Équipe d'ingénierie de l'Internet (IETF)
**Request for Comments : 7542**
RFC rendue obsolète : 4282
Catégorie : En cours de normalisation
ISSN : 2070-1721

A. DeKok, FreeRADIUS
mai 2015

Traduction Claude Brière de L'Isle

# Identifiant d'accès réseau

**Résumé**
Pour fournir des services d'authentification inter domaines, il est nécessaire d'avoir une méthode normalisée que puissent utiliser les domaines pour identifier leurs utilisateurs respectifs. Le présent document définit la syntaxe de l'identifiant d'accès réseau (NAI, *Network Access Identifier*) l'identifiant d'utilisateur soumis par le client avant d'accéder aux ressources. Le présent document est une version révisée de la RFC 4282. Il traite des questions en relation avec les jeux de caractères internationaux et apporte un certain nombre d'autres corrections à la RFC 4282.



**Statut de ce mémoire**
Ceci est un document de l'Internet en cours de normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la [RFC5741].

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc7542



## Table des Matières

1. Introduction....2
1.1 Terminologie....3
1.2 Langage des exigences....4
1.3 Objet....4
1.4 Motivation....4
2. Définition du NAI....5
2.1 Syntaxe et normalisation UTF-8....5
2.2 Syntaxe formelle....5
2.3 Considérations sur la longueur du NAI....6
2.4 Prise en charge de la confidentialité du nom d'utilisateur....6
2.5 Jeux de caractères internationaux....7
2.6 Processus de normalisation....7
2.7 Utilisation dans d'autres protocoles....8
2.8 Utilisation du format de NAI pour d'autres identifiants....9
3. Acheminement à l'intérieur des systèmes AAA....9
3.1 Compatibilité avec les noms d'utilisateur de la messagerie électronique....10

3.2 Compatibilité avec le DNS....10
3.3 Construction de domaine....11
3.4 Exemples....12
4. Considérations pour la sécurité....12
4.1 Corrélation des identités dans le temps et à travers les protocoles....13
4.2 Identifiants multiples....13
5. Administration des noms....13
6. Références....14
6.1. Références normatives....14
6.2. Références pour information....14
Appendice A. Changements par rapport à la RFC4282....15

## 1. Introduction

Il existe un intérêt considérable pour un ensemble de caractéristiques qui entrent dans la catégorie générale de l'authentification inter domaines, ou "capacité d'itinérance" pour l'accès au réseau, incluant les utilisateurs qui accèdent à l'Internet par la numérotation, l'usage des réseaux privés virtuels (VPN, *Virtual Private Network*), l'authentification de LAN sans fil, et d'autres applications.

Par "authentification inter domaines", le présent document se réfère à des situations où un usager a des accréditifs d'authentification à un domaine "de rattachement" mais est capable de les présenter à un second domaine "visité" pour accéder à certains services dans le domaine visité. Les deux domaines ont généralement une relation préexistante, de sorte que les accréditifs peuvent être passés du domaine visité au domaine de rattachement pour vérification. Le domaine de rattachement répond normalement par une permission/refus, qui peut aussi inclure des paramètres d'autorisation que le domaine visité est supposé appliquer à l'utilisateur.

C'est-à-dire que le scénario "itinérance" implique un usager qui visite, ou "en itinérance" dans un domaine de non rattachement et qui demande l'utilisation de services dans ce domaine visité.

Les parties intéressées pourraient être les suivantes :
* Les fournisseurs d'accès Internet (FAI) régionaux qui opèrent dans un pays ou région particulier, cherchant à combiner leurs efforts avec ceux des autres fournisseurs régionaux pour offrir un service commuté sur une zone plus large.
* Les compagnies de télécommunications qui souhaitent combiner leurs opérations avec celles d'une ou plusieurs compagnies dans d'autres zones ou pays, afin d'offrir un service d'accès réseau plus complet dans des zones où il n'y a pas de service (par exemple, dans un autre pays).
* Des points chauds de LAN sans fil fournissant le service à un ou plusieurs FAI.
* Des sociétés souhaitant offrir à leurs employés un paquetage complet de services commutés sur une base mondiale. Ces services peuvent inclure l'accès Internet aussi bien qu'un accès sûr à des intranets d'entreprise via un VPN, activés par des protocoles de tunnelage tels que le protocole de tunnelage de point à point (PPTP, *Point-to-Point Tunneling Protocol*) [RFC2637], le protocole de transmission de couche 2 (L2F, *Layer 2 Forwarding protocol*) [RFC2341], le protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*) [RFC2661], et le mode tunnel IPsec [RFC4301].
* D'autres protocoles qui sont intéressés à développer les accréditifs d'utilisateurs afin de tirer parti d'un cadre d'authentification existant.

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

Lorsque le NAI a été défini pour l'accès réseau, il avait pour effet collatéral de définir un identifiant qui pouvait être utilisé dans des systèmes non AAA. Certains systèmes non AAA définissaient des identifiants qui étaient compatibles avec le NAI, et les développements utilisaient le NAI. Ce traitement a simplifié la gestion des accréditifs, en réutilisant le même accréditif dans plusieurs situations. Les protocoles qui réutilisent le même accréditif ou le même format d'identifiant peuvent bénéficier de cette gestion simplifiée. La solution de remplacement est d'avoir des formats d'accréditifs ou d'identifiant spécifiques du protocole, ce qui augmente les coûts aussi bien de l'usager que de l'administrateur.

Il y a des implications sur la confidentialité à utiliser un seul identifiant sur plusieurs protocoles. Voir les paragraphe 2.7 et la Section 4 pour plus d'informations sur ce sujet.

Les objectifs du présent document sont de définir le format d'un identifiant qui peut être utilisé dans de nombreux protocoles. Un protocole peut transporter une version codée du NAI (par exemple, '.' comme %2E). Cependant, la définition du NAI est indépendante du protocole. Le but de ce document est d'encourager l'adoption la plus large du format de NAI. Cette adoption

diminuera le travail requis pour améliorer l'identification et l'authentification dans les autres protocoles. Cela va aussi diminuer la complexité de systèmes non AAA pour les utilisateurs finaux et les administrateurs.

Le présent document suggère seulement que le format de NAI soit utilisé ; il n'exige pas un tel usage. De nombreux protocoles définissent déjà leur propre format d'identifiants. Certains d'entre eux sont incompatibles avec le NAI, tandis que d'autres permettent le NAI en plus d'identifiants non NAI. La définition du NAI dans le présent document ne fait peser aucune exigence sur les spécifications de protocoles, de mises en œuvre, ou de déploiements.

Cependant le présent document suggère qu'utiliser un seul format standard d'identifiant est préférable à l'utilisation de multiples formats d'identifiants incompatibles. Lorsque des identifiants doivent être utilisés dans de nouveaux protocoles et/ou spécifications, il est RECOMMANDÉ que le format de NAI soit utilisé. C'est-à-dire que l'interprétation de l'identifiant est spécifique du contexte, tandis que le format de l'identifiant reste le même. Ces questions sont discutées plus en détail au paragraphe 2.8.

La recommandation d'un format d'identifiant standard n'est pas une recommandation que chaque utilisateur ait un seul identifiant universel. Bien au contraire, le présent document permet l'utilisation d'identifiants multiples et recommande l'utilisation d'identifiants anonymes lorsque ces identifiants sont publiquement visibles.

Le présent document est une version révisée de la [RFC4282], qui définissait à l'origine les NAI internationalisés. Les différences et améliorations par rapport à ce document sont énumérées à l'Appendice A.

### 1.1 Terminologie

Le présent document utilise fréquemment les termes suivants :

Texte "local" ou "localisé" : c'est un texte qui est en forme soit non UTF-8, soit non normalisée. Le jeu de caractères, le codage, et les particularismes sont (en général) inconnus pour les protocoles réseau d'authentification, d'autorisation et de comptabilité (AAA, *Authentication, Authorization, and Accounting*). Le client qui "connaît" les particularités locales peut avoir de ce texte un concept différent que les autres entités AAA, qui ne connaissent pas les mêmes particularités locales.

Identifiant d'accès réseau : le NAI, *(Network Access Identifier)* est un format commun des identifiants d'usagers soumis par un client durant l'authentification. L'objet du NAI est de permettre à un usager d'être associé à un nom de compte, ainsi qu'à aider à l'acheminement de la demande d'authentification à travers plusieurs domaines. Noter que le NAI peut n'être pas nécessairement le même que l'adresse de messagerie électronique de l'usager ou que l'identifiant d'usager soumis dans une authentification de couche application.

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

Capacité d'itinérance : elle peut être définie en gros comme la capacité à utiliser un des multiples fournisseurs d'accès Internet (FAI) tout en conservant une relation formelle de client à fournisseur avec un seul d'entre eux. Des exemples de cas où la capacité d'itinérance peut être requise incluent des "confédérations" de FAI et la prise en charge d'accès réseau d'entreprise fournie par FAI.

Normalisation ou canonisation : ces termes sont définis à la Section 4 de la [RFC6365] ; ces définitions sont incorporées ici par référence.

Particularités locales : ce terme est défini dans la [RFC6365], Section 8 ; cette définition est incorporée ici par référence.

Service de tunnelage : Un service de tunnelage est tout service réseau activé par des protocoles de tunnelage tels que PPTP, L2F, L2TP, et le mode tunnel IPsec. 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", "RECOMMANDÉ", "NON RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

### 1.3 Objet

Comme décrit dans la [RFC2194], il y a un certain nombre de fournisseurs qui offrent des services d'accès réseau, et l'essentiel des fournisseurs d'accès Internet sont impliqués dans des consortiums d'itinérance.

Pour être capable d'offrir une capacité d'itinérance, une des exigences est d'être capable d'identifier le serveur d'authentification de rattachement de l'usager. Pour être utilisée dans l'itinérance, cette fonction est accomplie via l'identifiant d'accès réseau (NAI) soumis par l'usager 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.

Le présent document suggère que d'autres protocoles puissent tirer parti du format de NAI. De nombreux protocoles comportent des capacités d'authentification, incluant de définir leur propre format d'identifiants. Ces identifiants peuvent alors finir par être transportés dans des protocoles AAA, de sorte que les protocoles d'origine puissent s'appuyer sur AAA pour l'authentification de l'usager. Il y a donc un besoin de définition d'un identifiant d'usager qui puisse être utilisé dans plusieurs protocoles.

Bien qu'on définisse ici le NAI, on notera que les protocoles et déploiements existants ne l'utilisent pas toujours. Les systèmes AAA DOIVENT donc être capables de traiter les identifiants d'usager qui ne sont pas au format de NAI. Le processus par lequel cela est fait sort du domaine d'application du présent document.

Les systèmes non AAA peuvent accepter des identifiants d'usager sous d'autres formes que le NAI. La présente spécification n'interdit pas cette pratique. Elle codifie seulement le format et l'interprétation du NAI. Le présent document ne peut pas changer les protocoles ou pratiques existants. Il peut, cependant, suggérer que l'utilisation d'une forme cohérente pour un identifiant d'usager est tout bénéfice pour la communauté.

Le présent document ne donne aucune définition spécifique d'un protocole pour un format d'identifiant, et ne fait aucun changement à un protocole existant. Il définit plutôt pour le NAI une forme indépendante des protocoles. On espère que le NAI est un identifiant d'usager qui peut être utilisé dans de multiples protocoles.

Utiliser un format d'identifiant commun simplifie les protocoles qui requièrent l'authentification, car ils n'ont plus besoin de spécifier un format spécifique du protocole pour les identifiants d'usagers. Cela augmente la sécurité, car des formats d'identifiants multiples permettent aux attaquants de faire des revendications contradictoires sans être détectés (voir au paragraphe 4.2 plus d'éléments sur ce sujet). Cela simplifie les déploiements, car un usager peut avoir un identifiant dans plusieurs contextes, ce qui lui permet d'être identifié de façon univoque, tant que cet identifiant est lui-même protégé contre les accès non autorisés.

En bref, avoir un standard est mieux que de ne pas en avoir.

### 1.4 Motivation

La liste détaillée des changements par rapport à la [RFC4282] figure à l'Appendice A. Cependant, quelques éléments supplémentaires sont appropriés pour motiver ces changements.

Le motif de la révision de la [RFC4282] commence avec les problèmes d'internationalisation soulevés dans le contexte de [EDUROAM]. Le paragraphe 2.1 de la [RFC4282] définit l'ABNF pour les domaines et limite la grammaire des domaines aux lettres de l'anglais, aux chiffres et au caractère trait d'union "-". L'intention paraît avoir été de coder, comparer, et transporter les domaines avec la forme de codage Punycode [RFC3492] comme décrit dans la [RFC5891]. Cette approche pose un certain nombre de problèmes :

* l'ABNF [RFC4282] n'est pas en ligne avec l'internationalisation du DNS ;
* l'exigence du paragraphe 2.1 de la [RFC4282] que les domaines soient en ASCII est en conflit avec le protocole d'authentification extensible (EAP) défini dans la [RFC3748], et avec RADIUS, qui sont tous deux en 8 bits, et qui tous deux recommandent l'utilisation de l'UTF-8 pour les identifiants ;
* le paragraphe 2.4 de la [RFC4282] exige des transpositions qui sont spécifiques de la langue et sont presque impossibles à effectuer correctement par les nœuds intermédiaires sans informations sur le langage ;

* le paragraphe 2.4 de la [RFC4282] demande la normalisation des noms d'utilisateur, qui peut entrer en conflit avec les exigences du système local ou administratif ;
* les recommandations du paragraphe 2.4 de la [RFC4282] pour le traitement de caractères bidirectionnels se sont révélées irréalisables ;
* l'interdiction de l'utilisation des codets non alloués du paragraphe 2.4 de la [RFC4282] interdit effectivement la prise en charge de nouveaux scénarios ;
* aucun client, mandataire, ou serveur d'authentification, autorisation, et comptabilité (AAA) n'a mis en œuvre les exigences du paragraphe 2.4 de la [RFC4282], entre autres.

Avec la croissance de la popularité de l'itinérance internationale, il est important que ces questions soient corrigées afin de fournir des services réseau robustes et interopérables.

De plus, le présent document a été motivé par le désir de codifier les pratiques existantes en matière d'utilisation du format de NAI et d'encourager une large utilisation de ce format.

## 2. Définition du NAI

### 2.1 Syntaxe et normalisation UTF-8

Les caractères UTF-8 peuvent être définis en termes d'octets en utilisant l'ABNF [RFC5234] suivant, tiré de la [RFC3629] :

UTF8-xtra-char = UTF8-2 / UTF8-3 / UTF8-4

UTF8-2 = %xC2-DF UTF8-tail

UTF8-3 = %xE0 %xA0-BF UTF8-tail / %xE1-EC 2( UTF8-tail ) / %xED %x80-9F UTF8-tail / %xEE-EF 2( UTF8-tail )

UTF8-4 = %xF0 %x90-BF 2( UTF8-tail ) / %xF1-F3 3( UTF8-tail ) / %xF4 %x80-8F 2( UTF8-tail )

UTF8-tail = %x80-BF

Ceci est défini normativement dans la [RFC3629] mais est répété dans ce document pour des raisons pratiques.

Voir la [RFC5198] et le paragraphe 2.6 de la présente spécification sur la discussion de la normalisation. Les chaînes qui ne sont pas en forme composée normale (NFC, *Normal Form Composed*) ne sont pas des NAI valides et NE DEVRAIENT PAS être traitées comme telles. Les mises en œuvre qui s'attendent à recevoir un NAI mais reçoivent à la place des chaînes UTF-8 non normalisées (mais par ailleurs valides) DEVRAIENT tenter de créer une version locale du NAI, qui soit normalisée à partir de l'identifiant d'entrée. Cette version locale peut alors être utilisée pour le traitement local. Cette version locale de l'identifiant NE DOIT PAS être utilisée en dehors du contexte local.

Lorsque les protocoles portent des identifiants dont on s'attend à ce qu'ils soient transportés sur un protocole AAA, il est RECOMMANDÉ que les identifiants soient en format NAI. Lorsque les identifiants ne sont pas dans le format de NAI, il appartient aux systèmes AAA de le découvrir et de les traiter. Le présent document ne suggère pas comment cela est fait. Cependant, les pratiques existantes indiquent que c'est possible.

Comme les noms de domaine internationalisés deviennent plus largement utilisés, les pratiques existantes vont vraisemblablement devenir inadéquates. Le présent document définit donc le NAI, qui est un format d'identifiant d'utilisateur qui peut correctement s'accommoder d'identifiants internationalisés.

### 2.2 Syntaxe formelle

La grammaire pour le NAI est donnée ci-dessous, décrite en format Backus-Naur augmenté (ABNF) comme documenté dans la [RFC5234].

```
nai                             = nom-d'utilisateur-utf8
nai                             =/ "@" domaine-utf8
nai                             =/ nom-d'utilisateur-utf8 "@" domaine-utf8
nom-d'utilisateur-utf8          = chaîne-séparée par des points
chaîne-séparée par des points   = chaîne *("."chaîne)
```

```
chaîne                    = 1*utf8-atext
utf8-atext =  ALPHA / DIGIT / "!" / "#" / "$" / "%" / "&" / "'" / "*" / "+" / "-" / "/" / "=" / "?" / "^" / "_" / "`" / "{" / "|" / "}" / "~"
              / UTF8-xtra-char
domaine-utf8   = 1*( étiquette "." ) étiquette
étiquette      = utf8-rtext *(ldh-str)
ldh-str        = *( utf8-rtext / "-" ) utf8-rtext
utf8-rtext     = ALPHA / CHIFFRE / UTF8-xtra-char
```

### 2.3 Considérations sur la longueur du NAI

Les appareils qui traitent les NAI DOIVENT accepter une longueur de NAI d'au moins 72 octets. Les appareils DEVRAIENT accepter une longueur de NAI de 253 octets. Cependant, les questions de mise en œuvre suivantes devraient être prises en compte :

* la contrainte de longueur en octets du NAI peut imposer une contrainte plus sévère au nombre de caractères UTF-8.
* Les NAI sont souvent transportés dans l'attribut User-Name *(nom d'utilisateur)* du protocole service d'authentification distante d'utilisateur appelant (RADIUS, *Remote Authentication Dial-In User Service*). Malheureusement, le paragraphe 5.1 de la [RFC2865] déclare que "la capacité à traiter au moins 63 octets est recommandée". Par suite, il se peut qu'il ne soit pas possible 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'attribut est de 253 octets, RADIUS est incapable de prendre en charge les longueurs de NAI de plus de 253 octets.
* Les NAI peuvent aussi être transportés dans l'attribut Nom-d'utilisateur de Diameter [RFC6733], qui accepte des longueurs de contenu jusqu'à 2^24 - 9 octets. Par suite, les NAI traités par seulement les nœuds Diameter peuvent être très longs. Cependant, un NAI transporté sur Diameter peut finalement être traduit en RADIUS, auquel cas les limitations ci-dessus vont s'appliquer.
* Les NAI peuvent être transportés dans d'autres protocoles. Chaque protocole peut avoir ses propres limitations sur la longueur maximum de NAI.

Les critères ci-dessus devraient permettre la plus large utilisation et la plus large interopérabilité possible du NAI.

### 2.4 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 portion nom-d'utilisateur-utf8 DEVRAIT être traitée comme des données opaques lorsque elle est traitée par des nœuds qui ne font pas partie du domaine de rattachement pour ce domaine.

C'est-à-dire, le seul domaine qui est capable d'interpréter la signification de la portion nom-d'utilisateur-utf8 du NAI est le domaine de rattachement. Aucun domaine tiers ne peut tirer de conclusions sur le nom-d'utilisateur-utf8 et ne peut le décoder en sous champs. Par exemple, il peut être utilisé comme "prénom.nom-de-famille", ou il peut être entièrement fait de chiffres, ou il peut être un identifiant aléatoire en hexadécimal. Il n'y a tout simplement aucun moyen (et aucune raison) qu'un domaine autre quelconque interprète le champ nom-d'utilisateur-utf8 comme ayant une signification quelle qu'elle soit.

Dans certaines situations, les NAI sont utilisés avec une méthode d'authentification séparée qui peut transférer la partie nom d'utilisateur d'une manière plus sûre pour augmenter la confidentialité. Dans ce cas, les NAI PEUVENT être fournis en 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, telle que "anonymous", car inclure une partie nom d'utilisateur fixe est ambigu à l'égard du fait que le NAI se réfère ou non à un seul usager. Cependant, la pratique courante est d'utiliser le nom d'utilisateur "anonymous" plutôt que d'omettre la partie nom d'utilisateur. Ce comportement est aussi permis.

Le cas d'utilisation le plus courant d'omission ou d'obscurcissement de la partie nom d'utilisateur est avec les méthodes EAP fondées sur TLS telles que le protocole de sécurité de la couche transport tunnelée (TTLS, *Tunneled Transport Layer Security*) [RFC5281]. Ces méthodes permettent un identifiant "extérieur", qui est normalement un "@domaine" rendu anonyme. Cet identifiant externe permet d'acheminer la demande d'authentification à partir d'un domaine visité vers un domaine de rattachement. En même temps, la confidentialité de la partie nom d'utilisateur est conservée à l'égard du réseau visité. Le protocole assure l'échange d'authentification "interne", dans lequel un identifiant complet est utilisé pour authentifier un usager.

Ce scénario offre le meilleur des deux modes. Un NAI anonyme peut être utilisé pour acheminer l'authentification au domaine de rattachement, et le domaine de rattachement a des informations suffisantes pour identifier et authentifier les utilisateurs.

Cependant, certains protocoles ne prennent pas en charge les méthodes d'authentification qui permettent des échanges

"internes" et "externes". Ces protocoles se limitent à utiliser un identifiant publiquement visible. Il est donc RECOMMANDÉ que de tels protocoles utilisent des identifiants éphémères. On reconnaît que cette pratique n'est pas utilisée actuellement et sera vraisemblablement difficile à mettre en œuvre.

De même que l'utilisateur anonyme, il peut y avoir des situations où des portions du domaine sont sensibles. Pour ces situations, il est RECOMMANDÉ que la portion sensible du domaine soit aussi omise (par exemple, d'utiliser "@exemple.com" au lieu de "@sensible.exemple.com", ou "anonymous@sensible.exemple.com"). Le domaine de rattachement est d'autorité pour les usagers dans tous les sous domaines et peut (si nécessaire) acheminer la demande d'authentification au sous-système approprié au sein du domaine de rattachement.

Pour les besoins de l'itinérance, il est normalement nécessaire de localiser le serveur d'authentification d'extrémité approprié pour le NAI en question avant que la conversation d'authentification puisse se faire. Par suite, l'acheminement de l'authentification est impossible tant que la portion domaine n'est pas disponible et n'est pas dans un format bien connu.

### 2.5 Jeux de caractères internationaux

La présente spécification permet les noms d'utilisateur et les domaines internationaux. Les noms d'utilisateur internationaux se fondent sur l'utilisation de caractères Unicode, codés en UTF-8. L'internationalisation de la portion nom d'utilisateur du NAI se fonde sur les extensions "En-têtes de messagerie électronique internationalisés" [RFC6532] à la portion "partie-locale" des adresses de messagerie électronique [RFC5322].

Pour s'assurer d'une représentation canonique, les caractères de la portion domaine dans un NAI DOIVENT correspondre à l'ABNF de la présente spécification ainsi qu'aux exigences spécifiées dans la [RFC5891]. En pratique, ces exigences consistent en les éléments suivants :

* Les domaines DOIVENT être d'une forme qui puisse être enregistrée comme un nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) dans le DNS.

Cette liste est significativement plus courte et plus simple que celle du paragraphe 2.4 de la [RFC4282]. La forme suggérée dans la [RFC4282] dépendait de ce que les nœuds intermédiaires effectuaient les canonisations sur la base d'informations insuffisantes, ce qui signifiait que la forme n'était pas canonique.

Spécifier l'exigence de domaine comme ci-dessus signifie que les exigences dépendent de spécifications qui sont référencées ici, plutôt que copiées. Cela permet de mettre à jour la définition de domaine lorsque les documents de référence changent, sans exiger de révision de la présente spécification.

Un avertissement sur la recommandation ci-dessus est le problème noté dans la [RFC6912]. Ce document note qu'il y a des restrictions supplémentaires autour de l'enregistrement DNS qui interdisent certains codets dans une étiquette U du DNS. Ces restrictions ne peuvent pas être exprimées par un algorithme.

Pour la présente spécification, cet avertissement signifie ce qui suit : les domaines qui ne correspondent pas à l'ABNF ci-dessus ne sont pas des NAI valides. Cependant, certains domaines qui correspondent à l'ABNF sont quand même des NAI invalides. C'est-à-dire, satisfaire à l'ABNF est une exigence nécessaire, mais pas suffisante pour un NAI.

En général, l'exigence ci-dessus signifie de suivre les exigences spécifiées dans la [RFC5891].

### 2.6 Processus de normalisation

La conversion en Unicode ainsi que la normalisation DEVRAIENT être effectuées par les systèmes périphériques (par exemple, tablettes, ordinateurs portables, téléphones intelligents, etc.) qui prennent le texte "local" en entrée. Ces systèmes périphériques conviennent le mieux pour déterminer l'intention de l'usager et convertir le texte "local" en forme normalisée.

Les autres systèmes AAA comme les mandataires n'ont pas accès aux particularités locales et aux informations de jeu de caractères qui sont disponibles aux systèmes périphériques. Donc, ils ne seront pas toujours capables de convertir les entrées locales en Unicode.

C'est-à-dire que tout le traitement des NAI des jeux de caractères "locaux" et des particularités locales en UTF-8 DEVRAIT être effectué par les systèmes périphériques, avant que le NAI entre dans le système AAA. À l'intérieur d'un système AAA, les NAI sont envoyés dans le réseau sous leur forme canonique, et cette forme canonique est utilisée pour toutes les comparaisons de NAI et/ou de domaine.

Copier le texte localisé en des champs qui puissent ensuite être placés dans l'attribut RADIUS Nom-d'utilisateur est problématique. Cette pratique peut résulter en ce qu'un mandataire AAA rencontre des caractères non UTF-8 dans ce qu'il s'attend à être un NAI. Un exemple de cette exigence est le paragraphe 2.1 de la [RFC3579], qui déclare : "le NAS DOIT copier le contenu du champ Données-de-type de la réponse/identité EAP reçue de l'homologue dans l'attribut Nom-d'utilisateur".

Il en résulte que les mandataires AAA s'attendent à ce que le contenu de la réponse/identité EAP envoyée par un demandeur EAP se compose de caractères UTF-8, et non de texte localisé. Utiliser du texte localisé dans les champs Nom d'utilisateur ou Identité AAA signifie que l'acheminement par le domaine devient difficile ou impossible.

À la différence du paragraphe 2.4 de la [RFC4282], les systèmes AAA ne sont pas supposés effectuer des comparaisons de NAI, des confrontations, et de l'acheminement AAA sur la base du NAI tel qu'il est reçu. La présente spécification donne une représentation canonique, s'assure que les systèmes AAA intermédiaires tels que les mandataires ne sont pas obligés d'effectuer des traductions, et qu'on peut s'attendre à travailler dans les systèmes AAA qui ne connaissent pas les jeux de caractères internationaux.

Dans l'idéal, les exigences suivantes seraient largement mises en œuvre :
* Les systèmes d'extrémité qui utilisent du texte "localisé" DEVRAIENT normaliser le NAI avant de l'utiliser comme identifiant dans un protocole d'authentification.
* Les systèmes AAA NE DEVRAIENT PAS normaliser le NAI, car ils peuvent n'avoir pas des informations suffisantes pour effectuer la normalisation.

Cette approche pose cependant quelques problèmes.

### 2.6.1 Problèmes du processus de normalisation

Les exigences du paragraphe précédent ne sont pas mises en œuvre à l'heure actuelle. Par exemple, la plupart des mises en œuvre de EAP utilisent un identifiant d'utilisateur qui leur est passe d'un autre système local. Cet identifiant est traité comme une tache opaque et est placé comme tel dans le champ EAP Identité. Tout système qui reçoit ensuite cet identifiant est supposé capable de le comprendre et le traiter.

Cette tache opaque peut malheureusement contenir du texte localisé, ce qui signifie que les systèmes AAA ont à traiter ce texte.

Ces limitations ont les implications théoriques et pratiques suivantes :
* les systèmes d'extrémité utilisés aujourd'hui ne normalisent généralement pas le NAI ;
* donc, les systèmes AAA DEVRAIENT tenter de normaliser le NAI.

La suggestion ci-dessus contredit celle du paragraphe précédent. C'est la réalité de protocoles imparfaits.

Lorsque l'identifiant d'utilisateur peut être normalisé, ou déterminé comme étant en forme normale, la forme normale DOIT être utilisée comme NAI. Dans toutes les autres circonstances, l'identifiant d'utilisateur NE DOIT PAS être traité comme un NAI. Ces données sont cependant quand même un identifiant d'utilisateur. Les systèmes AAA NE DOIVENT PAS échouer à l'authentification simplement parce que l'identifiant d'utilisateur n'est pas un NAI.

C'est-à-dire que lorsque la portion domaine du NAI n'est pas reconnue par un serveur AAA, il DEVRAIT essayer de normaliser le NAI en forme NFC. Cette forme normalisée peut alors être utilisée pour voir si le domaine correspond à un domaine connu. Si aucune correspondance n'est trouvée, la forme originale du NAI DEVRAIT être utilisée dans tout les traitements suivants.

Le serveur AAA peut aussi convertir les domaines en Punycode et effectuer toutes les comparaisons de domaine sur les chaînes Punycode résultantes. Cette conversion suit les recommandations ci-dessus mais peut avoir des effets opérationnels et des modes d'échec différents.

## 2.7 Utilisation dans d'autres protocoles

Comme noté précédemment, le format de NAI peut être utilisé dans d'autres protocoles non AAA. Il est RECOMMANDÉ que la définition donnée ici soit utilisée inchangée. Utiliser d'autres définitions pour les identifiants d'utilisateur peut affecter l'interopérabilité, ainsi que la capacité de l'utilisateur à réussir à s'authentifier. Il est RECOMMANDÉ que les protocoles qui requièrent l'utilisation d'un identifiant d'utilisateur utilisent le format de NAI.

Le présent document ne peut pas exiger que les autres protocoles utilisent le format de NAI pour les identifiants d'utilisateur. Leurs besoins ne sont pas connus et, pour l'instant, inconnaissables. Le présent document suggère que l'interopérabilité et l'authentification inter domaines sont utiles et devraient être encouragées.

Lorsque un protocole est à 8 bits, il peut vraisemblablement transporter le NAI tel qu'il est, sans autre modification.

Lorsque un protocole n'est pas à 8 bits, il ne peut pas transporter le NAI tel quel. Le présent document présume plutôt qu'une couche de transport spécifique du protocole se charge du codage du NAI à l'entrée du protocole et le décode lorsque le NAI sort du protocole. La version codée ou en échappement du NAI n'est pas un NAI valide et NE DOIT PAS être présentée au système AAA.

Par exemple, HTTP porte des identifiants d'utilisateur mais échappe le caractère '.' par "%2E" (entre autres). Lorsque HTTP est utilisé pour transporter le NAI "fred@exemple.com", les données telles que transportées seront sous la forme "fred@exemple %2Ecom". Ces données n'existent que dans HTTP et ne sont pertinentes pour aucun système AAA.

Toute comparaison, validation, ou utilisation du NAI DOIT être faite sous sa forme non échappée (c'est-à-dire, en utf8 strict).

### 2.8 Utilisation du format de NAI pour d'autres identifiants

Comme exposé à la Section 1, il est RECOMMANDÉ que le format de NAI soit utilisé comme format standard pour les identifiants d'utilisateur. Ce paragraphe expose cette utilisation plus en détail.

Il est souvent utile de créer de nouveaux identifiants à utiliser dans des contextes spécifiques. Ces identifiants peuvent avoir un certain nombre de propriétés différentes, dont la plupart sont sans importance pour le présent document. L'objectif du présent document est de créer des identifiants qui soient dans un format bien connu et qui auront des espaces de noms. Le format de NAI correspond à ces exigences.

Un exemple d'une telle utilisation est "l'identité d'utilisateur privé", qui est un identifiant défini par le projet en partenariat de la troisième génération (3GPP, *3rd Generation Partnership Project*). Cet identifiant est utilisé pour identifier de façon univoque l'utilisateur du réseau. L'identifiant est utilisé pour l'autorisation, l'authentification, la comptabilité, l'administration, etc. L'identité d'utilisateur privé est unique au monde et est définie par l'opérateur du réseau de rattachement. Le format de l'identifiant est explicitement le NAI, comme c'est déclaré au paragraphe 13.3 de [3GPP] : l'identité d'utilisateur privé devra prendre la forme d'un NAI, et devra avoir la forme "nom d'utilisateur@domaine" comme spécifié au paragraphe 2.1 de la RFC4282 de l'IETF.

Pour le 3GPP, la portion "nom d'utilisateur" est un identifiant univoque qui est déduit des informations spécifiques de l'appareil. La portion "domaine" est composée d'informations sur le réseau de rattachement, suivie par la chaîne de base "3gppnetwork.org" (par exemple, 234150999999999@ims.mnc015.mcc234.3gppnetwork.org).

Ce format tel que défini par le 3GPP assure que l'identifiant est unique au monde, car il se fonde sur le domaine "3gppnetwork.org". Il assure que la portion "domaine" est spécifique d'un réseau (ou organisation) de rattachement particulier, via le préfixe "ims.mnc015.mcc234" du domaine. Finalement, il assure que la portion "nom d'utilisateur" suit un format bien connu.

Le présent document suggère que le format de NAI soit utilisé pour toutes les nouvelles spécifications et/ou protocoles où un identifiant d'utilisateur est requis. Lorsque les portions "nom d'utilisateur" ont besoin d'être créées avec des sous-champs, une méthode bien connue et documentée, comme cela a été fait avec le 3GPP, est préférable à des méthodes ad hoc.

## 3. Acheminement à l'intérieur des systèmes AAA

De nombreux systèmes AAA utilisent la portion "domaine-utf8" du NAI pour acheminer les demandes au sein d'un réseau mandataire AAA. La sémantique de cette opération implique un tableau logique d'acheminement AAA, où la portion "domaine-utf8" agit comme une clé, et les valeurs mémorisées dans le tableau sont un ou plusieurs serveurs AAA de "prochain bond".

Les nœuds intermédiaires DOIVENT utiliser la portion "domaine-utf8" du NAI sans modification pour effectuer cette recherche. Comme on l'a noté précédemment, les nœuds intermédiaires peuvent ne pas avoir accès aux mêmes informations sur les particularités locales que le système qui a injecté le NAI dans les systèmes d'acheminement AAA. Donc, presque toutes les comparaisons "insensibles à la casse" peuvent être fausses. Lorsque le "domaine-utf8" est entièrement en ASCII, les systèmes AAA courants effectuent parfois une confrontation insensible à la casse sur les domaines. Cette méthode PEUT être

poursuivie car il s'est révélé qu'elle fonctionne en pratique.

De nombreux systèmes non AAA existants ont des identifiants d'utilisateur qui sont similaires en format au NAI mais ne sont pas conformes à la présente spécification. Par exemple, ils peuvent utiliser une forme non NFC, ou ils peuvent avoir plusieurs caractères "@" dans l'identifiant d'utilisateur. Les nœuds intermédiaires DEVRAIENT normaliser les identifiants non NFC en NFC, avant de chercher le "domaine-utf8" dans le tableau d'acheminement logique. Les nœuds intermédiaires NE DOIVENT PAS modifier les identifiants qu'ils transmettent. Les données telles qu'entrées par l'usager sont inviolables.

Le "domaine-utf8" fourni dans le tableau d'acheminement logique AAA DEVRAIT être fourni par le mandataire avant qu'il reçoive aucun trafic AAA. Le "domaine-utf8" DEVRAIT être fourni par le système de "prochain bond" ou de "rattachement" qui fournit aussi les informations d'acheminement nécessaires pour que les paquets atteignent le prochain bond.

Ces informations de "prochain bond" peuvent être toute information parmi les suivantes : adresse IP, accès, secret partagé RADIUS, certificat TLS, nom d'hôte DNS, ou instructions pour utiliser la découverte dynamique de DNS (c'est-à-dire, la recherche d'un enregistrement dans le domaine "domaine-utf8"). Cette liste n'est pas exhaustive et peut être étendue par de futures spécifications.

Il est RECOMMANDÉ d'utiliser la totalité du "domaine-utf8" pour les décisions d'acheminement. Cependant, les systèmes AAA PEUVENT utiliser une portion de la portion "domaine-utf8", pour autant que cette portion soit un "domaine-utf8" valide et soit traité comme ci-dessus. Par exemple, acheminer "fred@exemple.com" à une destination "com" est interdit, parce que "com" n'est pas un "domaine-utf8" valide. Cependant, acheminer "fred@ventes.exemple.com" à la destination "exemple.com" est permis.

Une autre raison d'interdire l'utilisation d'une seule étiquette (par exemple, "fred@ventes") est que de nombreux systèmes non AAA traitent une seule étiquette comme étant un identifiant local au sein de leur domaine. C'est-à-dire qu'un usager qui se connecte comme "fred@ventes" à un domaine "exemple.com" serait traité comme si le NAI était "fred@ventes.exemple.com". Permettre l'utilisation d'une seule étiquette signifierait changer l'interprétation et la signification de la seule étiquette, ce qui ne peut être fait.

### 3.1 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 qu'alors que la portion usager du NAI se fonde sur la portion "partie-locale" du "Format du message Internet" [RFC5322] d'une adresse de messagerie électronique telle qu'étendue par "En-têtes de messagerie électronique internationalisés" [RFC6532], elle a été modifiée pour les besoins du paragraphe 2.2. Il ne permet pas le texte entre guillemets avec des espaces blanches de "saut à la ligne" ou "non saut à la ligne" qui sont couramment utilisées dans les adresses de messagerie électronique. À ce titre, le NAI n'est pas nécessairement équivalent aux noms d'utilisateur utilisés dans le message électronique.

Cependant, il est de pratique courante d'utiliser les adresses de messagerie électronique comme identifiants d'utilisateur dans les systèmes AAA. L'ABNF du paragraphe 2.2 est défini comme étant proche de la portion "addr-spec" de la [RFC5322] telle qu'étendue par la [RFC6532], tout en étant encore compatible avec la [RFC4282].

À l'inverse du paragraphe 2.5 de la [RFC4282], le présent document déclare que les exigences d'internationalisation pour les NAI et les adresses de messagerie électronique sont similaires en substance. Le NAI et les identifiants de messagerie électronique peuvent être identiques, et tous deux ont besoin d'être entrés par l'usager et/ou l'opérateur qui fournit l'accès réseau à cet usager. Il y a donc de bonnes raisons pour que les exigences d'internationalisation soient similaires.

### 3.2 Compatibilité avec le DNS

La portion "domaine-utf8" du NAI est destinée à être compatible avec les noms de domaines internationalisés (IDN) [RFC5890]. Comme défini ci-dessus, la portion "domaine-utf8" telle qu'elle est transportée au sein un protocole à 8 bits pur comme RADIUS et EAP peut contenir tout caractère UTF-8 valide. Il n'y a donc pas de raison pour qu'un NAS convertisse la portion "domaine-utf8" d'un NAI en une forme de codage Punycode [RFC3492] avant de placer le NAI dans un attribut Nom-d'utilisateur RADIUS.

Le NAI ne fait pas de distinction entre les étiquettes A et les étiquettes U, car ce sont des termes spécifiques du DNS. C'est plutôt une étiquette IDNA valide, selon le premier élément du paragraphe 2.3.2.1 de la [RFC5890]. Comme on l'a noté dans ce paragraphe, le terme de "étiquette IDNA valide" englobe les deux étiquettes "A" et "U".

Lorsque la portion domaine du NAI est utilisée comme base d'une résolution de nom, il peut être nécessaire de convertir les

noms de domaine internationalisés en forme de codage Punycode [RFC3492] comme décrit dans la [RFC5891]. Comme noté à la Section 2 de la [RFC6055], les interfaces de programmation d'application (API, *Application Programming Interface*) de résolveur ne sont pas nécessairement spécifiques du DNS, de sorte que la conversion en Punycode doit être faite avec soin :
Les applications qui convertissent un IDN en forme étiquette A avant d'appeler (par exemple) getaddrinfo() vont résulter en un échec de résolution de nom si le nom Punycode est directement utilisé dans de tels protocoles. Avoir des bibliothèques ou des protocoles pour convertir des étiquettes A en les schémas de codage définis par le protocole (par exemple, UTF-8) exigerait des changements aux API et/ou aux serveurs, ce que les noms de domaines internationalisés pour les applications (IDNA, *Internationalized Domain Names for Applications*) étaient destinés à éviter.

Il en résulte que les applications NE DEVRAIENT PAS supposer que les noms non ASCII peuvent se résoudre en utilisant le DNS public et en les convertissant aveuglément en étiquettes A sans savoir quel protocole sera choisi par la bibliothèque de résolution de noms.

### 3.3 Construction de domaine

Le domaine de rattachement apparaît normalement dans la portion "domaine-utf8" 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 joignable que via des mandataires intermédiaires.

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 sait explicitement que (a) l'autre domaine spécifié est disponible et (b) l'autre domaine accepte cet usage. L'envoyeur peut déterminer l'accomplissement de ces conditions par une base de données, une 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'usage ou de l'application désirée.

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

#### 3.3.1 Pratiques historiques

Certains systèmes AAA ont historiquement utilisé des modifications de NAI avec plusieurs décorations de "préfixe" et "suffixe" pour effectuer un acheminement explicite à travers plusieurs mandataires à l'intérieur d'un réseau AAA.

Dans des environnements fondés sur RADIUS, l'utilisation de NAI décorés est NON RECOMMANDÉE pour les raisons suivantes :

* L'utilisation de chemins d'acheminement explicite est fragile et ne permet pas de faire face aux changements dans le réseau suite à l'activation/désactivation des serveurs ou des changements de relations d'affaires.
* Il n'y a pas de protocole d'acheminement RADIUS, ce qui signifie que les chemins d'acheminement doivent être communiqués "hors bande" à tous les nœuds AAA intermédiaires, et aussi à tous les systèmes bordures (par exemple, demandeurs) qui attendent d'obtenir l'accès réseau.
* Utiliser des chemins d'acheminement explicites exige de mettre à jour des milliers, sinon des millions, de systèmes bordures avec les nouvelles informations de chemins lorsque change un chemin d'acheminement AAA. Cela ajoute un coût énorme qu'il vaudrait mieux ne faire que sur quelques systèmes AAA dans le réseau.
* Les mises à jour manuelles des chemins RADIUS sont coûteuses, en temps et en argent, et enclines à l'erreur.
* Créer des formats compatibles pour le NAI est difficile lorsque des "préfixes" et "suffixes" définis en local entrent en conflit avec des pratiques similaires ailleurs dans le réseau. Ces conflits signifient que connecter deux réseaux peut être impossible dans certains cas, car il n'y a pas moyen que des paquets soient acheminés correctement d'une façon qui satisfasse toutes les exigences de tous les mandataires intermédiaires.
* Exercer une pression sur le système des noms de domaines du DNS établit un espace de nom unique au monde pour les domaines.

En résumé, les pratiques et capacités du réseau ont changé de façon significative depuis que les NAI ont été pour la première fois surchargés pour définir des chemins AAA à travers un réseau. Bien que l'acheminement par chemin explicite géré manuellement ait été autrefois utile, le moment est venu d'utiliser de meilleures méthodes.

En dépit des recommandations précédentes, la pratique décrite ci-dessus est largement utilisée pour l'acheminement Diameter [RFC5729]. Les chemins qui y sont décrits sont gérés automatiquement pour le provisionnement d'accréditifs et les mises à jour d'acheminement. Ces chemins existent aussi dans des cadres particuliers (typiquement, de 3G) où l'adhésion est contrôlée et le comportement de système est normalisé. Il n'y a pas de problème connu à l'utilisation de l'acheminement explicite dans un tel environnement.

Cependant, si des identifiants décorés sont utilisés comme dans "domaine_de_rattachement.exemple.org! usager@autredomaine.exemple.net" alors la partie avant le '!' (non échappé) DOIT être un "domaine-utf8" comme défini dans l'ABNF du paragraphe 2.2. Lors de la réception d'un tel identifiant, le système "autredomaine.exemple.net" DOIT convertir l'identifiant en "usager@domaine_de_rattachement.exemple.org" avant de transmettre la demande. Le système de transmission DOIT alors appliquer l'acheminement AAA normal AAA pour la transaction, sur la base de l'identifiant mis à jour.

### 3.4 Exemples

Les 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
\(usager\)@exemple.net

Le NAI valide supplémentaire est montré ci-dessous comme une chaîne hexadécimale, car le présent document ne peut contenir que des caractères ASCII :

626f 6240 ceb4 cebf ceba ceb9 cebc ceae 2e63 6f6d

Des exemples d'identifiants d'accès réseau invalides sont les suivants :

fred@exemple
fred@exemple_9.com
fred@exemple.net@exemple.net
fred.@exemple.net
eng:nancy@exemple.net
eng;nancy@exemple.net
(usager)@exemple.net
<nancy>@exemple.net

Un exemple donné dans la [RFC4282] est permis par l'ABNF, mais est NON RECOMMANDÉ à cause de l'utilisation de la forme de codage Punycode [RFC3492] pour ce qui est maintenant une chaîne UTF-8 valide :

alice@xn--tmonesimerkki-bfbb.exemple.net

## 4. Considérations pour la sécurité

Comme un NAI révèle l'affiliation de rattachement d'un usager, il peut aider un agresseur à bien sonder l'espace du nom d'utilisateur. Normalement, ce problème concerne plutôt les protocoles qui transmettent le nom d'utilisateur en clair à travers l'Internet, comme dans RADIUS [RFC2865], [RFC2866]. Afin d'empêcher la divulgation 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 [RFC6733].

La présente spécification ajoute la possibilité de cacher la partie nom d'utilisateur dans le NAI, en l'omettant. Comme exposé au paragraphe 2.4, ceci n'est possible que lorsque les NAI sont utilisés avec une méthode d'authentification séparée qui puisse transférer le nom d'utilisateur d'une façon sécurisée. Dans certains cas, des mécanismes spécifiques de l'application ont aussi été utilisés avec les NAI. Par exemple, certaines méthodes EAP 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.

### 4.1 Corrélation des identités dans le temps et à travers les protocoles

Les recommandations des paragraphes 2.7 et 2.8 sur l'utilisation du NAI dans les autres protocoles ont des implications sur la confidentialité. Tout attaquant qui est capable d'observer le trafic qui contient le NAI peut retracer l'usager et peut corréler son activité au fil du temps et à travers de multiples protocoles. Les accréditifs d'authentification DEVRAIENT donc être transportés sur des canaux qui permette des communications privées, ou alors plusieurs identifiants DEVRAIENT être utilisés, afin que le traçage de l'usager soit impossible.

Il est RECOMMANDÉ d'améliorer la confidentialité d'usager par la configuration de plusieurs identifiants pour un usager. Ces identifiants peuvent être changés au fil du temps, afin de rendre plus difficile le traçage d'usager par un observateur malveillant. Cependant, le provisionnement et la gestion des identifiants peuvent être difficiles en pratique – raison probable pour laquelle des identifiants multiples sont rarement utilisés aujourd'hui.

### 4.2 Identifiants multiples

Le paragraphe 1.3 déclare que plusieurs formats d'identifiant permettent à des attaquants de faire des revendications contradictoires sans être détectés. Cette affirmation mérite des commentaires. Le paragraphe 2.4 discute des identifiants "internes" et "externes" dans le contexte de TTLS [RFC5281]. Une lecture attentive de cette spécification montre qu'il n'est pas exigé que les identifiants interne et externe soit dans une relation quelconque. C'est-à-dire qu'il est parfaitement valide d'utiliser "@exemple.com" pour un identifiant externe et "usager@exemple.org" comme identifiant interne. La demande d'authentification sera alors acheminée à "exemple.com", qui sera probablement incapable d'authentifier "usager@exemple.org".

Pire encore, une mauvaise configuration de "exemple.com" signifie qu'elle peut à son tour mandater la demande d'authentification au domaine "exemple.org". Une telle authentification inter domaines est très problématique, et il y a peu de bonnes raisons pour la permettre. Il est donc RECOMMANDÉ que les systèmes qui permettent des identifiants "externes" anonymes exigent que le domaine "interne" soit le même que, ou soit un sous domaine du domaine "externe". Une demande d'authentification qui utilise des domaines disparates est une violation de la sécurité, et la demande DEVRAIT être rejetée.

La situation empire lorsque plusieurs protocoles sont impliqués. Le protocole TTLS permet au CHAP de Microsoft (MS-CHAP) [RFC2433] d'être transporté dans le tunnel TLS. MS-CHAP définit son propre identifiant, qui est encapsulé dans l'échange MS-CHAP. Il n'est pas exigé un format particulier pour cet identifiant, il n'est pas exigé qu'il soit en UTF-8, et, en pratique, il peut être dans un des nombreux jeux de caractères inconnus. Il n'y a en pratique aucun moyen de déterminer quel jeu de caractères a été utilisé pour cet identifiant. Le résultat est que l'identité EAP "externe" portée par TTLS ne va probablement même pas partager le même jeu de caractères que l'identifiant "interne" utilisé par MS-CHAP. Les deux identifiants sont entièrement indépendants et fondamentalement incomparables. Un tel concept de protocole est NON RECOMMANDÉ.

## 5. Administration des noms

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

Les noms de domaines de NAI doivent être univoques, et l'obtention du droit d'utiliser un certain domaine de NAI pour les besoins de l'itinérance coïncide avec l'acquisition des droits d'utiliser un certain nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*). Ceux qui souhaitent utiliser un nom de domaine de NAI devraient d'abord acquérir les droits d'utilisation du FQDN correspondant. Les administrateurs NE DOIVENT PAS utiliser publiquement un domaine de NAI si ils ne possèdent pas le FQDN correspondant. L'utilisation privée de domaines de FQDN qu'on ne possède pas dans un domaine administratif est permis, bien qu'il soit RECOMMANDÉ que des noms d'exemple soient utilisés, comme "exemple.com".

Noter que l'usage d'un FQDN comme nom de domaine n'exige pas l'utilisation du DNS pour la localisation du serveur d'authentification. Bien que Diameter [RFC6733] prenne 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 d'effectuer l'acheminement d'authentification. Les mises en œuvre décrites dans la [RFC2194] n'utilisaient pas le DNS pour la localisation du serveur d'authentification dans un domaine. De même, les mises en œuvre existantes n'ont pas éprouvé le besoin de protocoles d'acheminement dynamique ou de propagation des informations d'acheminement mondial. Noter aussi qu'il n'est pas exigé que le NAI représente une adresse de messagerie électronique valide.

# 6. Références

## 6.1. Références normatives

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

[RFC3629] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", STD 63, novembre 2003.

[RFC5198] J. Klensin, M. Padlipsky, "Format Unicode pour les échanges sur le réseau", mars 2008. *(P.S.)*

[RFC5234] D. Crocker, éd., P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

[RFC5890] J. Klensin, "Noms de domaine internationalisés pour les applications (IDNA) : Définitions et cadre documentaire", août 2010. *(Remplace RFC3490) (P.S.)*

[RFC5891] J. Klensin, "Noms de domaine internationalisés pour les applications (IDNA) : Le protocole", août 2010. *(P.S.)*

[RFC6365] P. Hoffman, J. Klensin, "Terminologie utilisée dans l'internationalisation à l'IETF", septembre 2011. (BCP0166)

## 6.2. Références pour information

[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. *(Hist.)*

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

[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, et autres, "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)*

[RFC3492] A. Costello, "Punycode : Codage Bootstring d'Unicode pour les noms de domaine internationalisés dans les applications (IDNA)", mars 2003. *(P.S.)*

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

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

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. (*Remplace* RFC2486) *(P.S.)*

[RFC4311] R. Hinden, D. Thaler, "Partage de charge d'hôte à routeur dans IPv6", novembre 2005. (*MàJ* RFC2461) *(P.S.)*

[RFC5281] P. Funk, S. Blake-Wilson, "Protocole authentifié de sécurité de couche Transport version 0 tunnelé dans le protocole d'authentification extensible (EAP-TTLSv0)", août 2008. *(Information)*

[RFC5322] P. Resnick, éd., "Format du message Internet", octobre 2008. (*Remplace* RFC2822) (MàJ RFC4021) *(D.S.)*

[RFC5335] Y. Abel, éd., "En-têtes de messagerie internationalisés", septembre 2008. (*MàJ* RFC2045, RFC2822) (*Remplacée par la* RFC6532) *(Expérimentale)*

[RFC5729] J. Korhonen, éd., M. Jones, L. Morand, T. Tsou, "Précisions sur l'acheminement des demandes Diameter sur la base du nom d'utilisateur et du domaine", décembre 2009, *(P. S.)*

[RFC6055] D. Thaler, J. Klensin, S. Cheshire. "Réflexions de l'IAB sur les codages des noms de domaines internationalisés", février 2011. (*MàJ* RFC2130) *(Information)*

[RFC6532] A. Yang, S. Steele, N. Freed, "En-têtes de messagerie électronique internationalisée", février 2012. *(P.S.)*

[RFC6733] V. Fajardo, J. Arkko, J. Loughney, G. Zorn, "Protocole de base Diameter", octobre 2012. *(P.S.)*

[RFC6912] A. Sullivan et autres, "Principes de l'inclusion de codets Unicode dans des étiquettes dans le DNS", 04/2013 *(Info.)*

[EDUROAM] "eduroam (EDUcation ROAMing)", < http://eduroam.org >.

[3GPP] 3GPP, "Numbering, addressing and Identification", 3GPP TS 23.003, Livraison du 12 juillet 2014, <ftp://ftp.3gpp.org/Specs/archive/23_series/23.003/ >.

## Appendice A. Changements par rapport à la RFC4282

Le présent document contient les mises à jour suivantes par rapport à la définition de NAI précédente de la [RFC4282] :

* La syntaxe formelle du paragraphe 2.1 a été mise à jour pour interdire les caractères non UTF-8 (par exemple, les caractères avec le "bit de poids fort" établi).
* La syntaxe formelle du paragraphe 2.1 de la [RFC4282] a été mise à jour pour permettre l'UTF-8 dans la portion "domaine" du NAI.
* La syntaxe formelle du paragraphe 2.1 de la [RFC4282] a été appliquée au NAI après son "internationalisation" via la fonction ToAscii. Le contenu du NAI avant son "internationalisation" était indéterminé. Le présent document met à jour la syntaxe formelle pour définir une forme internationalisée du NAI et interdire l'utilisation de la fonction ToAscii pour "l'internationalisation" du NAI.
* La grammaire de la portion utilisateur et de la portion domaine se fonde sur une combinaison du "nai" défini au paragraphe 2.1 de la [RFC4282] et de "utf8-addr-spec" défini au paragraphe 4.4 de la [RFC5335].
* Toute utilisation de la fonction ToAscii a été déplacée dans les exigences normales pour les mises en œuvre du DNS lorsque les domaines sont utilisés comme base de recherche dans le DNS. Cela n'implique pas de changement à l'infrastructure existante du DNS.
* La discussion sur les jeux de caractères internationalisés du paragraphe 2.4 de la [RFC4282] a été mise à jour. La suggestion d'utiliser la fonction ToAscii pour les comparaisons de domaines a été retirée. Aucun système AAA n'a mis en œuvre cette suggestion, de sorte que ce changement ne devrait avoir aucun impact opérationnel.
* La Section "Acheminement à l'intérieur des systèmes AAA" est introduite dans le présent document. Le concept d'un "tableau local d'acheminement AAA" est nouveau lui aussi, bien qu'il décrive précisément la fonctionnalité de mises en œuvre très répandues.
* Les paragraphes "Compatibilité avec les noms d'utilisateur de messagerie électronique" et "Compatibilité ave les DNS" ont été révisés et mis à jour. Il est suggéré de n'utiliser la transformation Punycode que lorsque un nom de domaine est utilisé pour des recherches dans le DNS, et même lorsque la fonction n'est utilisée que par une API de résolution sur le système local, et même alors, il est recommandé que seul le réseau de rattachement effectue cette conversion.
* Le paragraphe "Construction de domaine" a été mis à jour pour noter que l'édition du NAI est NON RECOMMANDÉE.
* Le paragraphe "Exemples" a été mis à jour pour retirer l'instance d'IDN converti en ASCII. Ce comportement est maintenant interdit.

**Remerciements**

Le texte initial de ce document était la [RFC4282], qui remplaçait la RFC2486, et a été bien rédigée. Les auteurs d'origine de la [RFC4282] étaient Bernard Aboba, Mark A. Beadles, Jari Arkko, et Pasi Eronen.

**Adresse de l'auteur**

Alan DeKok
The FreeRADIUS Server Project
mél : aland@freeradius.org