Groupe de travail Réseau
**Request for Comments : 4334**
RFC rendue obsolète : 3770
Catégorie : Sur la voie de la normalisation

R. Housley,Vigil Security
T. Moore, Microsoft
février 2006
Traduction Claude Brière de L'Isle

# Extensions de certificat et attributs prenant en charge l'authentification dans le protocole point à point (PPP) et les réseaux de zone locale sans fil (WLAN)



**Résumé**
Le présent document définit deux valeurs d'usage de clés étendues du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) et une extension de certificat de clé publique pour porter les identifiants de service système (SSID, *System Service identifier*) de LAN sans fil (WLAN, *Wireless LAN*). Ce document rend obsolète la RFC 3770.

## 1. Introduction

Plusieurs méthodes d'authentification du protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) [RFC3748] emploient des certificats de clé publique X.509. Par exemple, EAP-TLS [RFC2716] peut être utilisé avec PPP [RFC1661] ainsi que IEEE 802.1X [802.1X]. PPP est utilisé pour les environnements de numérotation et de VPN. La norme IEEE 802.1X définit un contrôle d'accès fondé sur l'accès, et elle est utilisée pour fournir un accès réseau authentifié pour les réseaux Ethernet, d'anneau à jetons *(Token Ring)*, de LAN sans fil (WLAN) [802.11], et autres réseaux IEEE 802.

La sélection automatisée des certificats de client à utiliser avec PPP et IEEE 802.1X est très souhaitable. En utilisant des extensions de certificat pour identifier l'environnement désiré pour un certificat particulier, on minimise le besoin d'une entrée de l'utilisateur. De plus, les extensions de certificat facilitent la séparation des fonctions administratives associées aux certificats utilisés pour les différents environnements.

IEEE 802.1X peut être utilisé pour l'authentification avec plusieurs réseaux. Par exemple, la même station sans fil peut utiliser IEEE 802.1X pour s'authentifier auprès d'un WLAN d'entreprise IEEE 802.11 et d'une borne publique d'accès sans fil IEEE 802.11. Chacun de ces WLAN IEEE 802.11 a un nom de réseau différent, appelé l'identifiant d'ensemble de service (SSIP, *Service Set Identifier*). Si les opérateurs de réseau ont un accord d'itinérance, l'authentification inter domaines permet d'utiliser le même certificat sur les deux réseaux. Cependant, si les réseaux n'ont pas d'accord d'itinérance, le demandeur IEEE 802.1X doit alors choisir un certificat pour l'environnement de réseau courant. Inclure une liste des SSID dans une extension de certificate facilite la sélection automatisée d'un certificat de clé publique X.509 approprié sans intervention de l'utilisateur humain. Autrement, un certificat d'attribut d'accompagnement pourrait contenir la liste des SSID.

Le présent document définit des valeurs d'usage de clés étendues et une extension de certificat spécifique pour les WLAN à utiliser dans les certificats produits aux clients de PPP et des WLAN.

### 1.1 Changements par rapport à la RFC 3770

Le présent document est très semblable à la RFC 3770. Six changements significntifs sont inclus :

* Ce document utilise les mêmes références normatives pour l'ASN.1 que la [RFC3280]. L'intention est d'avoir les mêmes annexes.

* La discussion du bit critique dans l'extension de certificat à la Section 2 est alignée sur la RFC 3280. Aussi, la discussion de l'extension de certificat d'usage de clé a été développée.

* La RFC 3770 contenait une erreur typographique dans l'identifiant d'objet pour l'attribut de certificat d'attribut de SSID de WLAN. La Section 4 corrige cette erreur typographique.

* Il est précisé que l'extension de SSID peut apparaître dans des certificats qui ne comportent pas l'extension d'usage de clé étendue.

* Le document utilise les termes "homologue", "serveur EAP", et "demandeur" comme ils sont définis dans la [RFC3748] et [802.1X]. La RFC 3770 utilisait "client" et "serveur".

* L'identifiant d'objet pour l'extension de certificat d'usage de clé étendue est mentionné dans la RFC 3280, et il n'est plus répété dans le présent document.

### 1.2 Conventions utilisées dans le document

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].

### 1.3 Notation de syntaxe abstraite

Toutes les extension de certificat [X.509] sont définies en utilisant l'ASN.1 [X.680], [X.690].

## 2. Valeurs d'usage de clé étendue EAP

La [RFC3280] spécifie l'extension de certificat X.509 d'usage de clé étendue. L'extension indique un ou plusieurs objets pour lesquels la clé publique certifiée peut être utilisée. L'extension d'usage de clé étendue peut être utilisée en conjonction avec l'extension d'usage de clé, qui indique l'objet prévu de la clé publique certifiée.

La syntaxe d'extension d'usage de clé étendue est répétée ici pour l'agrément du lecteur :

ExtKeyUsageSyntax ::= SEQUENCE TAILLE (1..MAX) DE KeyPurposeId

KeyPurposeId ::= IDENTIFIANT D'OBJET

La présente spécification définit deux valeurs de KeyPurposeId *(identifiant de clé proposée)* : une pour EAP sur PPP, et une pour EAP sur LAN (EAPOL). L'inclusion de la valeur de EAP sur PPP indique que la clé publique certifiée est appropriée pour l'utilisation par un homologue avec EAP dans l'environnement PPP. L'inclusion de la valeur EAPOL indique que la clé publique certifiée est appropriée pour une utilisation par un homologue avec EAP dans l'environnement de LAN. L'inclusion des deux valeurs indique que la clé publique certifiée est appropriée pour être utilisée par un homologue dans l'un ou l'autre environnement.

IDENTIFIANT D'OBJET id-kp ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 3 }

IDENTIFIANT D'OBJET id-kp-eapOverPPP ::= { id-kp 13 }

IDENTIFIANT D'OBJET id-kp-eapOverLAN ::= { id-kp 14 }

L'extension d'usage de clé étendue PEUT, au choix du producteur de certificat, être soit critique, soit non critique.

Les applications qui utilisent les certificats PEUVENT exiger que soit présente l"extension d'usage de clé étendue dans un certificat, et elles PEUVEN exiger que soit présente une valeur particulière de KeyPurposeId (comme id-kp-eapOverPPP

ou id-kp-eapOverLAN) au sein de l'extension d'usage de clé étendue. Si plusieurs valeurs de KeyPurposeId sont incluses, l'application qui utilise le certificat n'a pas besoin de les reconnaître tous, pour autant que la valeur requise de KeyPurposeId est présente.

Si un certificat contient une extension d'usage de clé, les bits KeyUsage qui sont nécessaires dépendent de la méthode EAP employée.

Si un certificat contient à la fois une extension d'usage de clé et une extension d'usage de clé étendue, le deux extensions DOIVENT alors être traitées indépendamment, et le certificat ne DOIT être utilisé que pour un objet cohérent avec les deux extensions. Si il n'y a pas d'objet cohérent commun aux deux extensions, l'application qui utilise le certificat NE DOIT utiliser le certificate pour aucun objet.

## 3. Extension de certificat de clé publique de SSID de WLAN

L'extension de certificat de clé publique des identifiants de service de système (SSID, *System Service identifier*) de LAN sans fil (WLAN, *Wireless LAN*) est toujours non critique. Elle contient une liste des SSID. La liste des SSID PEUT être utilisée pour choisir le certificat correct pour l'authentification dans un WLAN particulier.

Si l'extension d'usage de clé étendue apparaît dans le même certificat que l'extension de SSID, l'extension d'usage de clé étendue DOIT indiquer que la clé publique certifiée est appropriée pour une utilisation avec EAP dans l'environnement de LAN en incluant la valeur de KeyPurposeId id-kp-eapOverLAN.

Comme les valeurs de SSID ne sont pas gérées, le même SSID peut apparaître dans différents certificats qui sont destinés à être utilisés dans des WLAN différents. Quand cela se procuit, la sélection automatique de certificat va échouer, et la mise en œuvre DEVRAIT obtenir de l'aide de la part de l'utilisateur pour choisir le certificat correct. Dans les cas où un utilisateur humain n'est pas disponible, chaque certificat potentiel PEUT être essayé jusqu'à ce qu'un réussisse. Cependant, en tenant une antémémoire d'adresses MAC de points d'accès ou une identité de serveur EAP avec laquelle le certificat a été authentifié avec succès, l'implication de l'utilisateur peut être minimisée. RADIUS [RFC2865], [RFC3580] est généralement utilisé comme service d'authentification dans les déploiements de WLAN. L'antémémoire peut être utilisée pour éviter de futures interactions d'utilisateur humain ou le choix du certificat par essai et erreur.

L'extension de SSID de WLAN est identifiée par id-pe-wlanSSID.

```
IDENTIFIANT D'OBJET id-pe ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                                1 }

IDENTIFIANT D'OBJET  id-pe-wlanSSID ::= { id-pe 13 }
```

La syntaxe pour l'extension SSID de WLAN est :

```
SSIDList  ::=  SEQUENCE TAILLE (1..MAX) DE SSID

SSID  ::=  CHAINE D'OCTETS (TAILLE (1..32))
```

## 4. Attribut de certificat d'attribut de SSID de WLAN

Quand le certificat de clé publique n'inclut pas d'extension de certificat SSID de WLAN, un certificat d'attribut [RFC3281] peut être utilisé pour associer une liste de SSID au certificat de clé publique. L'attribut de certificat d'attribut de SSID de WLAN contient une liste des SSID, et la liste des SSID PEUT être utilisée pour choisir le certificat correct pour l'authentification dans un environnement de WLAN particulier.

L'attribut de certificat d'attribut de SSID de WLAN est identifié par id-aca-wlanSSID.

```
IDENTIFIANT D'OBJET id-aca ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
                                 pkix(7) 10 }

IDENTIFIANT D'OBJET id-aca-wlanSSID  ::= { id-aca 7 }
```

La syntaxe pour l'attribut de certificat d'attribut de SSID de WLAN est exactement la même que pour l'extension de SSID de WLAN :

SSIDList ::= SEQUENCE TAILLE (1..MAX) DE SSID

SSID ::= CHAINE D'OCTETS (TAILLE (1..32))

## 5. Considérations sur la sécurité

Les procédures et pratiques employées par l'autorité de certification (CA) DOIVENT assurer que les valeurs correctes pour l'extension d'usage de clé étendue et l'extension de SSID sont insérées dans chaque certificat produit. Les consommateurs d'assertions peuvent accepter ou rejeter un certificat particulier pour une certaine utilisation sur la base des informations fournies dans ces extensions. Une représentation incorrecte des information dans l'une ou l'autre extension pourrait causer le rejet par le consommateur d'assertions d'un certificat par ailleurs approprié, ou l'acceptation d'un certificat qui devrait être rejeté.

Si plusieurs SSID sont inclus dans un certificat, des informations peuvent alors être obtenues d'un certificat sur les SSID associés à plusieurs WLAN, et non au WLAN auquel on a actuellement accès. L'utilisation prévue des extenxions SSID est d'aider un homologue à déterminer le certificat correct à présenter quand on essaye d'obtenir l'accès à un WLAN. Dans la plupart des situations, y compris EAP-TLS, l'homologue va avoir l'opportunité de valider le certificat fourni par le serveur EAP avant de transmettre un de ses propres certificats au serveur EAP. Alors que l'homologue peut n'être pas sûr que le serveur EAP a accès à la clé privée correspondante jusqu'à un point utltérieur de l'échange de protocole, les informations d'identité dans le certificat de serveur EAP peuvent être utilisées pour déterminer si le certificat de l'homologue devrait ou non être fourni. Quand le même certificat d'homologue est utilisé pour s'authentifier auprès de plusieurs WLAN, la liste des SSID est disponible à partir des serveurs associés à chaque WLAN. Bien sûr, la liste des SSID est aussi rendue disponible à tous ceux qui espionnent sur le WLAN. Chaque fois que cette divulgation de SSID pose problème, des certificats d'homologues différents devraient être utilisés pour chaque WLAN.

Les valeurs de SSID ne sont pas gérées ; donc, les SSID peuvent n'être pas uniques. Il est donc possible que les certificats d'homologues qui sont destinés à être utilisés avec des WLAN differents contiennent le même SSID. Dans ce cas, la sélection automatique de certificat va échouer, et la mise en œuvre DEVRAIT obtenir de l'aide de la part de l'utilisateur pour choisir le certificat correct. Si un utilisateur humain n'est pas disponible, chaque certificat potentiel PEUTêtre essayé jusqu'à ce qu'un réussisse, divulguant la liste des SSID associés à chaque certificat, qui autrement ne seraient pas divulgués. Donc, il est RECOMMANDÉ que l'essai à la suite de chaque certificat ne soit employé que quand le choix par l'utilisateur est indisponible ou impraticable.

En pratique, la divulgation du SSID ne pose pas de problème. Certains experts de la sécurité des WLAN recommandent qu'il soit masqué dans la balise envoyée par les points d'accès (AP, *Access Point*). L'intention est de rendre plus difficile à un attaquant de trouver l'AP correct à cibler. Cependant, d'autres messages de gestion de WLAN comportent le SSID, de sorte que cette pratique force seulement l'attaquant à espionner les messages de gestion de WLAN au lieu de la balise. Donc, placer le SSID dans le certificat n'empire pas les choses.

## 6. Considérations relatives à l'IANA

Les extensions de certificat et les valeurs d'usage de clé étendues sont identifiées par des identifiants d'objets (OID). Les OID utilisés dans le présent document ont été alloués à partir d'un arc délégué par l'IANA. Aucune autre action de l'IANA n'est nécessaire pour le présent document ou ses mises à jour prévisibles.

## 7. Références

### 7.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3281] S. Farrell et R. Housley, "Profil de certificat d'attribut Internet pour l'autorisation", avril 2002. *(Obsolète, voir*

RFC5755)

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[X.509] Recommandation UIT-T X.509: "L'annuaire - cadre d'authentification". 2000.

[X.680] Recommandation UIT-T X.680, "Technologies de l'information - Notation de syntaxe abstraite n° 1", 1997.

[X.690] Recommandation UIT-T X.690, "Technologies de l'information - Règles de codage ASN.1 : spécification des règles de codage de base (BER), règles de codage canoniques (CER) et règles de codage distinctives (DER), 1997.

### 10.2 Références pour information

[802.11] Norme IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[802.1X] Norme IEEE 802.1X, "Port-based Network Access Control", 2001.

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

[RFC2716] B. Aboba, D. Simon, "Protocole d'authentification des TLS d'EAP dans PPP" octobre 1999. (*Obsolète, 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, RFC8044) *(D.S.)*

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

## 8. Module ASN.1

```
WLANCertExtn  { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-
                mod-wlan-extns2005(37) }

ÉTIQUETTES DE DÉFINITIONS IMPLICITES ::= DÉBUT

-- Arcs d'OID

IDENTIFIANT D'OBJET id-pe ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                                1 }

IDENTIFIANT D'OBJET id-kp ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7)
                                3 }

IDENTIFIANT D'OBJET id-aca ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
                                 pkix(7) 10 }

-- Valeurs d'usage de clé étendue

IDENTIFIANT D'OBJET id-kp-eapOverPPP ::=  { id-kp 13 }

IDENTIFIANT D'OBJET id-kp-eapOverLAN ::=  { id-kp 14 }


-- Extension de SSID de LAN sans fil
```

```
IDENTIFIANT D'OBJET id-pe-wlanSSID ::= { id-pe 13 }
SSIDList ::= SEQUENCE TAILLE (1..MAX) DE SSID
SSID  ::= CHAINE D' OCTETS (TAILLE (1..32))


-- Attribut de certificat d'attribut de SSID de LAN sans fil   -- utilise la même syntaxe que l'extension de certificat :
                                                                  SSIDList

IDENTIFIANT D'OBJET id-aca-wlanSSID ::= { id-aca 7 }

FIN
```

## Adresse des auteurs

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
mél : housley@vigilsec.com

Tim Moore
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
mél : timmoore@microsoft.com

## Déclaration de droits de reproduction



**Remerciement**
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien admin,istrzatif de l'IETF (IASA).