d'authentification d'extrémité arrière ; les paquets reçus du serveur d'authentification d'extrémité arrière destinés à l'homologue lui sont transmis.

Un hôte qui reçoit un paquet EAP peut seulement faire une des trois choses suivante avec lui : agir sur lui, l'abandonner, ou le transmettre. La décision de transmission est normalement fondée sur le seul examen des champs Code, Identifiant, et Longueur. Une mise en œuvre de passeur authentificateur DOIT être capable de transmettre les paquets EAP reçus de l'homologue avec le code 2 (Réponse) au serveur d'authentification d'extrémité arrière. Il DOIT aussi être capable de recevoir des paquets EAP du serveur d'authentification d'extrémité arrière et de transmettre les paquets EAP de code 1 (Demande), code 3 (Succès), et code 4 (Échec) à l'homologue.

Sauf si l'authentificateur met en œuvre une ou plusieurs méthodes d'authentification en local qui prennent en charge le rôle d'authentificateur, les champs d'en-tête de couche de méthode EAP (Type, Type-Données) ne sont pas examinés au titre de la décision de transmission. Lorsque l'authentificateur prend en charge des méthodes d'authentification locales, il PEUT examiner le champ Type pour déterminer si il faut agir sur le paquet lui-même ou le transmettre. Les mises en œuvre conformes d'authentificateur passeur DOIVENT par défaut transmettre les paquets EAP de tout type.

Les paquets EAP reçus avec le code 1 (Demande), code 3 (Succès), et code 4 (Échec) sont démultiplexés par la couche EAP et livrés à la couche homologue. Donc, sauf si un hôte met en œuvre une couche EAP d'homologue, ces paquets seront éliminés en silence. De même, les paquets EAP reçus avec le code 2 (Réponse) sont démultiplexés par la couche EAP et livrés à la couche d'authentificateur. Donc, sauf si un hôte met en œuvre une couche d'authentificateur EAP, ces paquets seront éliminés en silence. Le comportement de "passeur homologue" est indéfini dans la présente spécification, et n'est pas pris en charge par les protocoles AAA tels que RADIUS [RFC3579] et Diameter [RFC4072].

Le modèle de transmission est illustré par la Figure 2.

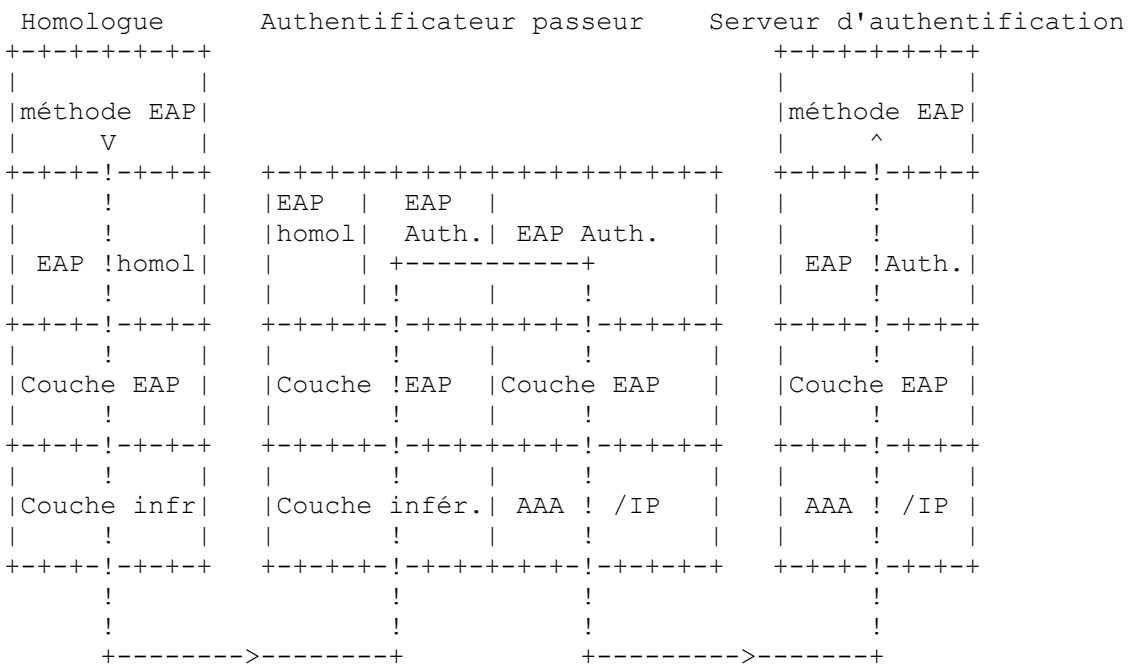


Figure 2 : Authentificateur passeur

Pour les sessions dans lesquelles l'authentificateur agit comme passeur, il DOIT déterminer le résultat de l'authentification

sur la seule base de l'indication Accepte/Rejette envoyée par le serveur d'authentification d'extrémité arrière ; le résultat NE DOIT PAS être déterminé par le contenu d'un paquet EAP envoyé avec l'indication Accepte/Rejette, ou l'absence d'un tel paquet EAP encapsulé.

2.4 Fonctionnement d'homologue à homologue

Comme EAP est un protocole d'homologue à homologue, une authentification indépendante et simultanée peut avoir lieu dans la direction inverse (selon les capacités de la couche inférieure). Les deux extrémités de la liaison peuvent agir comme authentificateurs et homologues en même temps. Dans ce cas, il est nécessaire que les deux extrémités mettent en œuvre les couches EAP authentificateur et homologue. De plus, les mises en œuvre de méthode EAP sur les deux homologues doivent prendre en charge les deux fonctionnalités d'authentificateur et d'homologue.

Bien que EAP prenne en charge le fonctionnement d'homologue à homologue, certaines mises en œuvre EAP, méthodes, protocoles AAA, et couches de liaison des données peuvent ne pas le faire. Certaines méthodes EAP peuvent prendre en charge l'authentification symétrique, avec un type d'accréditif requis pour l'homologue et un autre type pour l'authentificateur. Les hôtes qui prennent en charge le fonctionnement d'homologue à homologue avec une telle méthode devront être provisionnés avec les deux types d'accréditifs.

Par exemple, EAP-TLS [RFC2716] est un protocole client-serveur dans lequel des profils de certificat différents sont normalement utilisés pour le client et le serveur. Cela implique qu'un hôte qui prend en charge l'authentification d'homologue à homologue avec EAP-TLS devra mettre en œuvre les deux couches d'homologue et d'authentificateur EAP, prendre en charge les deux rôles d'homologue et d'authentificateur dans la mise en œuvre EAP-TLS, et fournir les certificats appropriés pour chaque rôle.

Les protocoles AAA comme RADIUS/EAP [RFC3579] et Diameter EAP [RFC4072] ne prennent en charge que le fonctionnement de "passeur authentificateur". Comme noté au paragraphe 2.6.2 de la [RFC3579], un serveur RADIUS répond à une demande d'accès qui encapsule un paquet Demande EAP, Succès, ou Échec par un Refus d'accès. Il n'y a donc pas de prise en charge du fonctionnement de "passeur homologue".

Même lorsque une méthode est utilisée qui prend en charge l'authentification mutuelle et l'indication de résultat, plusieurs considérations peuvent dicter que deux authentifications EAP (une dans chaque direction) sont requises. Cela inclut :

(1) La prise en charge de la déduction de clé de session bidirectionnelle dans la couche inférieure. Les couches inférieures comme IEEE 802.11 peuvent seulement prendre en charge la déduction unidirectionnelle et le transport de clés de session transitoires. Par exemple, la prise de contact de clé de groupe définie dans [IEEE-802.11i] est unidirectionnelle, car dans le mode d'infrastructure IEEE 802.11, seul le point d'accès (AP) envoie du trafic en diffusion/diffusion groupée. Dans le mode ad hoc IEEE 802.11, où l'un ou l'autre homologue peut envoyer du trafic en diffusion/diffusion groupée, deux échanges de clé de groupe unidirectionnelle sont requis. Du fait des limitations de la conception cela implique aussi que le besoin de déduction de clé en envoi individuel et d'échanges de méthode EAP se produise dans chaque direction.

(2) La prise en charge d'un départage à la couche inférieure. Les couches inférieures comme IEEE 802.11 ad hoc ne prennent pas en charge le "départage" dans lequel deux hôtes initiant l'authentification mutuelle vont seulement poursuivre une seule authentification. Cela implique que même si 802.11 prenait en charge une prise de contact bidirectionnelle de clé de groupe, il y aurait quand même deux authentifications, une dans chaque direction.

(3) Satisfaction de la politique de l'homologue. Les méthodes EAP peuvent prendre en charge les indications de résultat, permettant à l'homologue d'indiquer au serveur EAP au sein de la méthode qu'il a authentifié avec succès le serveur EAP, ainsi qu'au serveur d'indiquer qu'il a authentifié l'homologue. Cependant, un passeur authentificateur ne saura pas si l'homologue a accepté les accréditifs offerts par le serveur EAP, sauf si cette information est fournie à l'authentificateur via le protocole AAA. L'authentificateur DEVRAIT interpréter la réception d'un attribut de clé au sein d'un paquet Accept comme l'indication que l'homologue a authentifié avec succès le serveur.

Cependant, il est possible que la politique d'accès de l'homologue EAP ne soit pas satisfaite durant l'échange initial EAP, même lorsque l'authentification mutuelle s'est produite. Par exemple, l'authentificateur EAP peut n'avoir pas démontré l'autorisation d'agir dans les deux rôles d'homologue et d'authentificateur. Par suite, l'homologue peut exiger une authentification supplémentaire dans la direction inverse, même si l'homologue a fourni l'indication que le serveur EAP s'était authentifié avec succès auprès de lui.

3. Comportement de couche inférieure

3.1 Exigences de couche inférieure

EAP fait les hypothèses suivantes sur les couches inférieures :

(1) Transport non fiable. Dans EAP, l'authentificateur retransmet les demandes qui n'ont pas encore reçu de réponse de sorte que EAP ne suppose pas que les couches inférieures sont fiables. Comme EAP définit son propre comportement de retransmission, il est possible (bien qu'indésirable) que la retransmission se produise à la fois à la couche inférieure et à la couche EAP lorsque EAP fonctionne sur une couche inférieure fiable. Noter que les paquets EAP Succès et Échec ne sont pas retransmis. Sans une couche inférieure fiable, et avec un taux d'erreurs non négligeable, ces paquets peuvent être perdus, résultant en fins de temporisations. Il est donc souhaitable que les mises en œuvre améliorent leur résilience à la perte de paquets EAP Succès ou Échec, comme décrit au paragraphe 4.2.

(2) Détection d'erreur de couche inférieure. Bien que EAP ne suppose pas que la couche inférieure est fiable, il ne s'appuie pas sur la détection d'erreur de la couche inférieure (par exemple, CRC, somme de contrôle, MIC, etc.). Les méthodes EAP peuvent ne pas inclure de MIC, ou si elles le font, il peut n'être pas calculé sur tous les champs du paquet EAP, comme les champs Code, Identifiant, Longueur, ou Type. Par suite, sans la détection d'erreur de la couche inférieure, des erreurs non détectées pourraient s'introduire dans les champs d'en-tête de la couche EAP ou de la couche méthode EAP, débouchant sur des échecs d'authentification. Par exemple, EAP TLS [RFC2716], qui calcule son MIC sur le seul champ Données de type, considère les échecs de validation de MIC comme des erreurs fatales. Sans la détection d'erreur de la couche inférieure, cette méthode, et d'autres comme elle, ne vont pas fonctionner de façon fiable.

(3) Sécurité de couche inférieure. EAP n'exige pas que les couches inférieures fournissent des services de sécurité comme la confidentialité, l'authentification, la protection de l'intégrité, et la protection contre la répétition par paquet. Cependant, lorsque ces services de sécurité sont disponibles, les méthodes EAP qui prennent en charge la déduction de clé (voir au paragraphe 7.2.1) peuvent être utilisées pour fournir de façon dynamique le matériel de chiffrement. Cela rend possible de lier l'authentification EAP aux données suivantes et de protéger contre la modification des données, l'usurpation d'identité, ou la répétition. Voir les détails au paragraphe 7.1.

(4) MTU minimum. EAP est capable de fonctionner sur les couches inférieures qui fournissent une taille de MTU EAP de 1020 octets ou plus. EAP ne prend pas en charge la découverte de la MTU de chemin, et la fragmentation et le réassemblage ne sont pas pris en charge par EAP, ni par les méthodes définies dans la présente spécification : des types Identité (1), Notification (2), Nak de réponse (3), Défi MD5 (4), Mot de passe à utilisation unique (OTP, *One Time Password*) (5), Carte de jeton générique (6), et Nak de réponse étendu (254). Normalement, l'homologue EAP obtient les informations sur la MTU EAP des couches inférieures et règle la taille de trame EAP à une valeur appropriée. Lorsque l'authentificateur fonctionne en mode passeur, le serveur d'authentification n'a pas de moyen direct de déterminer la MTU EAP, et s'appuie donc sur l'authentificateur pour qu'elle lui fournisse cette information, comme via l'attribut Framed-MTU, décrit au paragraphe 2.4 de la [RFC3579]. Bien que les méthodes comme EAP-TLS [RFC2716] prennent en charge la fragmentation et le réassemblage, les méthodes EAP conçues à l'origine pour être utilisées avec PPP où une MTU de 1500 octets est garantie pour les trames de contrôle (voir le paragraphe 6.1 de la [RFC1661]) peuvent ne pas avoir les caractéristiques de fragmentation et réassemblage. Les méthode EAP peuvent supposer une MTU EAP minimum de 1020 octets en l'absence d'autres informations. Les méthodes EAP DEVRAIENT inclure la prise en charge de la fragmentation et du réassemblage si leurs charges utiles peuvent être plus grandes que cette MTU EAP minimum. EAP est un protocole en mode rigide, ce qui implique une certaine inefficacité pour le traitement de la fragmentation et du réassemblage. Donc, si la couche inférieure prend en charge la fragmentation et le réassemblage (comme lorsque EAP est transporté sur IP) il peut être préférable que la fragmentation et le réassemblage se fassent dans la couche inférieure plutôt que dans EAP. Cela peut être accompli en fournissant une MTU EAP artificiellement élevée à EAP, causant le traitement de la fragmentation et du réassemblage au sein de la couche inférieure.

(5) Duplication possible. Lorsque la couche inférieure est fiable, elle va fournir à la couche EAP un flux de paquets non dupliqués. Cependant, bien qu'il soit désirable que les couches inférieures assurent la non duplication, ce n'est pas exigé. Le champ Identifiant fournit à l'homologue et à l'authentificateur la capacité de détecter les dupliqués.

(6) Garanties d'ordre. EAP n'exige pas que l'identifiant soit à croissance monotone, et s'appuie ainsi sur la garantie d'ordre de la couche inférieure pour son fonctionnement correct. EAP était à l'origine conçu pour fonctionner sur PPP, et la Section 1 de la [RFC1661] a une exigence d'ordre : "Le protocole point à point a été conçu pour les liaisons simples qui transportent des paquets entre deux homologues. Ces liaisons permettent un fonctionnement bidirectionnel simultané, et sont supposées livrer les paquets dans l'ordre". Les transports de couche inférieure pour EAP DOIVENT préserver l'ordre entre une source et une destination à un certain niveau de priorité (la garantie d'ordre fournie par [IEEE-802]). La remise en ordre, si elle se produit, va normalement résulter en un échec d'authentification EAP, causant un recommencement de l'authentification EAP. Dans un environnement dans lequel la remise en ordre est probable, on s'attend donc à ce que les échecs d'authentification EAP soient courants. Il est RECOMMANDÉ que EAP ne soit effectué que sur les couches inférieures qui fournissent des garanties d'ordre ; effectuer EAP sur un transport IP brut ou UDP N'EST PAS RECOMMANDÉ. L'encapsulation de EAP au sein de RADIUS [RFC3579] satisfait aux exigences d'ordre, car RADIUS est un protocole en "mode rigide" qui livre les paquets dans l'ordre.

3.2 Usage d'EAP au sein de PPP

Pour établir les communications sur une liaison point à point, chaque extrémité de la liaison PPP envoie d'abord des paquets LCP pour configurer la liaison de données durant la phase d'établissement de liaison. Après l'établissement de la liaison, PPP fournit une phase facultative d'authentification avant de procéder à la phase de protocole de couche réseau.

Par défaut, l'authentification n'est pas obligatoire. Si l'authentification de la liaison est désirée, une mise en œuvre DOIT spécifier l'option Configuration de protocole d'authentification durant la phase d'établissement de liaison.

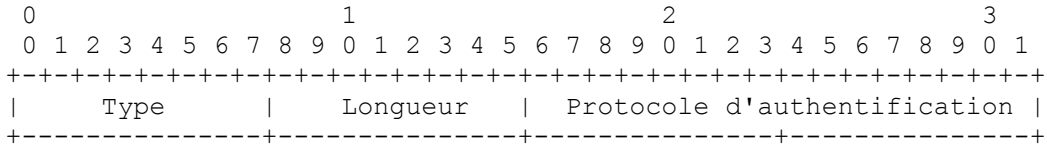
Si l'identité de l'homologue a été établie dans la phase Authentification, le serveur peut utiliser cette identité pour le choix des options pour la suite des négociations de couche réseau.

Lorsque mis en œuvre avec PPP, EAP ne choisit pas un mécanisme d'authentification spécifique à la phase de contrôle de liaison PPP, mais retarde plutôt cela jusqu'à la phase d'authentification. Cela permet à l'authentificateur de demander plus d'informations avant de déterminer le mécanisme d'authentification spécifique. Cela permet aussi d'utiliser un serveur "d'extrémité arrière" qui met en fait en œuvre les divers mécanismes pendant que l'authentificateur PPP passe simplement à travers l'échange d'authentification. Les phases Établissement de liaison PPP et Authentification, et l'option Configuration de protocole d'authentification sont définies dans le protocole point à point (PPP) [RFC1661].

3.2.1 Format de l'option de configuration PPP

Un résumé du format de l'option Configuration de protocole d'authentification PPP pour négocier EAP suit. Les champs sont transmis de gauche à droite.

Exactement un paquet EAP est encapsulé dans le champ Information d'une trame PPP de couche de liaison des données où le champ Protocole indique le type hex C227 (PPP EAP).



Type : 3

Longueur : 4

Protocole d'authentification : C227 (Hex) pour EAP..

3.3 Usage d'EAP au sein de IEEE 802

L'encapsulation de EAP sur IEEE 802 est définie dans [IEEE-802.1X]. L'encapsulation IEEE 802 de EAP n'implique pas PPP, et IEEE 802.1X n'inclut pas la prise en charge de négociations de couche liaison ou réseau. Par suite, au sein de IEEE 802.1X, il n'est pas possible de négocier des mécanismes d'authentification non EAP, tels que PAP ou CHAP [RFC1994].

3.4 Indications des couches inférieures

La fiabilité et la sécurité des indications de couche inférieure dépendent de la couche inférieure. Comme EAP est indépendant du support, la présence ou l'absence de la sécurité de la couche inférieure n'est pas prise en compte dans le traitement des messages EAP.

Pour améliorer la fiabilité, si un homologue reçoit à la couche inférieure une indication de succès comme défini au paragraphe 7.12, il PEUT en conclure qu'un paquet Succès a été perdu, et se comporter comme si il l'avait en fait reçu. Cela inclut de choisir d'ignorer le Succès dans certaines circonstances comme décrit au paragraphe 4.2.

Une discussion de certaines questions de fiabilité et de sécurité avec les indications de la couche inférieure dans PPP, les réseaux câblés IEEE 802, et les LAN sans fil IEEE 802.11 se trouve au paragraphe 7.12 dans les Considérations sur la sécurité.

Après l'achèvement de l'authentification EAP, l'homologue va normalement transmettre et recevoir des données via l'authentificateur. Il est souhaitable de donner l'assurance que les entités qui transmettent des données sont les mêmes que celles qui ont bien achevé l'authentification EAP. Pour ce faire, il est nécessaire que la couche inférieure fournisse la

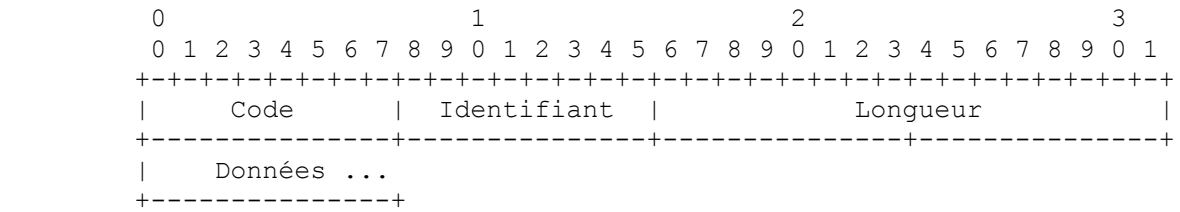
protection par paquet de l'intégrité, l'authentification et la protection contre la répétition, et de lier ces services par paquet aux clés déduites durant l'authentification EAP. Autrement, il est possible que le trafic de données suivant soit modifié, usurpé, ou répété.

Lorsque le matériel de chiffrement pour la suite de chiffrement de la couche inférieure est lui-même fourni par EAP, la négociation de suite de chiffrement et l'activation de clé sont contrôlées par la couche inférieure. Dans PPP, les suites de chiffrement sont négociées au sein de ECP de sorte qu'il n'est pas possible d'utiliser les clés déduites de l'authentification EAP jusqu'à l'achèvement de ECP. Donc, un échange initial EAP ne peut pas être protégé par une suite de chiffrement PPP, bien que la réauthentification EAP puisse être protégée.

Dans un support IEEE 802, l'activation de clé initiale se produit aussi normalement après l'achèvement de l'authentification EAP. Donc un échange initial EAP ne peut normalement pas être protégé par la suite de chiffrement de la couche inférieure, bien qu'un échange de réauthentification ou pré authentification EAP puisse être protégé.

4. Format de paquet EAP

Un résumé du format de paquet EAP est montré ci-dessous. Les champs sont transmis de gauche à droite.



Code : Le champ Code fait un octet et identifie le type du paquet EAP. Les codes EAP sont alloués comme suit :
1 : Demande
2 : Réponse
3 : Succès
4 : Échec

Comme EAP définit seulement les codes 1 à 4, les paquets EAP avec d'autres codes DOIVENT être éliminés en silence par les authentificateurs et les homologues.

Identifiant : le champ Identifiant fait un octet et aide à faire correspondre les réponses avec les demandes.

Longueur : le champ Longueur fait deux octets et indique la longueur, en octets, du paquet EAP incluant les champs Code, Identifiant, Longueur et Données. Les octets en dehors de la gamme du champ Longueur devraient être traités comme du bourrage de couche de liaison des données et DOIVENT être ignorés à réception. Un message avec le champ Longueur réglé à une valeur supérieure au nombre d'octets reçus DOIT être éliminé en silence.

Données : le champ Données fait zéro ou plus octets. Le format du champ Données est déterminé par le champ Code.

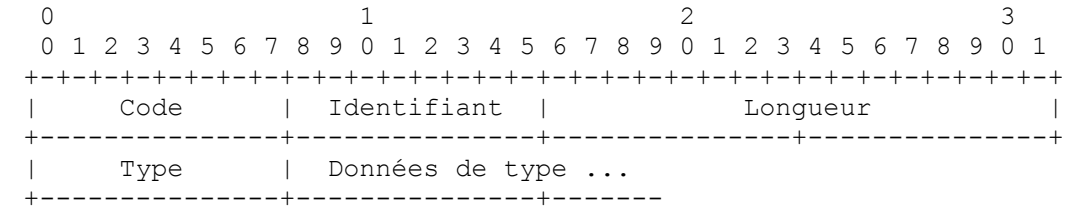
4.1 Demande et réponse

Description : le paquet Demande (champ Code réglé à 1) est envoyé par l'authentificateur à l'homologue. Chaque demande a un champ Type qui sert à indiquer ce qui est demandé. Des paquets Demande supplémentaires DOIVENT être envoyés jusqu'à ce qu'un paquet Réponse valide soit reçu, qu'un compteur facultatif de réessai arrive à expiration, ou qu'une indication de défaillance de la couche inférieure soit reçue.

Les demandes retransmises DOIVENT être envoyées avec la même valeur d'identifiant afin de les distinguer des nouvelles demandes. Le contenu du champ Données dépend du type de demande. L'homologue DOIT envoyer un paquet Réponse en réponse à un paquet Demande valide. Les réponses ne DOIVENT être envoyées qu'en réponse à une demande valide et jamais être retransmises sur un temporisateur.

Si un homologue reçoit une demande dupliquée valide pour laquelle il a déjà envoyé une réponse, il DOIT renvoyer sa demande originale sans retraiter la demande. Les demandes DOIVENT être traitées dans l'ordre de leur réception, et DOIVENT être traitées jusqu'à leur achèvement avant d'inspecter la demande suivante.

Un résumé du format de paquet de demande et réponse suit. Les champs sont transmis de gauche à droite.



Code : 1 pour Demande. 2 pour Réponse

Identifiant : le champ Identifiant fait un octet. Le champ Identifiant DOIT être le même si un paquet Demande est retransmis à cause d'une fin de temporisation pendant l'attente d'une réponse. Toute nouvelle demande (non retransmise) DOIT modifier le champ Identifiant. Le champ Identifiant de la réponse DOIT correspondre à celui de la demande actuellement en instance. Un authentificateur qui reçoit une réponse dont la valeur d'identifiant ne correspond pas à celle de la demande actuellement en instance DOIT éliminer en silence la réponse. Afin d'éviter la confusion entre nouvelles demandes et retransmissions, la valeur d'identifiant choisie pour chaque nouvelle Demande doit seulement être différente de celle de la demande précédente, mais n'a pas besoin d'être unique au sein de la conversation. Une façon de réaliser cela est de commencer l'identifiant à une valeur initiale et de l'incrémenter pour chaque nouvelle demande. Initialiser le premier identifiant avec un nombre aléatoire plutôt que zéro est recommandé, car cela rend les attaques de séquence un peu plus difficiles. Comme l'espace d'identifiants est unique pour chaque session, les authentificateurs ne sont pas restreints à 256 conversations d'authentification simultanées. De même, avec la réauthentification, une conversation EAP peut continuer sur une longue période, et n'est pas limitée à 256 allers retours.

Note de mise en œuvre : l'authentificateur est chargé de retransmettre les messages Demande. Si le message Demande est obtenu d'ailleurs (comme d'un serveur d'authentification d'extrémité arrière) l'authentificateur aura alors besoin de sauvegarder une copie de la demande pour ce faire. L'homologue est chargé de la détection et du traitement des messages Demande dupliqués avant de les traiter de quelque façon que ce soit, incluant de les passer à un tiers extérieur. L'authentificateur est aussi chargé d'éliminer les messages Réponse qui ont une valeur d'identifiant qui ne correspond pas avant d'agir de quelque manière que ce soit sur eux, incluant de les passer au serveur d'authentification d'extrémité arrière pour vérification. Comme l'authentificateur peut retransmettre avant de recevoir une réponse de l'homologue, l'authentificateur peut recevoir plusieurs réponses, chacune avec un identifiant qui correspond. Jusqu'à ce qu'une nouvelle Demande soit reçue par l'authentificateur, la valeur d'identifiant n'est pas mise à jour, de sorte que l'authentificateur transmet les réponses une par une au serveur d'authentification d'extrémité arrière.

Longueur : le champ Longueur fait deux octets et indique la longueur du paquet EAP incluant les champs Code, Identifiant, Longueur, Type, et Données de type. Les octets en dehors de la gamme du champ Longueur devraient être traités comme du bourrage de couche de liaison des données et DOIVENT être ignorés à réception. Un message dont le champ Longueur est réglé à une valeur supérieure au nombre d'octets reçus DOIT être éliminé en silence.

Type : le champ Type fait un octet. Il indique le type de demande ou réponse. Un seul Type DOIT être spécifié pour chaque Demande ou Réponse EAP. Une spécification initiale des types est donnée à la Section 5 du présent document. Le champ Type d'une Réponse DOIT soit correspondre à celui de la Demande, soit correspondre à un Nak traditionnel ou étendu (voir au paragraphe 5.3) indiquant qu'un type de demande est inacceptable pour l'homologue. Un homologue NE DOIT PAS envoyer un Nak (traditionnel ou étendu) en réponse à une Demande, après l'envoi d'une Réponse initiale non Nak. Un serveur EAP qui reçoit une Réponse qui ne satisfait pas à ces exigences DOIT l'éliminer en silence.

Données de type : le champ Données de type varie avec le type de demande et de réponse associée.

4.2 Succès et échec

Le paquet Succès est envoyé par l'authentificateur à l'homologue après l'achèvement d'une méthode d'authentification EAP (Type 4 ou supérieur) pour indiquer que l'homologue s'est bien authentifié auprès de l'authentificateur. L'authentificateur DOIT transmettre un paquet EAP avec le champ Code réglé à 3 (Succès). Si l'authentificateur ne peut pas authentifier l'homologue (Réponses inacceptables à une ou plusieurs demandes) après l'échec de l'achèvement de la méthode EAP en cours, la mise en œuvre DOIT alors transmettre un paquet EAP avec le champ Code réglé à 4 (Échec). Un authentificateur PEUT souhaiter procurer plusieurs demandes avant d'envoyer une réponse d'échec afin de permettre l'entrée des fautes par une personne humaine. Les paquets Succès et Échec NE DOIVENT PAS contenir de données supplémentaires.

Les paquets Succès et Échec NE DOIVENT PAS être envoyés par un authentificateur EAP si la spécification de la méthode

ne permet pas explicitement que la méthode se finisse à ce point. Une mise en œuvre d'homologue EAP qui reçoit un paquet Réussite ou Échec lorsque son envoi n'est pas explicitement permis DOIT l'éliminer en silence. Par défaut, un homologue EAP DOIT éliminer en silence un paquet Succès "emboîté" (un paquet Succès envoyé immédiatement après la connexion). Cela assure qu'un authentificateur pirate ne sera pas capable d'outrepasser l'authentification mutuelle en envoyant un paquet Succès avant la conclusion de la conversation de méthode EAP.

Note de mise en œuvre : comme les paquets Succès et Échec ne reçoivent pas d'accusé de réception, ils ne sont pas retransmis par l'authentificateur, et peut être éventuellement perdus. Un homologue DOIT traiter ces circonstances comme décrit dans cette note. Voir aussi au paragraphe 3.4 des lignes directrices sur le traitement par la couche inférieure des indications de succès et d'échec.

Comme décrit au paragraphe 2.1, une seule méthode d'authentification EAP est permise au sein d'une conversation EAP. Les méthodes EAP peuvent mettre en œuvre des indications de résultat. Après que l'authentificateur a envoyé une indication d'échec à l'homologue, sans considération de la réponse de l'homologue, il DOIT ensuite envoyer un paquet Échec. Après que l'authentificateur a envoyé une indication de succès à l'homologue et reçu une indication de succès de l'homologue, il DOIT ensuite envoyer un paquet Succès.

Sur l'homologue, une fois que la méthode est achevée sans succès (c'est-à-dire, soit l'authentificateur envoie une indication d'échec, soit l'homologue décide qu'il ne veut pas continuer la conversation, éventuellement après l'envoi d'une indication d'échec) l'homologue DOIT terminer la conversation et indiquer l'échec à la couche inférieure. L'homologue DOIT éliminer en silence les paquets Succès et PEUT éliminer en silence les paquets Échec. Par suite, la perte d'un paquet Échec n'a pas besoin de résulter en une fin de temporisation.

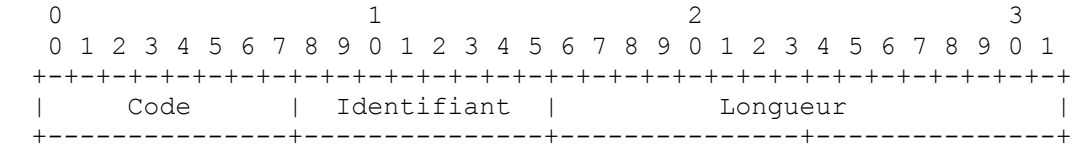
Sur l'homologue, après l'échange des indications de résultat de succès par les deux côtés, un paquet Échec DOIT être éliminé en silence. L'homologue PEUT, si un Succès EAP n'était pas reçu, conclure que le paquet EAP Succès a été perdu et que l'authentification s'est conclue avec succès.

Si l'authentificateur n'a pas envoyé d'indication de résultat, et si l'homologue veut continuer la conversation, il attendra un paquet Succès ou Échec une fois la méthode achevée, et NE DOIT PAS en éliminer en silence. Dans le cas où ni un paquet Succès ni un paquet Échec n'est reçu, l'homologue DEVRAIT terminer la conversation pour éviter de longues temporisations pour le cas où le paquet perdu était un Échec EAP.

Si l'homologue tente de s'authentifier auprès de l'authentificateur et échoue à le faire, l'authentificateur DOIT envoyer un paquet Échec et NE DOIT PAS accorder l'accès en envoyant un paquet Succès. Cependant, un authentificateur PEUT omettre d'authentifier l'homologue dans des situations où un accès limité est offert (par exemple, accès d'invité). Dans ce cas, l'authentificateur DOIT envoyer un paquet Succès.

Lorsque l'homologue s'authentifie avec succès auprès de l'authentificateur, mais que l'authentificateur n'envoie pas d'indication de résultat, l'authentificateur PEUT refuser l'accès en envoyant un paquet Échec où l'homologue n'est pas actuellement autorisé à accéder au réseau.

Un résumé du format de paquet Succès et Échec est donné ci-dessous. Les champs sont transmis de gauche à droite.



Code : 3 pour Succès, 4 pour Échec.

Identifiant : le champ Identifiant fait un octet et aide à faire correspondre les réponses aux Réponses. Le champ Identifiant DOIT correspondre au champ Identifiant du paquet Réponse auquel il est envoyé en réponse.

Longueur : 4

4.3 Comportement de retransmission

Comme le processus d'authentification va souvent impliquer des entrées de la part de l'utilisateur, un certain soin doit être apporté à la décision des stratégies de retransmission et aux temporisations d'authentification. Par défaut, lorsque EAP fonctionne sur une couche inférieure non fiable, le temporisateur de retransmission EAP DEVRAIT être estimé de façon dynamique. Un maximum de 3 à 5 retransmissions est suggéré.

Lorsque il fonctionne sur une couche inférieure fiable (par exemple, EAP sur ISAKMP/TCP, comme dans [PIC]), le temporisateur de retransmission de l'authentificateur DEVRAIT être réglé à une valeur infinie, afin que les retransmissions ne se produisent pas à la couche EAP. L'homologue peut quand même garder une valeur de temporisation de façon à éviter d'attendre indéfiniment une demande.

Lorsque le processus d'authentification exige une entrée de l'utilisateur, le temps d'aller retour mesuré peut être déterminé par la capacité de réponse de l'utilisateur plutôt que par les caractéristiques du réseau, de sorte que l'estimation dynamique du RTO peut n'être pas utile. À la place, le temporisateur de retransmission DEVRAIT être réglé de façon à donner à l'usager un délai suffisant pour répondre, avec de plus longues temporisations nécessaires dans certains cas, comme lorsque des cartes à jetons (voir au paragraphe 5.6) sont impliquées.

Afin de donner des lignes directrices à l'authentificateur EAP sur le réglage de la valeur appropriée de temporisateur, un conseil peut être communiqué à l'authentificateur par le serveur d'authentification d'extrémité arrière (comme via l'attribut RADIUS Temporisateur de session).

Pour estimer dynamiquement le temporisateur de retransmission EAP, les algorithmes pour l'estimation du SRTT, RTTVAR, et RTO décrits dans la [RFC2988] sont RECOMMANDÉS, y compris l'utilisation de l'algorithme de Karn, avec les modifications éventuelles suivantes :

[a] Afin d'éviter les comportements de synchronisation qui pourraient se produire avec des temporisateurs fixes dans des systèmes répartis, le temporisateur de retransmission est calculé avec une gigue en utilisant la valeur du RTO et en ajoutant une valeur aléatoire comprise entre -RTOmin/2 et RTOmin/2. D'autres calculs pour créer une gigue PEUVENT être utilisés. Ils DOIVENT être pseudo aléatoires. Pour une discussion sur la générations de nombres pseudo aléatoires, voir la [RFC1750].

[b] Lorsque EAP est transporté sur une seule liaison (par opposition à sur l'Internet) de plus petites valeurs de RTOinitial, RTOmin, et RTOmax PEUVENT être utilisées. Les valeurs recommandées sont RTOinitial = 1 s, RTOmin = 200 ms, et RTOmax = 20 s.

[c] Lorsque EAP est transporté sur une seule liaison (par opposition à sur l'Internet) les estimations PEUVENT être faites par authentificateur, plutôt que par session. Cela permet que l'estimation de retransmission fasse la meilleure utilisation des informations sur le comportement de la couche de liaison.

[d] Une mise en œuvre EAP PEUT éliminer SRTT et RTTVAR après avoir retardé plusieurs fois le temporisateur, car il est probable que le SRTT et le RTTVAR courants sont faux dans cette situation. Une fois que SRTT et RTTVAR sont éliminés, ils devraient être initialisés avec le prochain échantillon de RTT pris comme décrit dans l'équation 2.2 de la [RFC2988].

5. Types de demande/réponse EAP initiales

Cette section définit le jeu initial de types EAP utilisé dans les échanges Demande/Réponse. D'autres types pourront être définis dans de futurs documents. Le champ Type fait un octet et identifie la structure d'un paquet Demande ou Réponse EAP. Les trois premiers types sont considérés comme des cas particuliers.

Les types restants définissent les échanges d'authentification. Les types Nak (type 3) ou Nak étendu (type 254) ne sont valides que pour des paquets Réponse ; ils NE DOIVENT PAS être envoyés dans une Demande.

Toutes les mises en œuvre EAP DOIVENT prendre en charge les types 1 à 4, qui sont définis dans le présent document, et DEVRAIENT prendre en charge le type 254. Les mises en œuvre PEUVENT prendre en charge les autres types définis ici ou dans de futures RFC.

1 Identité
2 Notification
3 Nak (seulement dans Réponse)
4 Défi MD5
5 Mot de passe à utilisation unique (OTP, *One Time Password*)
6 Carte à jeton générique (GTC, *Generic Token Card*)
254 Types étendus
255 Utilisation expérimentale

Les méthodes EAP PEUVENT prendre en charge l'authentification sur la base de secrets partagés. Si le secret partagé est une phrase de passe entrée par l'utilisateur, les mises en œuvre PEUVENT prendre en charge l'entrée de phrases de passe avec des caractères non ASCII. Dans ce cas, l'entrée devrait être traitée en utilisant un profil de stringprep [RFC3454] approprié, et codée en octets en utilisant le codage UTF-8 [RFC2279]. Une version préliminaire d'un profil stringprep possible est décrite dans la [RFC4013].

5.1 Identité

Description : le type Identité est utilisé pour demander l'identité de l'homologue. Généralement, l'authentificateur va produire cela comme demande initiale. Un message facultatif affichable PEUT être inclus pour inviter l'homologue dans le cas où une interaction avec un utilisateur est espérée. Une Réponse de type 1 (Identité) DEVRAIT être envoyée en réponse à une Demande de type 1 (Identité). Certaines mises en œuvre EAP portent diverses options dans la demande Identité après un caractère NUL. Par défaut, une mise en œuvre EAP NE DEVRAIT PAS supposer qu'une Demande ou Réponse Identité peut faire plus de 1020 octets. Il est RECOMMANDÉ que la réponse Identité soit utilisée principalement pour les besoins de l'acheminement et le choix de la méthode EAP à utiliser. Les méthodes EAP DEVRAIENT inclure un mécanisme spécifique de la méthode pour obtenir l'identité, afin qu'elles n'aient pas à s'appuyer sur la réponse Identité. Les demandes et réponses Identité sont envoyées en clair, de sorte qu'un attaquant peut usurper l'identité, ou même modifier ou simuler les échanges d'identité. Pour contrer ces menaces, il est préférable qu'une méthode EAP inclut un échange d'identité qui prenne en charge l'authentification, la protection de l'intégrité et de la confidentialité et la protection contre la répétition par paquet. La réponse Identité peut n'être pas l'identité appropriée pour la méthode ; elle peut avoir été tronquée ou obscurcie pour assurer la confidentialité, ou elle peut avoir été complétée pour les besoins de l'acheminement. Lorsque l'homologue est configuré à n'accepter que les méthodes d'authentification qui prennent en charge les échanges d'identité protégés, l'homologue PEUT fournir une réponse Identité abrégée (comme en omettant la portion nom de l'homologue du NAI [RFC2486]). Pou un exposé plus complet de la protection de l'identité, voir au paragraphe 7.3.

Note de mise en œuvre : l'homologue PEUT obtenir l'identité via une entrée de l'usager. Il est suggéré que l'authentificateur réessaye la demande Identité dans le cas d'une identité invalide ou d'une défaillance de l'authentification pour permettre d'éventuelle fautes de frappe de la part de l'usager. Il est suggéré que la demande Identité soit réessayée un minimum de trois fois avant de terminer l'authentification. La demande Notification PEUT être utilisée pour indiquer une tentative d'authentification invalide avant de transmettre une nouvelle demande Identité (facultativement, la défaillance PEUT être indiquée au sein du message de la nouvelle demande Identité elle-même).

Type : 1

Données de type : ce champ PEUT contenir un message affichable dans la demande, contenant des caractères UTF-8 codés selon ISO 10646 [RFC2279]. Lorsque la demande contient un caractère NUL, seule la portion du champ avant le NUL est affichée. Si l'identité est inconnue le champ Réponse d'identité devrait être long de zéro octet. Le champ Réponse d'identité NE DOIT PAS être terminé par un caractère NUL. Dans tous les cas, la longueur du champ Données de type est déduite du champ Longueur du paquet Demande/Réponse.

Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : aucun
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non applicable
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.2 Notification

Description : le type Notification est facultativement utilisé pour porter un message affichable de l'authentificateur à l'homologue. Un authentificateur PEUT envoyer une demande Notification à l'homologue à tout moment quand il n'y a pas de demande en instance, avant l'achèvement d'une méthode d'authentification EAP. L'homologue DOIT répondre à une

demande Notification par une réponse Notification sauf si la méthode d'authentification EAP spécifie une interdiction de l'utilisation de messages Notification. Dans tous les cas, une réponse Nak NE DOIT PAS être envoyée en réponse à une demande Notification. Noter que la longueur maximum par défaut d'une demande Notification est de 1020 octets. Par défaut, cela laisse au plus 1015 octets pour le message lisible par l'homme.

Une méthode EAP PEUT indiquer dans sa spécification que les messages Notification ne doivent pas être envoyés durant cette méthode. Dans ce cas, l'homologue DOIT éliminer en silence les demandes Notification à partir du point où il est répondu à une demande initiale de ce type par une réponse du même type.

L'homologue DEVRAIT afficher ce message à l'usager ou l'enregistrer si il ne peut pas être affiché. Le type Notification est destiné à fournir un accusé de réception de notification de nature impérative, mais il n'est pas une indication d'erreur, et donc ne change pas l'état de l'homologue. Les exemples incluent un mot de passe avec une heure d'expiration qui est sur le point d'expirer, un entier de séquence OTP qui est proche de 0, un avertissement d'échec d'authentification, etc. Dans la plupart des circonstances, la notification ne devrait pas être exigée.

Type : 2

Données de type : le champ Données de type dans la demande contient une message affichable supérieur à zéro octets, contenant des caractères UTF-8 codés selon la norme ISO 10646 [RFC2279]. La longueur du message est déterminée par le champ Longueur dans le paquet Demande. Le message NE DOIT PAS être terminé par un caractère NUL. Une réponse DOIT être envoyés en réponse à la demande avec un champ type de 2 (Notification). Le champ Données de type de la réponse fait zéro octet. La réponse devrait être envoyée immédiatement (indépendamment de la façon dont le message est affiché ou enregistré).

Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : aucun
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non applicable
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.3 Nak

5.3.1 Nak traditionnel

Description : le type Nak traditionnel n'est valide que dans les messages Réponse. Il est envoyé en réponse à une demande dans laquelle le type d'authentification désiré est inacceptable. Les types d'authentification ont des numéros à partir de 4. La réponse contient un ou plusieurs types d'authentification désirés par l'homologue. Le type zéro (0) est utilisé pour indiquer que l'envoyeur n'a pas de solution de remplacement viable, et donc l'authentificateur NE DEVRAIT PAS envoyer une autre demande après la réception d'une réponse Nak contenant une valeur zéro.

Comme le type Nak traditionnel n'est valide que dans les réponses et a une fonction très limitée, il NE DOIT PAS être utilisé comme indication d'erreur générale, comme pour la communication de messages d'erreur, ou la négociation de paramètres spécifiques d'une méthode EAP particulière.

Code : 2 pour Réponse.

Identifiant : le champ Identifiant fait un octet et aide à faire correspondre les réponses aux demandes. Le champ Identifiant d'une réponse de Nak traditionnel DOIT correspondre au champ Identifiant du paquet Demande auquel il est envoyé en réponse.

Longueur : ≥ 6

Type : 3

Données de type : lorsque un homologue reçoit une demande pour un type d'authentification inacceptable (4 à 253, 255) ou lorsque un homologue sans prise en charge des types étendus reçoit une demande de type 254, une réponse Nak (type 3) DOIT être envoyée. Le champ Données de type de la réponse Nak (type 3) DOIT contenir un ou plusieurs octets indiquant le ou les types d'authentification désirés, un octet par type, ou la valeur zéro (0) pour indiquer qu'il n'y a pas de solution de remplacement proposée. Un homologue prenant en charge les types étendus qui reçoit une demande pour un type d'authentification inacceptable (4 à 253, 255) PEUT inclure la valeur 254 dans la réponse Nak (type 3) pour indiquer le désir d'un type d'authentification étendu. Si l'authentificateur peut satisfaire cette préférence, il répondra par une demande de type étendu (type 254).

Revendications de sécurité (voir au paragraphe 7.2) :

Mécanismes d'authentification : aucun
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non applicable
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.3.2 Nak étendu

Description : le type Nak étendu n'est valide que dans les messages Réponse. Il DOIT être seulement être envoyé en réponse à une demande de type 254 (type étendu) lorsque le type d'authentification est inacceptable. Le type Nak étendu utilise le format Type étendu lui-même, et la réponse contient un ou plusieurs types d'authentification désirés par l'homologue, tous en format Type étendu. Le type zéro (0) est utilisé pour indiquer que l'envoyeur n'a pas de solution de remplacement viable. Le format général pour le type étendu est décrit au paragraphe 5.7.

Comme le type Nak étendu n'est valide que dans les réponses et a une fonction très limitée, il NE DOIT PAS être utilisé comme indication d'erreur générale, comme pour communiquer les messages d'erreur, ou la négociation de paramètres spécifiques d'une méthode EAP particulière.

Code : 2 pour Réponse.

Identifiant : le champ Identifiant fait un octet et aide à faire correspondre les réponses aux demandes. Le champ Identifiant d'une réponse Nak étendu DOIT correspondre au champ Identifiant du paquet Demande auquel il est envoyé en réponse.

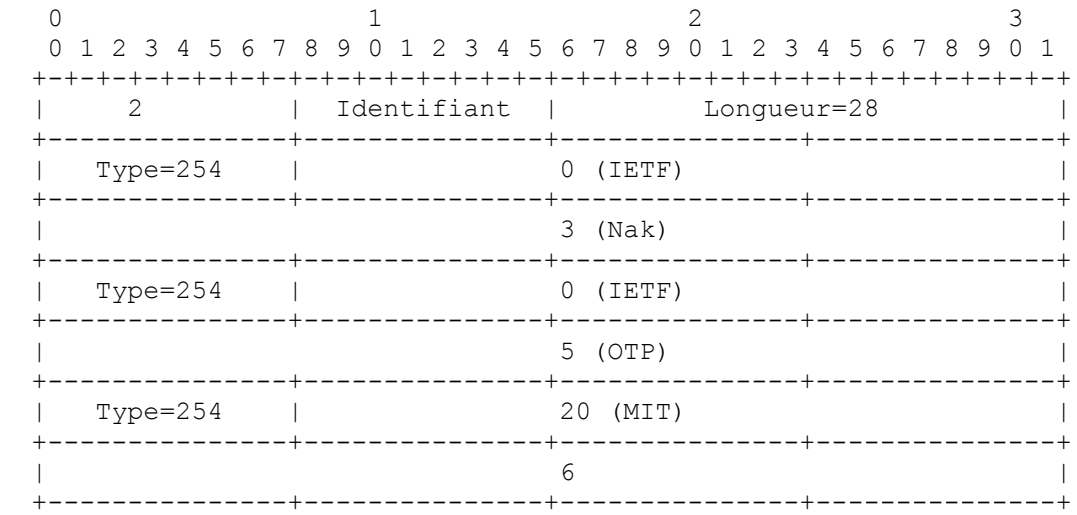
Longueur : ≥ 20

Type : 254

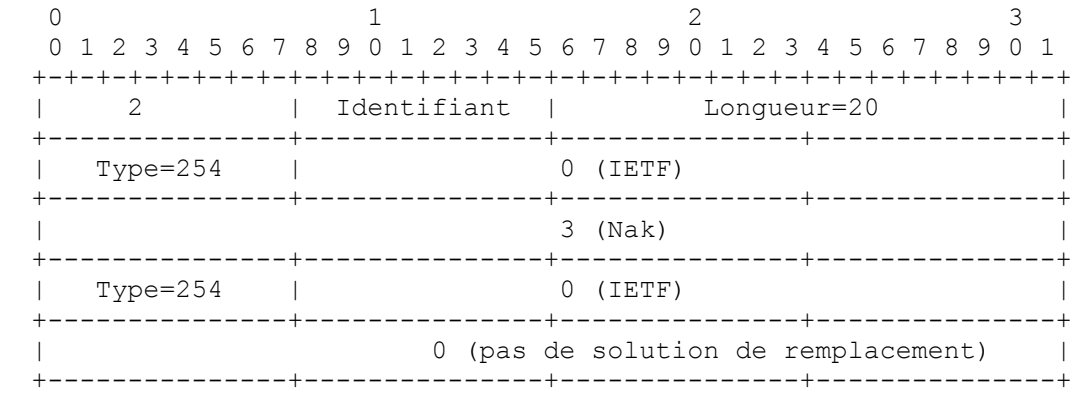
Identifiant de fabricant : 0 (IETF)

Type de fabricant : 3 (Nak)

Données de fabricant : le type Nak étendu n'est envoyé que lorsque la demande contient un type étendu (254) comme défini au paragraphe 5.7. Le champ Identifiant de fabricant de la réponse Nak DOIT contenir un ou plusieurs types d'authentification (4 ou plus) tous en format étendu, de 8 octets par type, ou la valeur zéro (0), aussi en format Type étendu, pour indiquer qu'aucune solution de remplacement n'est proposée. Les types d'authentification proposés peuvent inclure un mélange de types spécifiques du fabricant et IETF. Par exemple, une réponse Nak étendu indiquant une préférence pour OTP (Type 5), et un type étendu MIT (Identifiant de fabricant=20) de 6 apparaîtrait comme suit :



Une réponse de Nak étendu indiquant qu'aucune solution de remplacement n'est désirée apparaîtrait comme suit :



Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : aucun
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non applicable
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.4 Défi MD5

Description : le type Défi MD5 est analogue au protocole PPP CHAP [RFC1994] (avec MD5 comme algorithme spécifié). La demande contient un message "défi" à l'homologue. Une réponse DOIT être envoyée en réponse à la demande. La réponse PEUT être du type 4 (Défi MD5), Nak (Type 3), ou Nak étendu (Type 254). La réponse Nak indique le ou les types d'authentification désirés par l'homologue. Les mises en œuvre d'homologue et serveur EAP DOIVENT prendre en charge le mécanisme de Défi MD5. Un authentificateur qui prend en charge seulement le rôle de passeur DOIT permettre la communication avec un serveur d'authentification d'extrémité arrière qui soit capable de prendre en charge le Défi MD5, bien que la mise en œuvre d'authentificateur EAP n'ait pas besoin de prendre en charge le Défi MD5 lui-même. Cependant, si l'authentificateur EAP peut être configuré à authentifier les homologues en local (par exemple, ne fonctionnant pas comme passeur) l'exigence de prise en charge du mécanisme de Défi MD5 s'applique alors.

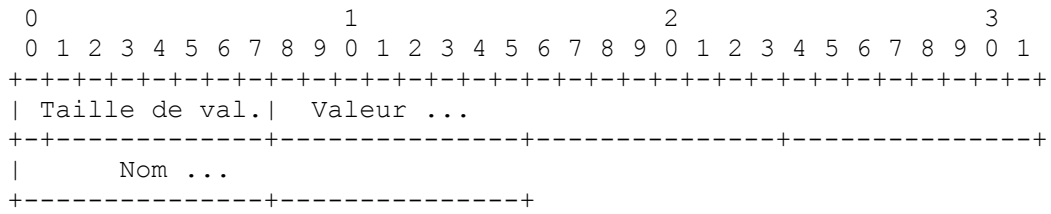
Noter que l'utilisation du champ Identifiant dans le type Défi MD5 est différente de celle décrite dans la [RFC1994]. EAP

permet la retransmission des paquets de demande Défi MD5, tandis que la [RFC1994] déclare que les deux champs Identifiant et Défi DOIVENT changer chaque fois qu'un Défi (équivalent CHAP du paquet Demande de Défi MD5) est envoyé.

Note : la [RFC1994] traite le secret partagé comme une chaîne d'octets, et ne spécifie pas comment il est entré dans le système (ou si il est même traité par l'utilisateur). Les mises en œuvre de Défi MD5 EAP PEUVENT prendre en charge l'entrée de phrases de passe avec des caractères non ASCII. Voir à la Section 5 des instructions sur la façon dont l'entrée devrait être traitée et codée en octets.

Type : 4

Données de type : le contenu du champ Données de type est résumé ci-dessous. Pour la référence sur l'utilisation de ces champs, voir le protocole PPP d'authentification par mise en cause de la pris e de contact [RFC1994].



Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : mot de passe ou clé pré partagée.
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.5 Mot de passe à usage unique

Description : le système de mot de passe à usage unique (OTP, *One-Time Password*) est défini dans "Système de mot de passe à usage unique" [RFC2289] et "Réponses OTP étendues" [RFC2243]. La demande contient un défi OTP dans le format décrit dans la [RFC2289]. Une réponse DOIT être envoyée en réponse à la Demande. La réponse DOIT être du type 5 (OTP), Nak (type 3), ou Nak étendu (Type 254). La réponse Nak indique le ou les types d'authentification désirés par l'homologue. La méthode EAP OTP est destinée à être utilisée seulement avec le système de mot de passe à usage unique, et NE DOIT PAS être utilisée pour la prise en charge de mots de passe en clair.

Type : 5

Données de type : le champ Données de type contient le "défi" OTP comme message affichable dans la Demande. Dans la Réponse, ce champ est utilisé pour les 6 mots du dictionnaire OTP [RFC2289]. Les messages NE DOIVENT PAS être terminés par un caractère NUL. La longueur du champ est déduite du champ Longueur du paquet Demande/Réponse.

Note : la [RFC2289] ne spécifie pas comment la phrase de passe secrète est entrée par l'utilisateur, ni comment la phrase de passe est convertie en octets. Les mises en œuvre OTP d'EAP PEUVENT prendre en charge l'entrée de phrases de passe avec des caractères non ASCII. Voir à la Section 5 des instructions sur la façon dont l'entrée devrait être traitée et codée en octets.

Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : mot de passe à utilisation unique
Négociation de suite de chiffrement : non
Authentification mutuelle : non

Protection de l'intégrité : non
Protection contre la répétition : oui
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.6 Carte de jeton générique

Description : le type Carte à jeton générique (GTC, *Generic Token Card*) est défini pour être utilisé avec diverses mises en œuvre de cartes à jeton qui exigent une entrée de l'usager. La demande contient un message affichable et la réponse contient les informations de carte à jeton nécessaires pour l'authentification. Normalement, elles devraient être des informations lues par un usager à partir de l'appareil de carte à jeton et entrées comme texte ASCII. Une réponse DOIT être envoyée en réponse à la demande. La réponse DOIT être du type 6 (GTC), Nak (type 3), ou Nak étendu (type 254). La réponse Nak indique les types d'authentification désirés par l'homologue. La méthode EAP GTC est destinée à être utilisée avec les cartes à jeton qui prennent en charge l'authentification par défi/réponse et NE DOIT PAS être utilisée pour la prise en charge de mots de passe en clair en l'absence d'un tunnel protégé avec authentification du serveur.

Type : 6

Données de type : le champ Données de type dans la demande contient un message affichable de plus de zéro octets. La longueur du message est déterminée par le champ Longueur du paquet Demande. Le message NE DOIT PAS être terminé par un caractère NUL. Une réponse DOIT être envoyée en réponse à la demande avec un champ Type de 6 (Carte à jeton générique). La réponse contient des données requises pour l'authentification provenant de la carte à jeton. La longueur des données est déterminée par le champ Longueur du paquet Réponse.

Les mises en œuvre GTC d'EAP PEUVENT prendre en charge l'entrée d'une réponse avec des caractères non ASCII. Voir à la Section 5 des instructions sur la façon dont les entrées devraient être traitées et codées en octets.

Revendications de sécurité (voir au paragraphe 7.2) :
Mécanismes d'authentification : jeton matériel
Négociation de suite de chiffrement : non
Authentification mutuelle : non
Protection de l'intégrité : non
Protection contre la répétition : non
Confidentialité : non
Déduction de clé : non
Force de clé : non applicable
Protection contre l'attaque du dictionnaire : non
Reconnexion rapide : non
Lien cryptographique : non applicable
Indépendance de session : non applicable
Fragmentation : non
Lien de canal : non

5.7 Types étendus

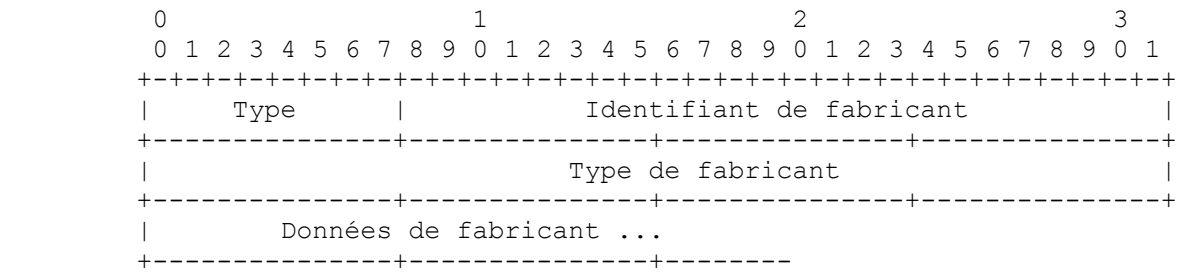
Description : comme beaucoup des utilisations existantes de EAP sont spécifiques d'un fabricant, la méthode Type étendu est disponible pour permettre aux fabricants de prendre en charge leurs propres types étendus qui ne conviennent pas à un usage général.

Le type étendu est aussi utilisé pour étendre l'espace global de type Méthode au delà des 255 valeurs d'origine. Un identifiant de fabricant de 0 transpose les 255 types possibles d'origine en 2^32-1 types possibles. (Le type 0 n'est utilisé que dans une réponse Nak pour indiquer qu'aucune solution de remplacement n'est acceptable).

Une mise en œuvre qui prend en charge l'attribut étendu DOIT traiter les types EAP qui sont de moins de 256 comme

équivalents, qu'ils apparaissent comme un seul octet ou comme le type de fabricant de 32 bits au sein d'un type étendu où l'identifiant de fabricant est 0. Les homologues qui ne sont pas équipés pour interpréter le type étendu DOIVENT envoyer un Nak comme décrit au paragraphe 5.3.1, et négocier une autre méthode d'authentification plus convenable.

Un résumé du format de type étendu est montré ci-dessous. Les champs sont transmis de gauche à droite.



Type : 254 pour type étendu

Identifiant de fabricant : il fait 3 octets et représente le code SMI d'entreprise privée de gestion de réseau du fabricant dans l'ordre des octets du réseau, comme alloué par l'IANA. Un identifiant de fabricant de zéro est réservé pour l'usage de l'IETF pour fournir un espace étendu global de type EAP.

Type de fabricant : le champ Type de fabricant fait quatre octets et représente le type de méthode spécifique du fabricant. Si l'identifiant de fabricant est zéro, le champ Type de fabricant est une extension et un sur ensemble de l'espace de noms existant de types EAP. Les 256 premiers types sont réservés pour la compatibilité avec les types EAP d'un seul octet qui ont déjà été alloués ou pourront être alloués à l'avenir. Donc, les types EAP de 0 à 255 sont sémantiquement identiques, qu'ils apparaissent comme des types EAP d'un seul octet ou comme types de fabricant lorsque Identifiant de fabricant est zéro. Il y a une exception à cette règle : les paquets Nak étendu et Nak traditionnels partagent le même type, mais doivent être traités différemment parce que ils ont un format différent.

Données de fabricant : le champ Données de fabricant est défini par le fabricant. Lorsque un Identifiant de fabricant de zéro est présent, le champ Données de fabricant sera utilisé pour transporter le contenu des méthodes EAP des types définis par l'IETF.

5.8 Expérimental

Description : le type Experimental n'a pas de format ou contenu fixe. Il est destiné à être utilisé lors de l'expérimentation de nouveaux types EAP. Ce type est destiné à des fins d'expérimentation et d'essai. Il n'y a aucune garantie d'interopérabilité entre homologues qui utilisent ce type, comme précisé dans la [RFC3692].

Type : 255

Données de type : indéfinies

6. Considérations relatives à l'IANA

Cette Section donne des lignes directrices à l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) concernant l'enregistrement des valeurs relatives au protocole EAP, conformément au BCP 26, [RFC2434].

Il y a deux espaces de nom dans EAP qui requièrent l'enregistrement : les codes de paquet et les types de méthodes.

EAP n'est pas destiné à être un protocole d'utilisation générale, et les allocations NE DEVRAIT PAS être faites pour des objets sans rapport avec l'authentification.

Les termes suivants sont utilisés ici avec la signification définie dans le BCP 26 : "espace de noms", "valeur allouée", "enregistrement".

Les politiques suivantes sont utilisées ici avec la signification définie dans le BCP 26 : "utilisation privée", "premier entré, premier servi", "révision par expert", "spécification exigée", "consensus de l'IETF", "action de normalisation".

Pour les demandes d'enregistrement où un expert désigné devrait être consulté, le directeur de zone responsable de l'IESG devrait nommer l'expert désigné. L'intention est que toute allocation soit accompagnée d'une RFC publiée. Mais afin de permettre l'allocation de valeurs avant que la publication de la RFC soit approuvée, l'expert désigné peut approuver les allocations une fois qu'il semble clair qu'une RFC sera publiée. L'expert désigné enverra une demande de commentaires et relecture à la liste de diffusion du groupe de travail EAP (ou à un successeur désigné par le directeur de zone) incluant un projet Internet. Avant l'expiration d'une période de 30 jours, l'expert désigné approuvera ou refusera la demande d'enregistrement et publiera une notice de la décision sur la liste de diffusion du groupe de travail EAP ou son successeur, et informera l'IANA. Une notice de refus doit être justifiée par une explication, et dans les cas où c'est possible, des suggestions concrètes sur la façon dont la demande peut être modifiée afin de devenir acceptable, devraient être fournies.

6.1 Types de paquet

Les codes de paquet sont dans la gamme de 1 à 255, dont 1 à 4 ont été alloués. Parce qu'un nouveau code de paquet a un impact considérable sur l'interopérabilité, un nouveau code de paquet exige une action de normalisation, et devrait être alloué en commençant à 5.

6.2 Types de méthodes

L'espace original de type de méthode EAP est dans la gamme de 1 à 255, et c'est la ressource la plus rare dans EAP, et donc elle doit être allouée avec soin. Les types de méthodes 1 à 45 ont été alloués, dont 20 sont disponibles pour réutilisation. Les types de méthodes 20 et 46 à 191 peuvent être alloués sur avis d'un expert désigné, avec spécification exigée.

L'allocation de blocs de types de méthodes (plus d'un pour un certain objet) devrait exiger le consensus de l'IETF. Les valeurs de type EAP 192 à 253 sont réservées et leur allocation exige une action de normalisation.

Le type de méthode 254 est alloué pour le type étendu. Lorsque le champ Identifiant de fabricant est différent de zéro, le type étendu est utilisé pour des fonctions spécifiques de la mise en œuvre d'EAP spécifique d'un fabricant, lorsque aucune interopérabilité n'est réputée utile. Lorsque utilisé avec un Identifiant de fabricant de zéro, le type de méthode 254 peut aussi être utilisé pour fournir un espace de type de méthode IETF étendu. Les valeurs de type de méthode 256 à 4 294 967 295 peuvent être allouées après que les valeurs de type de 1 à 191 auront été allouées, sur avis d'un expert désigné, avec spécification exigée.

Le type de méthode 255 est alloué pour utilisation expérimentale, comme l'essai de nouvelles méthodes EAP avant qu'un type permanent soit alloué.

7. Considérations sur la sécurité

Cette section définit un modèle générique de menace ainsi que les revendications de sécurité des méthodes EAP pour contrer ces menaces.

On s'attend à ce que le modèle générique de menaces et les revendications de sécurité correspondantes soient utilisés pour définir les exigences de méthode EAP à utiliser dans des environnements spécifiques. Un exemple d'une telle analyse d'exigences est fourni dans la [RFC4017]. Une section de revendications de sécurité est exigée dans les spécifications de méthode EAP, afin que les méthodes EAP soient évaluées par rapport à ces exigences.

7.1 Modèle des menaces

EAP a été développé pour être utilisé avec PPP [RFC1661] et a ensuite été adapté pour l'usage des réseaux filaires IEEE 802 [IEEE-802] dans [IEEE-802.1X]. Ensuite, EAP a été proposé à l'utilisation de réseaux LAN sans fil et sur l'Internet. Dans toutes ces situations, il est possible qu'un attaquant obtienne l'accès aux liaisons sur lesquelles des paquets EAP sont transmis. Par exemple, des attaques sur les infrastructures de téléphone sont documentées dans [DECEPTION].

Un attaquant qui a accès à la liaison peut porter un certain nombre d'attaques, incluant :

1. Un attaquant peut essayer de découvrir les identités des utilisateurs en espionnant le trafic d'authentification.
2. Un attaquant peut essayer de modifier ou usurper les paquets EAP.
3. Un attaquant peut lancer des attaques de déni de service en espionnant les indications de la couche inférieure ou les paquets Succès/Échec, en répétant les paquets EAP, ou en générant des paquets avec des identifiants qui se chevauchent.

4. Un attaquant peut tenter de récupérer les phrases de passe en montant une attaque de dictionnaire hors ligne.
5. Un attaquant peut tenter de convaincre l'homologue de se connecter à un réseau qui n'est pas de confiance en montant une attaque par interposition.
6. Un attaquant peut tenter de perturber la négociation EAP afin de causer le choix d'une méthode d'authentification faible.
[7. Un attaquant peut tenter de récupérer des clés en tirant parti de techniques de déduction de clé faible utilisées dans des méthodes EAP.
8. Un attaquant peut tenter de tirer parti de suites de chiffrement faibles utilisées ensuite après l'achèvement de la conversation EAP.
9. Un attaquant peut tenter d'effectuer des attaques en dégradation sur la négociation de suite de chiffrement de la couche inférieure afin de s'assurer qu'une suite de chiffrement plus faible est utilisée ensuite pour l'authentification EAP.
10. Un attaquant agissant comme authentificateur peut fournir des informations incorrectes à l'homologue et/ou serveur EAP via un mécanisme hors bande (comme via un protocole AAA ou de couche inférieure). Cela inclut de se faire passer pour un autre authentificateur, ou de fournir des informations incohérentes à l'homologue et serveur EAP.

Selon la couche inférieure, ces attaques peuvent être menées sans exiger de connexité physique. Lorsque EAP est utilisé sur des réseaux sans fil, les paquets EAP peuvent être transmis par les authentificateurs (par exemple, préauthentification) de sorte que l'attaquant n'a pas besoin d'être dans la zone de couverture d'un authentificateur pour mener à bien une attaque sur son ou ses homologues. Lorsque EAP est utilisé sur l'Internet, des attaques peuvent être conduites à une distance encore plus grande.

7.2. Revendications de sécurité

Afin d'articuler clairement la sécurité fournie par une méthode EAP, les spécifications de méthode EAP DOIVENT inclure une section de revendications de sécurité, incluant les déclarations suivantes :

[a] Mécanisme. C'est une déclaration de la technologie d'authentification : certificats, clés prépartagées, mots de passe, cartes à jetons, etc.

[b] Revendications de sécurité. C'est une déclaration des propriétés de sécurité revendiquées par la méthode, en utilisant les termes définis au paragraphe 7.2.1 : authentification mutuelle, protection de l'intégrité, protection contre la répétition, confidentialité, déduction de clé, résistance aux attaques de dictionnaire, reconnexion rapide, lien cryptographique. La section Revendications de sécurité d'une spécification de méthode EAP DEVRAIT fournir des justifications des revendications faites. Cela peut être accompli en incluant une preuve en appendice, ou en incluant une référence à une preuve.

[c] Force de clé. Si la méthode déduit des clés, la force de clé effective DOIT être estimée. Cette estimation est destinée aux utilisateurs potentiel de la méthode pour déterminer si les clés produites sont assez fortes pour l'application prévue. La force de clé effective DEVRAIT être déclarée comme un nombre de bits, définis comme suit : si la force de clé effective est N bits, les meilleures méthodes actuellement connues pour récupérer la clé (avec une probabilité non négligeable) exigent en moyenne un effort comparable à 2^(N-1) opérations d'un chiffrement de bloc normal. La déclaration DEVRAIT être accompagnée d'une brève explication, précisant comme ce nombre a été déduit. Cette explication DEVRAIT inclure les paramètres requis pour réaliser la force de clé déclarée sur la base de la connaissance actuelle des algorithmes. (Noter que bien qu'il soit difficile de définir ce que "effort comparable" et "chiffrement de bloc normal" signifient exactement, des approximations raisonnables sont ici suffisantes. Se référer par exemple à [SILVERMAN] pour un exposé plus détaillé.) La force de clé dépend des méthodes utilisées pour déduire les clés. Par exemple, si les clés sont déduites d'un secret partagé comme un mot de passe ou un secret à long terme) et éventuellement des informations publiques comme des noms occasionnels, la force effective de la clé est limitée par la force du secret à long terme (en supposant que la procédure de déduction soit simple à calculer). Pour prendre un autre exemple, lorsque on utilise des algorithmes de clé publique, la force de la clé symétrique dépend de la force des clés publiques utilisées.

[d] Description de la hiérarchie des clés. Les méthodes EAP qui déduisent des clés DOIVENT faire référence à une spécification de hiérarchie de clés, ou décrire comment les clés de session maîtresses (MSK, *Master Session Key*) et les clés de session maîtresses étendues (EMSK, *Extended Master Session Key*) sont déduites.

[e] Indication des vulnérabilités. En plus des revendications de sécurité qui sont faites, la spécification DOIT indiquer parmi les revendications de sécurité détaillées au paragraphe 7.2.1 celles qui NE SONT PAS faites.

7.2.1 Terminologie des revendications de sécurité pour les méthodes EAP

Les termes suivants sont utilisés pour décrire les propriétés de sécurité des méthodes EAP :

Négociation de suite de chiffrement protégée.

Ceci se réfère à la capacité d'une méthode EAP de négocier la suite de chiffrement utilisée pour protéger la conversation EAP, ainsi que protéger l'intégrité de la négociation. Cela ne se réfère pas à la capacité de négocier la suite de chiffrement utilisée pour protéger les données.

Authentification mutuelle.
Ceci se réfère à une méthode EAP dans laquelle, au sein d'un échange verrouillé, l'authentificateur authentifie l'homologue et l'homologue authentifie l'authentificateur. Deux méthodes unidirectionnelles indépendantes, fonctionnant dans des directions opposées n'assurent pas l'authentification mutuelle telle que définie ici.

Protection de l'intégrité.
Ceci se réfère à la fourniture de l'authentification de l'origine des données et de la protection contre la modification non autorisée des informations des paquets EAP (incluant les demandes et réponses EAP). Lorsque elle fait cette revendication, une spécification de méthode DOIT décrire les paquets EAP et les champs qui au sein du paquet EAP sont protégés.

Protection contre la répétition.
Ceci se réfère à la protection contre la répétition d'une méthode EAP ou de ses messages, incluant les indications de résultat de succès et d'échec.

Confidentialité.
Ceci se réfère au chiffrement des messages EAP, incluant les demandes et réponses EAP, et les indications de résultat de succès et d'échec. Une méthode qui fait cette revendication DOIT prendre en charge la protection de l'identité (voir au paragraphe 7.3).

Déduction de clé.
Ceci se réfère à la capacité de la méthode EAP de déduire du matériel de chiffrement exportable, comme la clé de session maîtresse (MSK), et la clé de session maîtresse étendue (EMSK). La MSK n'est utilisée que pour une autre déduction de clé, et pas directement pour la protection de la conversation EAP ou des données qui suivent. L'utilisation de la EMSK est réservée.

Force de clé.
Si la force de clé effective est de N bits, les meilleures méthodes actuellement connues pour récupérer la clé (avec une probabilité non négligeable) exigent en moyenne un effort comparable de 2^(N-1) opérations d'un chiffrement de bloc normal.

Résistance à l'attaque du dictionnaire.
Lorsque l'authentification par mot de passe est utilisée, les mots de passe sont couramment choisis à partir d'un petit ensemble (comparé à un ensemble de clés de N bits) qui pose problème vis à vis des attaques de dictionnaire. Une méthode peut être dite fournir protection contre l'attaque du dictionnaire si, lorsque elle utilise un mot de passe comme secret, la méthode ne permet pas une attaque hors ligne qui ait un facteur de travail fondé sur le nombre de mots de passe du dictionnaire d'un attaquant.

Reconnexion rapide.
Capacité, dans le cas où une association de sécurité a été préalablement établie, de créer une association de sécurité nouvelle, ou rafraîchie, plus efficace ou dans un plus petit nombre d'allers retours.

Lien cryptographique.
Démonstration de l'homologue EAP au serveur EAP qu'une seule entité a agit comme homologue EAP pour toutes les méthodes exécutées au sein d'une méthode tunnel. Le lien PEUT aussi impliquer que le serveur EAP démontre à l'homologue qu'une seule entité a agit comme serveur EAP pour toutes les méthodes exécutées au sein d'une méthode tunnel. Si il est exécuté correctement, le lien sert à atténuer les vulnérabilités d'interposition.

Indépendance de session.
C'est la démonstration que des attaques passives (comme la capture de la conversation EAP) ou des attaques actives (incluant la compromission de la MSK ou EMSK) ne permet pas la compromission des MSK ou EMSK suivantes ou antérieures.

Fragmentation.
Ceci se réfère au fait qu'une méthode EAP prend ou non en charge la fragmentation et le réassemblage. Comme noté au paragraphe 3.1, les méthodes EAP devraient prendre en charge la fragmentation et le réassemblage si les paquets EAP peuvent excéder la MTU minimum de 1020 octets.

Lien de canal.
Communication au sein d'une méthode EAP de propriétés de protection de l'intégrité du canal comme identifiants de points

d'extrémité qui peuvent être comparés aux valeurs communiquées via des mécanismes hors bande (comme via un protocole AAA ou de couche inférieure).

Note : cette liste de revendications de sécurité n'est pas exhaustive. Des propriétés supplémentaires, comme une protection supplémentaire contre le déni de service, peuvent aussi être pertinentes.

7.3 Protection d'identité

Un échange d'identité est facultatif au sein de la conversation EAP. Donc, il est possible d'omettre entièrement l'échange d'identité, ou d'utiliser un échange d'identité spécifique de la méthode une fois qu'un canal protégé a été établi.

Cependant, lorsque l'itinérance est prise en charge comme décrit dans la [RFC2607], il peut être nécessaire de localiser le serveur d'authentification d'extrémité arrière approprié avant que la conversation d'authentification puisse se poursuivre. La portion domaine de l'identifiant d'accès réseau (NAI, *Network Access Identifier*) [RFC2486] est normalement incluse dans la réponse d'identité EAP afin de permettre que l'échange d'authentification soit acheminé au serveur d'authentification d'extrémité arrière approprié. Donc, bien que la portion nom d'homologue du NAI puisse être omise dans la réponse d'identité EAP lorsque des mandataires ou relais sont présents, la portion domaine peut être requise.

Il est possible que l'identité dans la réponse d'identité soit différente de l'identité authentifiée par la méthode EAP. Ce peut être intentionnel dans le cas de confidentialité de l'identité. Une méthode EAP DEVRAIT utiliser l'identité authentifiée lors de la prise de décisions de contrôle d'accès.

7.4 Attaques par interposition

Lorsque EAP est tunnelé au sein d'un autre protocole qui omet l'authentification de l'homologue, il existe une vulnérabilité potentielle d'attaque par interposition. Pour les détails, voir [BINDING] et [MITM].

Comme noté au paragraphe 2.1, EAP ne permet pas de séquences non tunnelées de méthodes d'authentification. Si une séquence de méthodes d'authentification EAP devait être permise, l'homologue pourrait n'avoir pas de preuve qu'une seule entité a agit comme l'authentificateur pour toutes les méthodes EAP au sein de la séquence. Par exemple, un authentificateur pourrait terminer une méthode EAP, puis transmettre la prochaine méthode dans la séquence à une autre partie à l'insu ou sans le consentement de l'homologue. De même, l'authentificateur pourrait ne pas avoir la preuve qu'une seule entité a agit comme homologue pour toutes les méthodes EAP au sein de la séquence.

Tunneler EAP au sein d'un autre protocole permet une attaque par une authentificateur EAP pirate qui tunnelle EAP à un serveur légitime. Lorsque le protocole de tunnelage est utilisé pour l'établissement de clés mais n'exige pas l'authentification de l'homologue, un attaquant qui convainc un homologue légitime de se connecter à lui va être capable de tunneler des paquets EAP à un serveur légitime, s'authentifiant avec succès et obtenant la clé. Cela permet à l'attaquant de réussir à s'établir comme interposé, obtenant l'accès au réseau, ainsi que d'avoir la capacité de déchiffrer le trafic de données entre l'homologue légitime et le serveur.

Cette attaque peut être contrée par les mesures suivantes :
[a] Exiger l'authentification mutuelle au sein des mécanismes de tunnelage EAP.
[b] Exiger un lien cryptographique entre le protocole de tunnelage EAP et les méthodes EAP tunnelées. Lorsque le lien cryptographique est pris en charge, un mécanisme est aussi nécessaire pour protéger contre les attaques en dégradation qui l'outrepasseraient. Pou plus de détails sur le lien cryptographique, voir [BINDING].
[c] Limiter les méthodes EAP autorisées sans protection, sur la base de la politique de l'homologue et de l'authentificateur.
[d] Éviter l'utilisation de tunnels lorsque une seule méthode forte est disponible.

7.5 Attaques de modification de paquets

Bien que les méthodes EAP puissent prendre en charge l'authentification d'origine des données, l'intégrité, et la protection contre la répétition par paquet, cette prise en charge n'est pas fournie au sein de la couche EAP.

Comme l'identifiant ne fait qu'un seul octet, il est facile de le deviner, ce qui permet à un attaquant de réussir à injecter ou répéter des paquets EAP. Un attaquant peut aussi modifier les en-têtes EAP (Code, Identifiant, Longueur, Type) au sein des paquets EAP lorsque l'en-tête n'est pas protégé. Ceci peut être cause que des paquets soient éliminés ou mal interprétés de façon inappropriée.

Pour protéger les paquets EAP contre la modification, l'usurpation, ou la répétition, les méthodes qui prennent en charge la négociation de suites de chiffrement protégées, l'authentification mutuelle, et la déduction de clé, ainsi que la protection de

l'intégrité et contre la répétition, sont recommandées. Voir au paragraphe 7.2.1 les définitions de ces revendications de sécurité.

Des MIC spécifiques de la méthode peuvent être utilisés pour assurer la protection. Si un MIC par paquet est employé au sein d'une méthode EAP, les homologues, serveurs d'authentification, et authentificateurs ne fonctionnant pas en mode passeur DOIVENT valider le MIC. Les échecs de validation de MIC DEVRAIENT être enregistrés. Qu'un échec de validation de MIC soit considéré comme une erreur fatale ou non est déterminé par la spécification de la méthode EAP.

Il est RECOMMANDÉ que les méthodes qui fournissent la protection de l'intégrité des paquets EAP incluent la couverture de tous les champs d'en-tête EAP, incluant les champs Code, Identifiant, Longueur, Type, et Données de type.

Comme les messages EAP des types Identité, Notification, et Nak n'incluent pas leur propre MIC, il peut être souhaitable que le MIC de méthode EAP couvre les informations contenues dans ces messages, ainsi que les en-têtes de chaque message EAP.

Pour assurer la protection, EAP peut aussi être encapsulé dans un canal protégé créé par des protocoles comme ISAKMP [RFC2408], comme il est fait dans la [RFC4306]] ou au sein de TLS [RFC2246]. Cependant, comme noté au paragraphe 7.4, le tunnelage EAP peut résulter en une vulnérabilité à l'interposition.

Les méthodes EAP existantes définissent des vérifications d'intégrité de message (les MIC) qui couvrent plus d'un paquet EAP. Par exemple, EAP-TLS [RFC2716] définit un MIC sur un enregistrement TLS qui pourrait être partagé en plusieurs fragments ; au sein du message FINISHED, le MIC est calculé sur les messages précédents. Lorsque le MIC couvre plus d'un paquet EAP, un échec de validation de MIC est normalement considéré comme une erreur fatale.

Dans EAP-TLS [RFC2716], un échec de validation de MIC est traité comme une erreur fatale, car c'est ce qui est spécifié dans TLS [RFC2246]. Cependant, il est aussi possible de développer des méthodes EAP qui prennent en charge des MIC par paquet, et répondent aux échecs de vérification en éliminant en silence le paquet défectueux.

Dans le présent document, les descriptions du traitement du message EAP supposent que la validation de MIC par paquet, lorsque elle se produit, est effectivement effectuée lorsque elle se produit avant d'envoyer une réponse ou de changer l'état de l'hôte qui reçoit le paquet.

7.6 Attaques de dictionnaire

Les algorithmes d'authentification par mot de passe comme EAP-MD5, MS-CHAPv1 [RFC2433], et Kerberos V [RFC1510] sont connus pour être vulnérables aux attaques de dictionnaire. Les vulnérabilités de MS-CHAPv1 sont documentées dans [PPTPv1] ; les vulnérabilités de MS-CHAPv2 sont documentées dans [PPTPv2] ; Les vulnérabilités de Kerberos sont décrites dans [KRBATTACK], [KRBLIM], et [KERB4WEAK].

Pour protéger contre les attaques de dictionnaire, on recommande des méthodes d'authentification résistantes aux attaques de dictionnaire (comme défini au paragraphe 7.2.1).

Si un algorithme d'authentification qui est connu pour être vulnérable aux attaques de dictionnaire est utilisé, la conversation peut alors être tunnelée au sein d'un canal protégé afin de fournir une protection supplémentaire. Cependant, comme noté au paragraphe 7.4, le tunnelage EAP peut résulter en une vulnérabilité à l'interposition, et donc les méthodes résistantes aux attaques de dictionnaire sont préférées.

7.7 Connexion à un réseau qui n'est pas de confiance

Avec les méthodes EAP qui prennent en charge l'authentification unidirectionnelle, comme EAP-MD5, l'homologue n'authentifie pas l'authentificateur, rendant l'homologue vulnérable à l'attaque par un authentificateur pirate. Les méthodes qui prennent en charge l'authentification mutuelle (comme défini au paragraphe 7.2.1) contrent cette vulnérabilité.

Dans EAP, il n'est pas exigé que l'authentification soit bidirectionnelle ou que le même protocole soit utilisé dans les deux directions. Il est parfaitement acceptable que des protocoles différents soient utilisés dans chaque direction. Cela va, bien sûr, dépendre du protocole spécifique négocié. Cependant, en général, réaliser une seule authentification mutuelle unitaire est préférable à deux authentifications unidirectionnelles, une dans chaque direction. C'est parce que des authentifications séparées qui ne sont pas liées cryptographiquement pour montrer qu'elles font partie de la même session sont enclines à des attaques par interposition, comme discuté au paragraphe 7.4.

7.8 Attaques de négociation

Dans une attaque de négociation, l'attaquant tente de convaincre l'homologue et l'authentificateur de négocier une méthode EAP moins sûre. EAP ne fournit pas de protection aux paquets de réponse Nak, bien qu'il soit possible à une méthode d'inclure la couverture des réponses Nak dans un MIC spécifique d'une méthode.

Au sein de chaque authentificateur ou associé à lui, il n'est pas prévu qu'un homologue désigné particulier prenne en charge un choix de méthodes. Cela rendrait l'homologue vulnérable aux attaques qui négocient la méthode la moins sûre d'un ensemble. Il DEVRAIT plutôt y avoir pour chaque homologue désigné une indication d'exactement une méthode utilisée pour authentifier ce nom d'homologue. Si un homologue a besoin d'utiliser des méthodes d'authentification différentes dans des circonstances différentes, des identités distinctes DEVRAIENT être employées, dont chacune identifie exactement une méthode d'authentification.

7.9 Particularités de mise en œuvre

L'interaction de EAP avec les couches inférieures comme PPP et IEEE 802 dépend largement de la mise en œuvre.

Par exemple, en cas d'échec de l'authentification, certaines mises en œuvre PPP ne terminent pas la liaison, limitant plutôt à un sous ensemble filtré le trafic dans les protocoles de couche réseau, ce qui à son tour donne à l'homologue l'opportunité de mettre à jour les secrets ou d'envoyer un message à l'administrateur du réseau pour indiquer un problème. De même, alors qu'un échec d'authentification va résulter en un refus d'accès à l'accès contrôlé dans [IEEE-802.1X], un trafic limité peut être permis sur l'accès non contrôlé.

Dans EAP, il n'y a aucune disposition pour réessayer une authentification qui a échoué. Cependant, dans PPP l'automate à états LCP peut renégocier le protocole d'authentification à tout moment, permettant ainsi une nouvelle tentative. De même, dans IEEE 802.1X, le solliciteur ou l'authentificateur peut se réauthentifier à tout moment. Il est recommandé que les compteurs utilisés pour l'échec d'authentification ne soient pas remis à zéro après la réussite de l'authentification, ou la terminaison subséquente de la liaison en échec.

7.10 Déduction de clé

Il est possible à l'homologue et au serveur EAP de s'authentifier mutuellement et de déduire les clés. Afin de fournir le matériel de chiffrement à utiliser dans une suite de chiffrement négociée ensuite, une méthode EAP qui prend en charge la déduction de clé DOIT exporter une clé de session maîtresse (MSK) d'au moins 64 octets, et une clé de session maîtresse étendue (EMSK) d'au moins 64 octets. Les méthodes EAP qui déduisent les clés DOIVENT assurer l'authentification mutuelle entre l'homologue et le serveur EAP.

La MSK et la EMSK NE DOIVENT PAS être utilisées directement pour protéger les données ; cependant, elles sont de taille suffisante pour permettre la déduction d'une clé AAA utilisée ensuite pour déduire les clés de session transitoires (TSK, *Transient Session Key*) à utiliser avec la suite de chiffrement choisie. Chaque suite de chiffrement est chargée de spécifier comment déduire les TSK de la clé AAA.

La clé AAA est déduite du matériel de chiffrement exporté par la méthode EAP (MSK et EMSK). Cette déduction se fait sur le serveur AAA. Dans de nombreux protocoles existants qui utilisent EAP, la clé AAA et la MSK sont équivalentes, mais des mécanismes plus compliqués sont possibles (voir les détails dans la [RFC5247]).

Les méthodes EAP DEVRAIENT s'assurer de la fraîcheur de la MSK et de l'EMSK, même dans les cas où une partie peut n'avoir pas un générateur de nombres aléatoires de grande qualité. Une méthode RECOMMANDÉE est que chaque partie fournisse au moins 128 bits, utilisés dans la déduction de la MSK et de la EMSK.

Les méthodes EAP exportent la MSK et la EMSK, mais pas les clés de session transitoires afin de permettre aux méthodes EAP d'être indépendantes du support et de la suite de chiffrement. Le matériel de chiffrement exporté par les méthodes EAP DOIT être indépendant de la suite de chiffrement négociée pour protéger les données.

Selon la couche inférieure, les méthodes EAP peuvent fonctionner avant ou après la négociation de la suite de chiffrement, afin que celle qui est choisie ne puisse pas être connue de la méthode EAP. En fournissant du matériel de chiffrement utilisable avec toute suite de chiffrement, les méthodes EAP peuvent être utilisées avec une large gamme de suites de chiffrement et de supports.

Afin de préserver l'indépendance de l'algorithme, les méthodes EAP qui déduisent les clés DEVRAIENT prendre en charge (et documenter) la négociation protégée de la suite de chiffrement utilisée pour protéger la conversation EAP entre l'homologue et le serveur. Ceci est distinct de la suite de chiffrement négociée entre l'homologue et l'authentificateur, utilisée pour protéger les données.

La force des clés de session transitoires (TSK) utilisées pour protéger les données est en fin de compte dépendante de la force des clés générées par la méthode EAP. Si une méthode EAP ne peut pas produire du matériel de chiffrement d'une force suffisante, les TSK peuvent alors être l'objet d'attaques en force brute. Afin de permettre des déploiements exigeant des clés fortes, les méthodes EAP qui prennent en charge la déduction de clé DEVRAIENT être capables de générer une MSK et une EMSK, chacune d'une force de clé effective d'au moins 128 bits.

Les méthodes qui prennent en charge la déduction de clé DOIVENT démontrer la séparation cryptographique entre les branches MSK et EMSK de la hiérarchie de clé EAP. Sans violer une hypothèse cryptographique fondamentale (comme la non réversibilité d'une fonction unidirectionnelle) un attaquant qui découvre la MSK ou la EMSK NE DOIT PAS être capable de découvrir les autres quantités avec un niveau d'effort inférieur à celui de la force brute.

Les sous chaînes sans chevauchement de la MSK DOIVENT être cryptographiquement séparées les unes des autres, comme défini au paragraphe 7.2.1. C'est-à-dire que la connaissance d'une sous chaîne NE DOIT PAS aider à découvrir une autre sous chaîne sans avoir à casser une hypothèse cryptographique forte. Ceci est nécessaire car certaines suites de chiffrement existantes forment des TSK en partageant simplement la clé AAA en morceaux de longueur appropriée. De même, des sous chaînes sans chevauchement de la EMSK DOIVENT être cryptographiquement séparés les unes des autres, ainsi que des sous chaînes de la MSK.

La EMSK est réservée pour une utilisation future et DOIT rester sur l'homologue et le serveur EAP où elle est déduite ; elle NE DOIT PAS être transportée à, ou partagée avec, des parties autres, ou utilisée pour déduire d'autres clés. (Cette restriction sera assouplie dans un futur document qui spécifiera comment la EMSK peut être utilisée.)

Comme EAP ne précise pas une négociation explicite de durée de vie de clé, les homologues, authentificateurs, et serveurs d'authentification EAP DOIVENT être prêts à des situations dans lesquelles une des parties élimine l'état de clé, qui reste valide chez une autre partie.

La présente spécification ne donne pas de lignes directrices détaillées sur la façon dont les méthodes EAP déduisent la MSK et la EMSK, comment la clé AAA est déduite de la MSK et/ou EMSK, ou comment les TSK sont déduites de la clé AAA.

Le développement et la validation des algorithmes de déduction de clés est difficile, et par suite, les méthodes EAP DEVRAIENT réutiliser les mécanismes bien établis et analysés de déduction de clé (comme ceux spécifiés dans IKE [RFC2409] ou TLS [RFC2246]) plutôt que d'en inventer de nouveaux. Les méthodes EAP DEVRAIENT aussi utiliser les mécanismes bien établis et analysés pour la déduction des MSK et EMSK. Plus de détails sur la déduction de clé EAP sont fournis dans la [RFC5247].

7.11 Suites de chiffrement faibles

Si après l'authentification EAP initiale, des paquets de données sont envoyés sans authentification, protection de l'intégrité et contre la répétition par paquet, un attaquant qui a accès au support peut injecter des paquets, des "bits sauteurs" au sein de paquets existants, répéter des paquets, ou même capturer complètement la session. Sans confidentialité par paquet, il est possible d'espionner les paquets de données.

Pour se protéger contre la modification des données, l'espionnage, ou l'usurpation d'identité, il est recommandé que les méthodes EAP prenant en charge l'authentification mutuelle et la déduction de clé (comme défini au paragraphe 7.2.1) soient utilisées, et que les couches inférieures fournissent la confidentialité, l'authentification, la protection de l'intégrité, et la protection contre la répétition par paquet.

De plus, si la couche inférieure effectue la négociation de la suite de chiffrement, il devrait être compris que EAP ne fournit pas par lui-même la protection de l'intégrité de cette négociation. Donc, pour éviter les attaques en dégradation qui conduiraient à l'utilisation de suites de chiffrement plus faibles, les clients qui mettent en œuvre la négociation de suite de chiffrement à la couche inférieure DEVRAIENT se protéger contre la dégradation de la négociation.

Ceci peut être fait en permettant aux usagers de configurer les suites de chiffrement qui sont acceptables au titre de la politique de sécurité, ou que la négociation de suite de chiffrement PEUT être authentifiée en utilisant le matériel de chiffrement déduit de l'authentification EAP et un algorithme de MIC accepté à l'avance par les homologues de couche inférieure.

7.12 Couche de liaison

Il y a des problèmes de fiabilité et de sécurité avec les indications de la couche de liaison des données dans PPP, les LAN IEEE 802, et les LAN sans fil IEEE 802.11 :

[a] PPP. Dans PPP, les indications de couche de liaison comme LCP-Terminate (une indication de défaillance de la liaison) et NCP (une indication de succès de la liaison) ne sont pas authentifiées ou protégées en intégrité. Elles peuvent donc être usurpées par un attaquant qui a accès à la liaison.

[b] IEEE 802. Les trames IEEE 802.1X EAPOL-Start et EAPOL-Logoff ne sont pas authentifiées ni protégées en intégrité. Elles peuvent donc être usurpées par un attaquant qui a accès à la liaison.

[c] IEEE 802.11. Dans IEEE 802.11, les indications de couche de liaison incluent des trames Disassociate et Deauthenticate (indications de défaillance de liaison) et le premier message de la prise de contact en quatre phases (indication de succès de la liaison). Ces messages ne sont pas authentifiés ou protégés en intégrité, et bien qu'ils ne soient pas transmissibles, ils peuvent être usurpés par un attaquant dans le secteur.

Dans IEEE 802.11, les trames de données IEEE 802.1X peuvent être envoyées comme trames de données en envoi individuel de classe 3, et sont donc transmissibles. Cela implique que alors que les messages EAPOL-Start et EAPOL-Logoff peuvent être authentifiés et protégés en intégrité, ils peuvent être usurpés par un attaquant authentifié loin de la cible lorsque la "préauthentification" est activée.

Dans IEEE 802.11, une indication "liaison morte" est une indication non fiable de défaillance de liaison, car la force du signal sans fil peut aller et venir et peut être influencée par des interférences radiofréquences générées par un attaquant. Pour éviter des rétablissements non nécessaires, il est conseillé de diluer ces indications, plutôt que de les passer directement à EAP. Comme EAP prend en charge la retransmission, il est robuste contre les pertes transitoires de connexité.

7.13 Séparation de l'authentificateur et du serveur d'authentification d'arrière

Il est possible à l'homologue et au serveur EAP de s'authentifier mutuellement et déduire une clé AAA pour une suite de chiffrement utilisée pour protéger le trafic de données qui suit. Cela ne présente pas de problème pour l'homologue, car l'homologue et le client EAP résident sur la même machine ; tout ce qui est exigé est que le client déduise la clé AAA de la MSK et de la EMSK exportées par la méthode EAP, et de passer ensuite une clé de session transitoire (TSK) au module de suite de chiffrement.

Cependant, dans le cas où l'authentificateur et le serveur d'authentification résident sur des machines différentes, il y a plusieurs implications pour la sécurité.

[a] L'authentification va se produire entre l'homologue et le serveur d'authentification, et non entre l'homologue et l'authentificateur. Cela signifie qu'il n'est pas possible à l'homologue de valider l'identité de l'authentificateur auquel il parle, en utilisant seulement EAP.

[b] Comme exposé dans la [RFC3579], l'authentificateur dépend du protocole AAA pour savoir le résultat d'une conversation d'authentification, et il ne cherche pas dans le paquet EAP encapsulé (si il en est un présent) pour déterminer le résultat. En pratique, cela implique que le protocole AAA parlé entre l'authentificateur et le serveur d'authentification DOIT prendre en charge l'authentification, la protection de l'intégrité et contre la répétition, par paquet.

[c] Après l'achèvement de la conversation EAP, lorsque les services de sécurité de la couche inférieure tels que la confidentialité l'authentification, la protection de l'intégrité et contre la répétition, par paquet sont activés, un protocole d'association sûr DEVRAIT être établi entre l'homologue et l'authentificateur afin de fournir l'authentification mutuelle entre l'homologue et l'authentificateur, garantir la vivacité des clés de session transitoires, fournir une suite de chiffrement protégée et une négociation de capacités pour les données à suivre, et synchroniser l'utilisation des clés.

[d] Une clé AAA déduite de la MSK et/ou EMSK négociée entre l'homologue et le serveur d'authentification PEUT être transmise à l'authentificateur. Donc, un mécanisme doit être fourni pour transmettre la clé AAA du serveur d'authentification à l'authentificateur qui en a besoin. La spécification des mécanismes de déduction de la clé AAA, du transport, et du comptage sortent du domaine d'application du présent document. Plus de détails sur la déduction de clé AAA figurent dans la [RFC5247].

7.14 Mots de passe en clair

La présente spécification ne définit pas un mécanisme pour l'authentification de mot de passe en clair. L'omission est intentionnelle. L'utilisation de mots de passe en clair permettrait que le mot de passe soit capturé par un attaquant qui aurait accès à une liaison sur laquelle les paquets EAP sont transmis.

Comme les protocoles qui encapsulent EAP, comme RADIUS [RFC3579], peuvent ne pas assurer la confidentialité, les paquets EAP peuvent être ensuite encapsulés pour le transport sur l'Internet où ils peuvent être capturés par un attaquant.

Par suite, les mots de passe en clair ne peuvent pas être utilisés de façon sûre dans EAP, sauf lorsque encapsulés dans un tunnel protégé par l'authentification du serveur. Certains des mêmes risques s'appliquent aux méthodes EAP sans résistance à l'attaque du dictionnaire, comme défini au paragraphe 7.2.1. Pour les détails, voir au paragraphe 7.6.

7.15. Lien de canal

Il est possible à un authentificateur EAP compromis ou mal mis en œuvre de communiquer des informations incorrectes à l'homologue et/ou serveur EAP. Cela peut permettre à un authentificateur de se faire passer pour un autre authentificateur ou de communiquer des informations incorrectes via des mécanismes hors bande (comme via un protocole AAA ou de couche inférieure).

Lorsque EAP est utilisé en mode passeur, l'homologue EAP ne vérifie normalement pas l'identité de l'authentificateur passeur, il vérifie seulement que le passeur authentificateur est de confiance pour le serveur EAP. Ceci crée une vulnérabilité potentielle de la sécurité.

Le paragraphe 4.3.7 de la [RFC3579] décrit comment un authentificateur passeur EAP agissant comme client AAA peut être détecté si il tente de se faire passer pour un autre authentificateur (comme en envoyant des attributs Identifiant de NAS [RFC2865], Adresse IP de NAS [RFC2865] ou Adresse IPv6 de NAS [RFC3162] incorrects via le protocole AAA). Cependant, il est possible à un authentificateur passeur agissant comme client AAA de fournir des informations correctes au serveur AAA tout en communiquant des informations trompeuses à l'homologue EAP via le protocole de couche inférieure.

Par exemple, il est possible à un authentificateur compromis d'utiliser l'identifiant de station appelée ou l'identifiant de NAS d'un autre authentificateur dans une communication avec l'homologue EAP via le protocole de la couche inférieure, ou à un authentificateur passeur qui agit comme client AAA de fournir un identifiant de station appelante d'homologue incorrect [RFC2865], [RFC3580] au serveur AAA via le protocole AAA.

Pour contrer cette vulnérabilité, les méthodes EAP peuvent prendre en charge un échange protégé de propriétés de canal comme des identifiants de point d'extrémité, incluant (mais non limité à) : Identifiant de station appelée [RFC2865], [RFC3580], Identifiant de station appelante [RFC2865], [RFC3580], Identifiant de NAS [RFC2865], Adresse IP de NAS [RFC2865], et Adresse IPv6 de NAS [RFC3162].

En utilisant un tel échange protégé, il est possible de confronter les propriétés du canal fournies par l'authentificateur via des mécanismes hors bande à celles échangées au sein de la méthode EAP. Lorsque des discordances apparaissent, elles DEVRAIENT être enregistrées ; des actions supplémentaires PEUVENT aussi être prises, comme de refuser l'accès.

7.16 Indications de résultat protégées

Au sein de EAP, les paquets Succès et Échec ne sont ni acquittés ni protégés en intégrité. Les indications de résultat améliorent la résilience à la perte des paquets Succès et Échec lorsque EAP fonctionne sur les couches inférieures qui ne prennent pas en charge la retransmission ou la synchronisation de l'état d'authentification. Sur des supports tels que IEEE 802.11, qui assurent la retransmission, ainsi que la synchronisation de l'état d'authentification via la prise de contact en quatre phases définie dans [IEEE-802.11i], une résilience supplémentaire apporte normalement un avantage marginal.

Selon la méthode et les circonstances, les indications de résultat peuvent être usurpées par un attaquant. Une méthode est dite fournir des indications de résultat protégées si elle prend en charge les indications de résultat, ainsi que les revendications de "protection de l'intégrité" et "protection contre la répétition". Une méthode qui prend en charge les indications de résultat protégées DOIT indiquer les indications de résultat qui sont protégées, et celles qui ne le sont pas.

Les indications de résultat protégées ne sont pas exigées pour protéger contre des authentificateurs pirates. Dans une méthode d'authentification mutuelle, exiger que le serveur s'authentifie auprès de l'homologue avant que l'homologue accepte un paquet Succès empêche un attaquant d'agir comme authentificateur pirate.

Cependant, il est possible à un attaquant de falsifier un paquet Succès après que le serveur s'est authentifié auprès de

l'homologue, mais avant que l'homologue se soit authentifié auprès du serveur. Si l'homologue devait accepter le paquet Succès falsifié et tenter d'accéder au réseau alors qu'il n'a pas encore réussi à s'authentifier avec succès auprès du serveur, une attaque de déni de service pourrait être montée contre l'homologue. Après une telle attaque, si la couche inférieure prend en charge les indications d'échec, l'authentificateur peut synchroniser l'état avec l'homologue en fournissant à la couche inférieure une indication d'échec. Voir les détails au paragraphe 7.12.

Si un serveur devait authentifier l'homologue et envoyer un paquet de Succès avant de déterminer si l'homologue a authentifié l'authentificateur, une temporisation d'inactivité peut se produire si l'authentificateur n'est pas authentifié par l'homologue. Lorsque c'est pris en charge par la couche inférieure, un authentificateur qui découvre l'absence de l'homologue peut libérer les ressources.

Dans une méthode qui prend en charge les indications de résultat, un homologue qui a authentifié le serveur ne considère pas l'authentification comme réussie tant qu'il n'a pas reçu une indication que le serveur l'a authentifié avec succès. De même, un serveur qui a authentifié avec succès l'homologue ne considère pas que l'authentification est réussie tant qu'il n'a pas reçu une indication que l'homologue a authentifié le serveur.

Afin d'éviter les problèmes de synchronisation, avant d'envoyer une indication de résultat de succès, il est souhaitable que l'envoyeur vérifie qu'une autorisation suffisante existe pour accorder l'accès, bien que, comme exposé ci-dessous, ceci ne soit pas toujours possible.

Bien que les indications de résultat puissent permettre la synchronisation du résultat de l'authentification entre l'homologue et le serveur, cela ne garantit pas que l'homologue et l'authentificateur vont être synchronisés en termes d'autorisation ou que des fins de temporisation ne vont pas se produire. Par exemple, le serveur EAP peut n'être pas informé d'une décision d'autorisation faite par un mandataire AAA ; le serveur AAA peut ne vérifier l'autorisation qu'après l'achèvement réussi de l'authentification, pour découvrir que l'autorisation ne peut pas être accordée, ou le serveur AAA peut accorder l'accès mais l'authentificateur peut être incapable de le fournir du fait d'un manque temporaire de ressources. Dans ces situations, la synchronisation peut n'être réalisée que via les indications de résultat de la couche inférieure.

Les indications de succès peuvent être explicites ou implicites. Par exemple, lorsque une méthode prend en charge les messages d'erreur, une indication implicite de succès peut être définie comme la réception d'un message spécifique sans un message d'erreur précédant. Les échecs sont normalement indiqués explicitement. Comme décrit au paragraphe 4.2, un homologue élimine en silence un paquet Échec reçu à un point où la méthode ne permet pas explicitement qu'il soit envoyé. Par exemple, une méthode qui fournit ses propres messages d'erreur peut exiger que l'homologue reçoive un message d'erreur avant d'accepter un paquet d'échec.

L'authentification, la protection en intégrité et contre la répétition par paquet des indications de résultat protège contre l'usurpation. Comme les indications de résultat protégées exigent l'utilisation d'une clé pour l'authentification et la protection d'intégrité par paquet, les méthodes qui prennent en charge les indications de résultat protégées DOIVENT aussi prendre en charge les revendications de "déduction de clé", "authentification mutuelle", "protection de l'intégrité", et "protection contre la répétition".

Les indications de résultat protégées règlent certaines vulnérabilités au déni de service dues à l'usurpation de paquets de Succès et Échec, mais pas toutes. Les méthodes EAP ne peuvent normalement fournir des indications de résultat protégées que dans certaines circonstances. Par exemple, des erreurs peuvent se produire avant la déduction de clé, et donc il peut n'être pas possible de protéger toutes les indications d'échec. Il est aussi possible que les indications de résultat ne puissent pas être prises en charge dans les deux directions ou que la synchronisation ne puisse pas être réalisée dans tous les modes de fonctionnement.

Par exemple, au sein de EAP-TLS [RFC2716], dans la prise de contact d'authentification de client, le serveur authentifie l'homologue, mais ne reçoit pas une indication protégée de si l'homologue l'a authentifié. À l'opposé, l'homologue authentifie le serveur et sait si le serveur l'a authentifié. Dans la prise de contact de reprise de session, l'homologue authentifie le serveur, mais ne reçoit pas une indication protégée de si le serveur l'a authentifié. Dans ce mode, le serveur authentifie l'homologue et sait si l'homologue l'a authentifié.

8. Remerciements

Le présent protocole a largement été inspiré par le document AHA de Dave Carrel, ainsi que par le protocole PPP CHAP [RFC1994]. Des retours précieux ont été fournis par Yoshihiro Ohba de Toshiba America Research, Jari Arkko de Ericsson, Sachin Seth de Microsoft, Glen Zorn de Cisco Systems, Jesse Walker de Intel, Bill Arbaugh, Nick Petroni et Bryan Payne de l'Université de Maryland, Steve Bellovin de AT&T Research, Paul Funk de Funk Software, Pasi Eronen de Nokia, Joseph Salowey de Cisco, Paul Congdon de HP, et des membres du groupe de travail EAP.

L'utilisation de sections de revendications de sécurité pour les méthodes EAP, comme demandé au paragraphe 7.2 et spécifié pour chaque méthode EAP décrite dans le présent document, a été inspirée par Glen Zorn dans la [RFC5836].

9. Références

9.1 Références normatives

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2243] C. Metz, "Réponses OTP étendues", novembre 1997. *(P.S.)*

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[RFC2289] N. Haller, C. Metz, P. Nesser, M. Straw, "Système de mot de passe à utilisation unique", février 1998. (STD0061)

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC5226)

[RFC2988] V. Paxson, M. Allman, "Calcul du temporisateur de retransmission de TCP", novembre 2000. *(P.S.)(Obs., voir* RFC6298)

[IEEE-802] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Overview and Architecture", IEEE Standard 802, 1990.

[IEEE-802.1X] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, septembre 2001.

9.2 Références pour information

[BINDING] Puthenkulam, J., "The Compound Authentication Binding Problem", Travail en cours, octobre 2003.

[DECEPTION] Slatalla, M. et J. Quittner, "Masters of Deception", Harper-Collins, New York, 1995.

[IEEE-802.11] Institute of Electrical and Electronics Engineers, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11, 1999.

[IEEE-802.11i] Institute of Electrical and Electronics Engineers, "Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE Draft 802.11i (travail en cours), 2003.

[KERB4WEAK] Dole, B., Lodin, S. and E. Spafford, "Misplaced trust: Kerberos 4 session keys", Proceedings of the Internet Society Network and Distributed System Security Symposium, pp. 60-70, mars 1997.

[KRBATTACK] Wu, T., "A Real-World Analysis of Kerberos Password Security", Proceedings of the 1999 ISOC Network and Distributed System Security Symposium, http://www.isoc.org/isoc/conferences/ndss/99/proceedings/papers/wu.pdf .

[KRBLIM] Bellovin, S. and M. Merrit, "Limitations of the Kerberos authentification system", Proceedings of the 1991 Winter USENIX Conference, pp. 253-267, 1991.

[MITM] Asokan, N., Niemi, V. and K. Nyberg, "Man-in-the-Middle in Tunneled Authentication Protocols", IACR ePrint Archive Report 2002/163, octobre 2002, < http://eprint.iacr.org/2002/163 >.

[PIC] Aboba, B., Krawczyk, H. and Y. Sheffer, "PIC, A Pre-IKE Credential Provisioning Protocol", Travail en cours, octobre 2002.

[PPTPv1] Schneier, B. and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol", Proceedings of the 5th ACM Conference on Communications et Computer Security, ACM Press, novembre 1998.

[PPTPv2] Schneier, B. and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", CQRE 99, Springer-Verlag, 1999, pp. 192-203.

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir* RFC6649)

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2284] L. Blunk, J. Vollbrecht, "Protocole extensible d'authentification (EAP) en PPP", mars 1998. (*Obs., voir* RFC3748) *(P.S.)*

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2433] G. Zorn, S. Cobb, "Extensions CHAP de Microsoft à PPP", octobre 1998. *(Information)*

[RFC2486] B. Aboba, M. Beadles, "Identifiant d'accès réseau", janvier 1999. (*Obsolète, voir* RFC4282) *(P.S.)*

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999. *(Info.)*

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2 "L2TP"", *(P.S.)*

[RFC2716] B. Aboba, D. Simon, "Protocole d'authentification des TLS d'EAP dans PPP" octobre 1999. (*Obs., voir* RFC5216) *(Exp.)*

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080) *(D.S.)*

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3162] B. Aboba, G. Zorn, D. Mitton, "RADIUS et IPv6", août 2001. *(P.S.)*

[RFC3454] P. Hoffman et M. Blanchet, "Préparation de chaînes internationalisées ("stringprep")", décembre 2002. *(P.S.)*

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS",

septembre 2003. (*MàJ par* RFC5080) *(Information)*

[RFC3580] P. Congdon et autres, "Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) IEEE 802.1X", septembre 2003. *(Information)*

[RFC3692] T. Narten, "L'allocation de numéros expérimentaux et d'essai est considérée comme utile", janvier 2004. (BCP0082)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4013] K. Zeilenga, "SASLprep : Profil Stringprep pour les noms d'utilisateur et mots de passe", février 2005.

[RFC4017] D. Stanley et autres, "Exigences de méthode pour le protocole d'authentification extensible (EAP) pour les LAN sans fil", mars 2005. *(Information)*

[RFC4072] P. Eronen et autres, "Application du protocole Diameter d'authentification extensible (EAP)", août 2005. *(P.S.)*

[RFC5247] B. Aboba et autres, "Cadre de gestion des clés du protocole d'authentification extensible (EAP)", août 2008. (*MàJ* RFC3748) *(P.S.)*

[RFC5836] Y. Ohba, Q. Wu, G. Zorn, "Position du problème de l'authentification précoce dans le protocole extensible d'authentification (EAP)", avril 2010. *(Information)*

[SILVERMAN] Silverman, Robert D., "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths", RSA Laboratories Bulletin 13, avril 2000 (révisé novembre 2001), http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html .

Appendice A. Changements par rapport à la RFC 2284

Voici la liste des changements majeurs entre la [RFC2284] et le présent document. Les changements mineurs, de style, grammaticaux, d'orthographe, et rédactionnels ne sont pas mentionnés ici.

- La section Terminologie (paragraphe 1.2) a été étendue, pour définir plus de concepts et donner des définitions plus exactes.

- Les concepts d'authentification mutuelle, de déduction de clé, et d'indications de résultat sont introduits et discutés tout au long du document lorsque approprié.

- La Section 2, spécifie explicitement que plus d'un échange de paquets Demande et Réponse peut survenir au titre de l'échange d'authentification EAP. Comment cela peut être utilisé ou non est spécifié en détail au paragraphe 2.1.

- À la Section 2, des exigences ont été rendues explicites pour l'authentificateur agissant en mode passeur.

- Un modèle de multiplexage EAP (paragraphe 2.2) a été ajouté pour illustrer une mise en œuvre normale d'EAP. Il n'est pas exigé qu'une mise en œuvre se conforme à ce modèle, tant que le comportement sur le réseau est cohérent avec lui.

- Comme EAP est maintenant utilisé avec diverses couches inférieures, et non plus seulement PPP pour lequel il avait d'abord été conçu, la Section 3 sur le comportement des couches inférieures a été ajoutée.

- Dans la description de l'interaction Demande Réponse EAP (paragraphe 4.1) le comportement à réception de demandes dupliquées, et lorsque des paquets devraient être éliminés en silence a été spécifié de façon plus exacte. Les notes de mise en œuvre y ont été substantiellement étendues.
- Au paragraphe 4.2, on a précisé que les paquets Succès et Échec ne doivent pas contenir de données supplémentaires, et la note de mise en œuvre a été développée. Un nouveau paragraphe donne les exigences pour le traitement des paquets de succès et d'échec.

- La Section 5 sur les types de demande/réponse EAP indique deux nouvelles valeurs de type : le type Étendu (paragraphe 5.7) qui est utilisé pour étendre l'espace de numéro de valeur de type, et le type Expérimental. Dans l'espace de numéro de type Étendu, le nouveau type Nak étendu (paragraphe 5.3.2) a été ajouté. Des précisions ont été apportées à la description de la plupart des types existants. Un résumé des revendications de sécurité a été ajouté pour les méthodes d'authentification.

- Une exigence a été ajoutée aux paragraphes 5.1, et 5.2, disant que les champs avec un message affichable devraient contenir des caractères UTF-8 codés selon la norme ISO 10646.

- Il est maintenant exigé au paragraphe 5.1 que si le champ Données de type d'une demande Identité contient un caractère NUL, seule la partie avant le NUL est affichée. La RFC 2284 interdit la terminaison par un caractère NUL du champ Données de type des messages Identité. Cette règle a été assouplie pour les messages Demande d'identité et le champ Données de type de la demande Identité peut maintenant être terminé par un caractère NUL.

- Au paragraphe 5.5, la prise en charge des réponses étendues OTP [RFC2243] a été ajoutée à EAP OTP.

- Une Section "Considérations relatives à l'IANA" (Section 6) a été ajoutée, donnant les politiques d'enregistrement pour les espaces de numérotation définis pour EAP.

- La Section Considérations sur la sécurité (Section 7) a été très étendue, donnant une couverture plus complète des menaces possibles et des autres considérations sur la sécurité.

- Au paragraphe 7.5, du texte a été ajouté sur le comportement spécifique de la méthode, donnant des lignes directrices sur la façon dont les vérifications d'intégrité spécifiques de la méthode EAP devraient être traitées. Lorsque possible, il est désirable qu'un MIC spécifique de la méthode soit calculé sur la paquet EAP entier, incluant l'en-tête de couche EAP (Code, Identifiant, Longueur) et et l'en-tête de couche de méthode EAP (Type, Données de type).

- Au paragraphe 7.14 sont décrits les risques pour la sécurité impliqués par l'utilisation de mots de passe en clair avec EAP.

- Au paragraphe 7.15 a été ajouté un texte sur la détection de comportements de NAS malveillant.

Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
téléphone : +1 425 706 6605
Fax : +1 425 936 6605
mél : bernarda@microsoft.com

Larry J. Blunk
Merit Network, Inc
4251 Plymouth Rd., Suite 2000
Ann Arbor, MI 48105-2785
USA
téléphone : +1 734-647-9563
Fax : +1 734-647-3185
mél : ljb@merit.edu

John R. Vollbrecht
Vollbrecht Consulting LLC
9682 Alice Hill Drive
Dexter, MI 48130
USA
mél : jrv@umich.edu

James Carlson
Sun Microsystems, Inc
1 Network Drive
Burlington, MA 01803-2757
USA
téléphone : +1 781 442 2084
Fax : +1 781 442 1677
mél : james.d.carlson@sun.com

Henrik Levkowetz
ipUnplugged AB
Arenavagen 33
Stockholm S-121 28
SWEDEN
téléphone : +46 708 32 16 08
mél : henrik@levkowetz.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.