Groupe de travail Réseau
Request for Comments : 4282
RFC rendue obsolète : 2486
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft Corporation
M. Beadles, ENDFORCE
J. Arkko, Ericsson
P. Eronen, Nokia
décembre 2005

L'identifiant d'accès réseau (NAI)

Résumé
Pour fournir les services d'itinérance, il est nécessaire d'avoir une méthode normalisée d'identification des utilisateurs. Le présent document définit la syntaxe de l'identifiant d'accès réseau (NAI, *Network Access Identifier*) l'identité d'utilisateur soumise par le client durant l'authentification par le réseau. "Itinérance" peut être défini en gros comme la capacité d'utiliser tout fournisseur d'accès Internet (FAI) tout en conservant une relation formelle de client à fournisseur avec l'un d'entre eux. Des exemples de cas où la capacité d'itinérance peut être nécessaire incluent des "confédérations" de FAI et la prise en charge de l'accès à un réseau d'entreprise fournie par un FAI. Le présent document est une version révisée de la RFC 2486, qui définissait à l'origine les NAI. Les améliorations incluent le jeu de caractères international et la prise en charge de la confidentialité ainsi qu'un certain nombre de corrections à la RFC originale.

Table des Matières

1. Introduction

Il existe un intérêt considérable pour un ensemble de caractéristiques qui entrent dans la catégorie générale de la "capacité d'itinérance" pour l'accès réseau, incluant les utilisateurs qui accèdent à l'Internet par numérotation, l'usage de réseau virtuel privé (VPN, *Virtual Private Network*), l'authentification de LAN sans fil, et d'autres applications. Les parties intéressées ont

incluent ce qui suit :

- Des fournisseurs d'accès Internet (FAI) régionaux fonctionnant au sein d'un état ou province particulier, cherchant à combiner leurs efforts avec ceux d'autres fournisseurs régionaux pour offrir le service commuté sur une plus large zone.
- Des FAI nationaux qui souhaitent combiner leur fonctionnement avec celui d'un ou plusieurs FAI dans d'autres pays pour offrir un service de numérotation plus complet dans un groupe de pays ou sur un continent.
- Des points d'accès de LAN sans fil fournissant le service à un ou plusieurs FAI.
- Des entreprises qui désirent offrir à leur employés un paquetage complet de services de numérotation à l'échelle mondiale. Ces services peuvent inclure l'accès Internet ainsi qu'un accès sûr à des intranets d'entreprise via un VPN, permis par des protocoles de tunnelage tels que le protocole de tunnelage point à point (PPTP, *Point-to-Point Tunneling Protocol*) [RFC2637], le protocole de transmission de couche 2 (L2F, *Layer 2 Forwarding*) [RFC2341], le protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*) [RFC2661], et le mode tunnel IPsec[RFC2401].

Afin d'améliorer l'interopérabilité des services d'itinérance, il est nécessaire d'avoir une méthode normalisée pour identifier les utilisateurs. Le présent document définit la syntaxe de l'identifiant d'accès réseau (NAI, *Network Access Identifier*). Des exemples de mise en œuvre de NAI, et la description de sa sémantique, se trouvent dans la [RFC2194].

Le présent document est une version révisée de la [RFC2486], qui à l'origine définissait les NAI. Les différences et améliorations par rapport à la RFC 2486 sont énumérées à l'Appendice A.

1.1 Terminologie

Le présent document utilise fréquemment les termes suivants :

Identifiant d'accès réseau : c'est l'identité d'utilisateur soumise par le client durant l'authentification d'accès réseau. En itinérance, l'objet du NAI est d'identifier l'utilisateur ainsi que d'aider à l'acheminement de la demande d'authentification. Noter que le NAI n'est pas nécessairement le même que l'adresse de messagerie électronique de l'utilisateur ni que l'identité d'utilisateur soumise dans une authentification de couche application.

Serveur d'accès réseau : (NAS, *Network Access Server*) c'est l'appareil auquel les clients se connectent pour obtenir l'accès au réseau. Dans la terminologie PPTP, c'est ce qu'on appelle le concentrateur d'accès PPTP (PAC, *PPTP Access Concentrator*) et dans la terminologie L2TP, ce qu'on appelle le concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*). Dans IEEE 802.11, on l'appelle un point d'accès.

Capacité d'itinérance : on peut la définir en gros comme la capacité à utiliser tout fournisseur d'accès Internet (FAI) tout en conservant une relation formelle de client à fournisseur avec un seul d'entre eux. Les exemples de cas où la capacité d'itinérance peut être exigée incluent des "confédérations" de FAI et la prise en charge de accès à un réseau d'entreprise par le FAI.

Service de tunnelage : c'est tout service réseau permis par les protocoles de tunnelage tels que PPTP, L2F, L2TP, et IPsec en mode tunnel. Un exemple de service de tunnelage est l'accès sûr aux intranets d'entreprise via un réseau privé virtuel (VPN, *Virtual Private Network*).

1.2 Langage 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].

1.3 Objet

Comme décrit dans la [RFC2194], un certain nombre de fournisseurs offrent des services d'accès réseau, et le nombre des fournisseurs d'accès Internet impliqués dans des consortiums d'itinérance augmente rapidement.

Afin d'être capables d'offrir une capacité d'itinérance, une des exigences est d'être capable d'identifier le serveur d'authentification de rattachement de l'utilisateur. Pour être utilisée dans l'itinérance, cette fonction est réalisée via l'identifiant d'accès réseau (NAI, *Network Access Identifier*) soumis par l'utilisateur au NAS dans l'authentification initiale de réseau. On s'attend aussi à ce que les NAS utilisent le NAI au titre du processus d'ouverture d'un nouveau tunnel, afin de déterminer le point d'extrémité du tunnel.

2. Définition du NAI

2.1 Syntaxe formelle

La grammaire des NAI est donnée ci-dessous, décrite en format Backus-Naur augmenté (ABNF) comme documenté dans la [RFC4234]. La grammaire du nom d'utilisateur se fonde sur la [RFC0821], et la grammaire du domaine est une version mise à jour de la [RFC1035].

```
nai =  nom d'utilisateur
nai =/ "@" domaine
nai =/ nom d'utilisateur "@" domaine

nom d'utilisateur = chaîne séparée par des points
chaîne séparée par des points =  chaîne
chaîne séparée par des points =/ chaîne séparée par des points "." chaîne
chaîne =  caractère
chaîne    =/ chaîne de caractères
caractère  =  c
caractère  =/ "\" x
c =  %x21          ; '!' permis ; '"' interdit
c =/ %x23          ; '#' permis
c =/ %x24          ; '$' permis
c =/ %x25          ; '%' permis
c =/ %x26          ; '&' permis
c =/ %x27          ; '''  permis, '(', ')' interdit
c =/ %x2A          ; '*' permis
c =/ %x2B          ; '+' permis, ','  interdit
c =/ %x2D          ; '-' permis, '.'  interdit
c =/ %x2F          ; '/' permis
c =/ %x30-39       ; '0'-'9' permis, ';', ':', '<' interdit
c =/ %x3D          ; '=' permis, '>'  interdit
c =/ %x3F          ; '?' permis, '@' interdit
c =/ %x41-5a       ; 'A'-'Z' permis, '[', '\', ']' interdit
c =/ %x5E          ; '^' permis
c =/ %x5F          ; '_' permis
c =/ %x60          ; '`' permis
c =/ %x61-7A       ; 'a'-'z' permis
c =/ %x7B          ; '{' permis
c =/ %x7C          ; '|' permis
c =/ %x7D          ; '}' permis
c =/ %x7E          ; '~' permis, DEL interdit
c =/ %x80-FF       ; UTF-8-Octet  permis (pas dans la RFC 2486) ; où UTF-8-octet est tout octet dans la représentation UTF-8 ;
                     multi octets d'un codet unicode au dessus de %x7F. Noter que c doit aussi satisfaire aux règles du paragraphe
                     2.4, incluant, par exemple, de vérifier qu'aucun résultat interdit n'est utilisé (voir aussi le paragraphe 2.3 de la
                     [RFC4013]).
x =  %x00-FF       ; tous les 128 caractères ASCII, sans exception, ainsi que tous les octets UTF-8 comme défini ci-dessus (ce qui
                     était interdit dans la RFC 2486). Noter que x doit néanmoins satisfaire aussi aux règles du paragraphe 2.4.
domaine =  1*( étiquette "." ) étiquette
étiquette  =  lettre-chiffre *(ldh-str)
ldh-str=  *( alpha / chiffre / "-" ) lettre-chiffre
lettre-chiffre  =  alpha / chiffre
alpha  =  %x41-5A      ; 'A'-'Z'
alpha   =/ %x61-7A     ; 'a'-'z'
chiffre  =  %x30-39    ; '0'-'9'
```

2.2 Considérations sur la longueur des NAI

Les appareils qui traitent les NAI DOIVENT prendre en charge une longueur de NAI d'au moins 72 octets. La prise en charge d'une longueur de NAI de 253 octets est RECOMMANDÉE. Cependant, les questions de mise en œuvre suivantes devraient être prises en considération :

o Les NAI sont souvent transportés dans l'attribut Nom d'utilisateur du protocole du service d'authentification distante

d'utilisateur appelant (RADIUS, *Remote Authentification Dial-In User Service*). Malheureusement, le paragraphe 5.1 de la [RFC2865] déclare que "la capacité de traiter au moins 63 octets est recommandée". Par suite, il peut être impossible de transférer des NAI de plus de 63 octets à travers tous les appareils. De plus, comme un seul attribut Nom d'utilisateur peut être inclus dans un message RADIUS et que la longueur maximum d'un attribut est de 253 octets, RADIUS est incapable de prendre en charge des longueurs de NAI au delà de 253 octets.

- Les NAI peuvent aussi être transportés dans l'attribut Nom d'utilisateur de Diameter [RFC3588], qui prend en charge des longueurs de contenu jusqu'à 2^24 - 9 octets. Par suite, les NAI traités seulement par des nœuds Diameter peuvent être très longs. Malheureusement, un NAI transporté sur Diameter peut finalement être traduit en RADIUS, et dans ce cas les limitations ci-dessus s'appliquent.

2.3 Prise en charge de la confidentialité du nom d'utilisateur

L'interprétation de la partie Nom d'utilisateur du NAI dépend du domaine en question. Donc, la partie "nom d'utilisateur" DEVRAIT être traitée comme données opaques lors du traitement pas des nœuds qui ne font pas partie du domaine d'autorité (au sens de la Section 4) pour ce domaine.

Dans certaines situations, les NAI sont utilisés avec une méthode d'authentification distincte qui peut transférer la partie Nom d'utilisateur d'une façon plus sûre pour améliorer la confidentialité. Dans ce cas, les NAI PEUVENT être fournis sous une forme abrégée en omettant la partie Nom d'utilisateur. Omettre la partie Nom d'utilisateur est RECOMMANDÉ plutôt que d'utiliser une partie Nom d'utilisateur fixe, comme "anonymous", car cela donne une façon non ambiguë de déterminer si le nom d'utilisateur est destiné à identifier de façon univoque un seul utilisateur.

Pour les besoins de l'itinérance, il est normalement nécessaire de localiser le serveur d'authentification d'extrémité arrière approprié pour le NAI en question avant que la conversation d'authentification puisse avoir lieu. Par suite, la portion domaine est normalement exigée afin que l'échange d'authentification soit acheminé au serveur approprié.

2.4 Jeux de caractères internationaux

La présente spécification permet les noms d'utilisateur et les domaines internationaux. Les noms d'utilisateur internationaux sont fondés sur l'utilisation de caractères Unicode, codés comme UTF-8 et traités avec un certain algorithme pour assurer une représentation canonique. L'internationalisation de la portion Domaine du NAI se fonde sur l'internationalisation des noms de domaines dans les applications (IDNA) [RFC3490].

Pour assurer une représentation canonique, les caractères de la portion Nom d'utilisateur d'un NAI DOIVENT satisfaire à l'ABNF de la présente spécification ainsi qu'aux exigences spécifiées dans la [RFC4013]. Ces exigences consistent en ce qui suit :

- Exigences de transposition, comme spécifiées au paragraphe 2.1 de la [RFC4013]. La transposition consiste à transposer certains caractères en d'autres (comme ESPACE) afin d'augmenter la probabilité d'effectuer correctement les comparaisons.
- Les exigences de normalisation, comme spécifiées au paragraphe 2.2 de la [RFC4013], sont aussi conçues pour aider aux comparaisons.
- Résultats interdits. Certains caractères ne sont pas permis dans les chaînes correctement formées qui suivent le paragraphe 2.3 de la [RFC4013]. S'assurer que les NAI se conforment à leur ABNF n'est pas suffisant ; il est aussi nécessaire de s'assurer qu'il ne contiennent pas de résultat prohibé.
- Les caractères bidirectionnels sont traités comme spécifié au paragraphe 2.4 de la [RFC4013].
- Les codets non alloués sont spécifiés au paragraphe 2.5 de la [RFC4013]. L'utilisation de codets non alloués est interdite.

Le traitement de la transposition, de la normalisation, et des caractères bidirectionnels DOIT être effectué par les systèmes d'extrémité qui prennent du texte international comme entrée. Dans un réglage d'accès réseau, de tels systèmes sont normalement le client et les serveurs d'authentification autorisation et comptabilité (AAA, *Authentication, Authorization, and Accounting*). Les NAI sont envoyés sur le réseau dans leur forme canonique, et les tâches telles que la normalisation n'ont normalement pas besoin d'être effectuées par les nœuds qui passent juste les NAI ou les reçoivent du réseau. Les systèmes d'extrémité DOIVENT aussi effectuer la vérification des résultats prohibés et des codets non alloués. D'autres systèmes PEUVENT effectuer des vérifications, lorsque ils savent qu'un élément de données particulier est un NAI.

Le nom de domaine est un "créneau de nom de domaine qui ignore l'IDN" comme défini dans la [RFC3490]. C'est-à-dire qu'il ne peut contenir que des caractères ASCII. Une mise en œuvre PEUT prendre en charge les noms de domaines internationalisés (IDN, *Internationalized Domain Name*) en utilisant l'opération ToASCII ; voir plus d'informations dans la [RFC3490].

La responsabilité de la conversion des noms de domaines internationalisés en ASCII revient aux systèmes d'extrémité, tels que les clients d'accès réseau et les serveurs AAA. De même, on s'attend à ce que les comparaisons de noms de domaines, les confrontations, la résolution, et l'acheminement AAA soient effectués sur les versions ASCII des noms de domaines internationalisés. Cela donne une représentation canonique, assure que les systèmes intermédiaires comme les mandataires AAA n'ont pas besoin d'effectuer les traductions, et on peut espérer que cela fonctionne avec des systèmes qui ignorent les jeux de caractères internationaux.

2.5 Compatibilité avec les noms d'utilisateur de la messagerie électronique

Comme proposé dans le présent document, l'identifiant d'accès réseau est de la forme usager@domaine. Noter que, alors que la portion utilisateur du NAI se fonde sur le BNF décrit dans la [RFC0821], il a été étendu pour la prise en charge de l'internationalisation ainsi que pour les objectifs du paragraphe 2.7, et n'est pas nécessairement compatible avec les noms d'utilisateur de la messagerie électronique.
Noter aussi que les exigences d'internationalisation sont différentes pour les NAI et les adresses de messagerie électronique, car les premières doivent être entrées par l'utilisateur lui-même et son propre opérateur, et non par d'autres.

2.6. Compatibilité avec le DNS

Le BNF de la portion domaine lui permet de commencer par un chiffre, ce qui n'est pas permis par le BNF décrit dans la [RFC1035]. Ce changement a été fait pour refléter les pratiques courantes; bien que non permis par le BNF décrit dans la [RFC1035]. Les noms de domaines pleinement qualifiés (FQDN, *Fully Qualified Domain Names*) tels que 3com.com sont couramment utilisés et acceptés par le logiciel actuel.

2.7 Construction de domaine

Les NAI sont utilisés, entre autres choses, pour acheminer les transactions AAA au domaine de rattachement de l'utilisateur. Généralement, le domaine de rattachement apparaît dans la portion Domaine du NAI, mais dans certains cas, un domaine différent peut être utilisé. Cela peut être utile, par exemple, lorsque le domaine de rattachement n'est accessible que via un autre domaine intermédiaire.

Un tel usage peut empêcher l'interopérabilité sauf si les parties impliquées ont un accord mutuel permettant cet usage. En particulier, les NAI NE DOIVENT PAS utiliser un domaine différent du domaine de rattachement sauf si l'envoyeur a la connaissance explicite que (a) l'autre domaine spécifié est disponible et (b) que l'autre domaine prend en charge un tel usage. L'envoyeur peut déterminer l'accomplissement de ces conditions par une base de données, la découverte dynamique, ou d'autres moyens non spécifiés ici. Noter que la première condition est affectée par l'itinérance, car la disponibilité de l'autre domaine peut dépendre de la localisation de l'usager ou de l'application désirée.

L'utilisation du domaine de rattachement DOIT être par défaut sauf autre configuration.

Si ces conditions sont remplies, un NAI tel que "usager@domainederattachement.exemple.net" PEUT être représenté comme "domainederattachement.exemple.net!usager@autredomaine.exemple.net".

Dans ce cas, la partie avant le '!' (non échappé) DOIT être un nom de domaine comme défini dans l'ABNF du paragraphe 2.1. Ce nom de domaine est un "créneau de nom de domaine qui ignore l'IDN", tout comme le nom de domaine après le caractère "@" ; voir les détails au paragraphe 2.4. À la réception d'un tel NAI, l'autre domaine DOIT reconvertir le format en "usager@domainederattachement.exemple.net" lorsque il transmet le NAI, ainsi qu'appliquer l'acheminement AAA approprié pour la transaction.

Le processus de conversion peut aussi s'appliquer de façon récurrente. C'est-à-dire, après la conversion, le résultat peut encore avoir un ou plusieurs caractères '!' dans le nom d'utilisateur. Par exemple, le NAI "autre2.exemple.net! rattachement.exemple.net!usager@autre1.exemple.net" serait d'abord converti en autre1.exemple.net à "rattachement.exemple.net!usager@autre2.exemple.net" et ensuite en autre2.exemple.net et finalement en "usager@domainederattachement.exemple.net".

Noter que la syntaxe décrite dans ce paragraphe est facultative et ne fait pas partie de l'ABNF. Le caractère '!' peut aussi apparaître dans la portion Nom d'utilisateur d'un NAI pour d'autres raisons, et dans ce cas, les règles mentionnées ici ne s'appliquent pas ; l'interprétation du nom d'utilisateur dépend d'un accord entre l'usager identifié et le domaine donné après le caractère '@'.

2.8 Exemples

Des exemples d'identifiants d'accès réseau valides incluent les suivants :
bob
joe@exemple.com
fred@foo-9.exemple.com
jack@3rd.depts.exemple.com
fred.smith@exemple.com
fred_smith@exemple.com
fred$@exemple.com
fred=?#$&*+-/^smith@exemple.com
nancy@eng.exemple.net
eng.exemple.net!nancy@exemple.net
eng%nancy@exemple.net
@privatecorp.exemple.net
\(user\)@exemple.net
alice@xn--tmonesimerkki-bfbb.exemple.net

Le dernier exemple utilise un IDN converti en représentation ASCII.

Des exemples d'identifiants d'accès réseau invalides incluent les suivants :
fred@exemple
fred@exemple_9.com
fred@exemple.net@exemple.net
fred.@exemple.net
eng:nancy@exemple.net
eng;nancy@exemple.net
(user)@exemple.net
<nancy>@exemple.net

3. Considérations sur la sécurité

Comme un NAI révèle l'affiliation de rattachement d'un utilisateur, il peut aider un attaquant à sonder plus profondément l'espace de nom d'utilisateur. Normalement, ce problème est surtout posé dans les protocoles qui transmettent le nom d'utilisateur en clair à travers l'Internet, comme dans RADIUS, décrit dans les [RFC2865] et [RFC2866]. Afin d'empêcher l'espionnage du nom d'utilisateur, les protocoles peuvent utiliser les services de confidentialité fournis par les protocoles qui les transportent, comme RADIUS protégé par IPsec [RFC3579] ou Diameter protégé par TLS [RFC3588].

La présente spécification ajoute la possibilité de lier la partie Nom d'utilisateur du NAI, en l'omettant. Comme discuté au paragraphe 2.3, ceci n'est possible que lorsque les NAI sont utilisés avec une méthode d'authentification séparée qui peut transférer le nom d'utilisateur d'une manière sûre. Dans certains cas, un mécanisme de confidentialité spécifique de l'application a aussi été utilisé avec les NAI. Par exemple, certaines méthodes de protocole d'authentification extensible (EAP, *Extensible Authentification Protocol*) appliquent des pseudonymes spécifiques de la méthode dans la partie Nom d'utilisateur du NAI [RFC3748]. Bien qu'aucune de ces approches ne puisse protéger la partie Domaine, leur avantage sur la protection du transport est que la confidentialité du nom d'utilisateur est protégée, même à travers les nœuds intermédiaires comme les NAS.

4. Considérations relatives à l'IANA

Afin d'éviter de créer de nouvelles procédures administratives, l'administration de l'espace de noms de domaine de NAI est portée par l'administration de l'espace de noms du DNS.

Les noms de domaine de NAI sont obligatoirement univoques, et le droit d'utiliser un certain domaine de NAI pour les besoins de l'itinérance est obtenu concurremment avec l'acquisition du droit d'utiliser un nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) particulier. Ceux qui souhaitent utiliser un nom de domaine de NAI devraient d'abord acquérir le droit d'utiliser le FQDN correspondant. L'utilisation d'un domaine de NAI sans posséder le FQDN correspondant crée la possibilité d'un conflit et est donc déconseillée.

Noter que l'utilisation d'un FQDN comme nom de domaine n'exige pas l'utilisation du DNS pour la localisation du serveur d'authentification. Tandis que Diameter [RFC3588] prend en charge l'utilisation du DNS pour la localisation des serveurs

d'authentification, les mises en œuvre existantes de RADIUS utilisent normalement des fichiers de configuration de mandataire afin de localiser les serveurs d'authentification au sein d'un domaine et utilisent l'acheminement de l'authentification. Les mises en œuvre décrites dans la [RFC2194] n'utilisaient pas le DNS pour localiser le serveur d'authentification au sein d'un domaine. De même, les mises en œuvre existantes n'ont pas éprouvé le besoin d'avoir des protocoles d'acheminement dynamique ou la propagation d'informations d'acheminement mondiales. Noter aussi qu'il n'est pas exigé que le NAI représente une adresse de messagerie électronique valide.

5. Références

5.1 Références normatives

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

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

[RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les* RFC5890 et 5891, *P.S.*)

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

[RFC4234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", octobre 2005. *(Remplace* RFC2234, remplacée par RFC5234)

5.2 Références pour information

[RFC0821] J. Postel, "Protocole simple de transfert de messagerie", STD 10, août 1982.

[RFC2194] B. Aboba, J. Lu, J. Alsop, J. Ding, W. Wang, "Récapitulation des mises en œuvre d'itinérance", septembre 1997. *(Info.)*

[RFC2341] A. Valencia, M. Littlewood, T. Kolar, "Protocole de transmission de couche 2 "L2F" de Cisco", mai 1998. *(Historique)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

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

[RFC2637] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little et G. Zorn, "Protocole de tunnelage point à point (PPTP)", juillet 1999.

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

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

[RFC2866] C. Rigney, "Comptabilité RADIUS", juin 2000. (*MàJ par* RFC2867, RFC5080) *(Information)*

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par* RFC5080) *(Information)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

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

[RFC5113] J. Arkko et autres, "Problème de la découvert et du choix d'un réseau", janvier 2008. *(Information)*

Appendice A. Changements depuis la RFC 2486

Le présent document contient les mises à jour suivantes par rapport à la définition originale de NAI de la [RFC2486] :

- La prise en charge de jeux de caractères internationaux a été ajoutée à la fois pour les noms d'utilisateurs et ceux de domaines. Noter que cela implique que des codes de caractères de 128 à 255 peuvent être utilisés dans la portion nom d'utilisateur, qui peuvent être inacceptables pour les nœuds qui ne prennent en charge que la RFC 2486. De nombreux appareils permettent cependant déjà ce comportement.

- La prise en charge de la cobnfidentialité du nom d'utilisateur a été ajoutée. Noter que les NAI sans nom d'utilisateur (à cause de la confidentialité) peuvent n'être pas acceptables pour les nœuds conformes à la RFC2486. De nombreux appareils permettent cependant déjà ce comportement.

- On a ajouté la recommandation de prise en charge de longueurs de NAI d'au moins 253 octets, et des considérations de compatibilité entre les longueurs de NAI dans la présente spécification et dans divers protocoles AAA sont exposées. Noter que les longs NAI peuvent n'être pas acceptables pour les nœuds conformes à la RFC2486.

- La syntaxe du réseau support et ses implications ont été pleinement décrites et non plus données seulement comme exemple. Noter que cette syntaxe nn'est pas destinée à être une solution complète de la découverte de réseau et des besoins de choix comme définis dans la [RFC5113]. Elle est plutôt destinée à une clarification de la RFC 2486. Cependant, comme exposé au paragraphe 2.7, la présente spécification exige que cette syntaxe ne s'applique que lorsque il y a une connaissance explicite que le système homologue prend en charge cette syntaxe.

- La définition d'entrée de BNF de BNF a été changée pour éviter une erreur (récurrence infinie) dans la spécification d'origine.

- Plusieurs éclaircissements et améliorations ont été incorporés dans la spécification de l'ABNF pour les NAI.

Appendice B. Remerciements

Merci à Glen Zorn pour les nombreuses discussions utiles sur cet espace de problème, et à Farid Adrangi pour sa suggestion de la représentation des réseaux supports dans les NAI. Jonathan Rosenberg a rapporté des erreurs de BNF. Dale Worley a suggéré des éclaircissements sur les entrées de BNF x et spéciales. Arne Norefors a rapporté les différences de longueur entre les RFC 2486 et RFC 2865. Paul Hoffman a donné son aide sur les questions de jeu de caractères international. Kalle Tammela, Stefaan De Cnodder, Nagi Jonnala, Bert Wijnen, Blair Bullock, Yoshihiro Ohba, Ignacio Goyret, John Loughney, Henrik Levkowetz, Ted Hardie, Bill Fenner, Sam Hartman, et Richard Perlman ont fourni de nombreux commentaires utiles sur le présent document. Le valideur d'ABNF à http://www.apps.ietf.org/abnf.html a été utilisé pour vérifier la correction syntaxique de l'ABNF du paragraphe 2.1.

Adresse des auteurs

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA
bernarda@microsoft.com

Mark A. Beadles
ENDFORCE
565 Metro Place South Suite 300
Dublin OH 43017
USA
mbeadles@endforce.com

Jari Arkko
Ericsson
Jorvas 02420
Finland
jari.arkko@ericsson.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland
pasi.eronen@nokia.com

Déclaration complète de droits de reproduction

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