

Groupe de travail Réseau
Request for Comments : 5122
RFC rendue obsolète : 4622
 Catégorie : Sur la voie de la normalisation

P. Saint-Andre, XSF
 février 2008

Traduction Claude Brière de L'Isle

Identifiants de ressource internationalisés (IRI) et identifiants de ressource universels (URI) pour le protocole extensible de messagerie et de présence (XMPP)

Statut du présent mémoire

Le présent document spécifie un protocole Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document définit l'utilisation des identifiants de ressource internationalisés (IRI, *Internationalized Resource Identifier*) et des identifiants de ressource universels (URI, *Uniform Resource Identifier*) pour identifier ou interagir avec des entités qui peuvent communiquer via le protocole extensible de messagerie et de présence (XMPP, *Extensible Messaging and Presence Protocol*).

Le présent document rend obsolète la RFC 4622.

Table des Matières

1. Introduction.....	2
1.1 Terminologie.....	2
2. Utilisation des IRI et URI XMPP.....	2
2.1 Raisons.....	2
2.2 Forme.....	3
2.3 Composant d'autorité.....	4
2.4 Composant de chemin.....	4
2.5 Composant d'interrogation.....	5
2.6 Composant d'identifiant de fragment.....	5
2.7 Génération des IRI/URI XMPP.....	6
2.8 Traitement des IRI/URI XMPP.....	8
2.9 Internationalisation.....	9
3. Enregistrement par l'IANA du schéma d'URI xmpp.....	9
3.1 Nom du schéma d'URI.....	9
3.2 Statut.....	9
3.3 Syntaxe du schéma d'URI.....	9
3.4 Sémantique du schéma d'URI.....	10
3.5 Considérations de codage.....	10
3.6 Applications/protocoles qui utilisent ce nom de schéma d'URI.....	10
3.7 Considérations d'interopérabilité.....	10
3.8 Considérations sur la sécurité.....	10
3.9 Contact.....	10
3.10 Auteur/contrôleur des changements.....	10
3.11 Références.....	11
4. Considérations relatives à l'IANA.....	11
5. Considérations sur la sécurité.....	11
5.1 Fiabilité et cohérence.....	11
5.2 Construction malveillante.....	11
5.3 Transcodage d'extrémité arrière.....	11
5.4 Informations sensibles.....	11
5.5 Attaques sémantiques.....	12
5.6 Tromperie.....	12

6. Remerciements.....	12
7. Références.....	12
7.1 Références normatives.....	12
7.2 Références pour information.....	12
Appendice A. Différences avec la RFC 4622.....	14
Appendice B. Conditions de copie.....	14
Adresse de l'auteur.....	14
Déclaration complète de droits de reproduction.....	14

1. Introduction

Le protocole extensible de messagerie et de présence (XMPP, *Extensible Messaging and Presence Protocol*) est une technologie de flux XML qui permet à deux entités sur un réseau d'échanger des éléments XML bien définis mais extensibles (appelés des "stances XML") à un débit proche du temps réel.

Comme spécifié dans la [RFC3920], les adresses d'entité utilisées dans les communications sur un réseau XMPP ne doivent pas être ajoutées avec un schéma d'identifiant de ressource universel (URI, *Uniform Resource Identifier*) (comme spécifié dans la [RFC3986]). Cependant, des applications externes à un réseau XMPP peuvent avoir besoin d'identifier des entités XMPP soit comme des URI, soit, de façon plus moderne, comme des identifiants de ressource internationalisés (IRI, *Internationalized Resource Identifier*) (voir la [RFC3987]). Des exemples de ces applications externes incluent des bases de données qui ont besoin de mémoriser des adresses XMPP et des agents d'utilisateur non natifs comme des navigateurs de la Toile et des applications de calendrier qui fournissent des interfaces à des services XMPP.

Le format d'une adresse XMPP est défini dans la [RFC3920]. Une telle adresse peut contenir presque tous les caractères Unicode [UNICODE] et doit respecter divers profils de stringprep [RFC3454]. Le résultat est qu'une adresse XMPP est pleinement internationalisable et est très proche d'être un IRI sans schéma. Cependant, étant donné qu'il n'y a pas de registre des schémas d'IRI, il est nécessaire de définir des identifiants XMPP principalement comme des URI plutôt que comme des IRI, et d'enregistrer un schéma d'URI XMPP plutôt qu'un schéma d'IRI. Donc, le présent document fait ce qui suit :

- o Il spécifie comment identifier les entités XMPP comme des IRI ou URI.
- o Il spécifie comment interagir avec les entités XMPP comme des IRI ou URI.
- o Il définit formellement la syntaxe pour les IRI et URI XMPP.
- o Il spécifie comment transformer les IRI XMPP en URI et vice versa.
- o Il enregistre le schéma d'URI xmpp.

1.1 Terminologie

Le présent document hérite de la terminologie des [RFC3987], [RFC3986], et [RFC3920].

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].

2. Utilisation des IRI et URI XMPP

2.1 Raisons

Comme décrit dans la [RFC3921], les applications de messagerie instantanée et de présence de XMPP doivent traiter les URI im: et pres: (comme spécifié par les [RFC3860] et [RFC3859]). Cependant, il y a de nombreuses autres applications de XMPP (incluant des systèmes de gestion de réseau, de flux de travail, de publication-abonnement générique, d'appels de procédure à distance, de fusion de contenu, de jeux, et de logiciel médiateur) et ces applications ne mettent pas en œuvre la sémantique de la messagerie instantanée et de présence. De plus, une entité générique XMPP ne met en œuvre la sémantique d'aucun schéma d'URI existant, comme http:, ftp:, ou mailto:. Donc, il est approprié de définir un nouveau schéma d'URI qui rende possible d'identifier ou interagir avec toute entité XMPP (pas juste des entités de messagerie instantanée et de présence) comme IRI ou URI.

Les IRI et URI XMPP sont définis pour être utilisés par des interfaces et applications non natives. Afin d'assurer l'interopérabilité sur les réseaux XMPP, quand des données sont acheminées à une entité XMPP (par exemple, quand une adresse XMPP est contenue dans l'attribut 'to' ou 'from' d'une stance XML) ou quand une entité XMPP est identifiée dans des éléments standard de protocole XMPP, l'entité DOIT être adressée comme <[nœud@]domaine[/ressource]> (c'est-à-

dire, sans être précédée d'un schéma) où les portions "identifiant de nœud", "identifiant de domaine", et "identifiant de ressource" d'une adresse XMPP se conforment aux définitions fournies à la Section 3 de la [RFC3920].

Note : pour des raisons historiques, le terme "identifiant de ressource" est utilisé dans XMPP pour se référer à la portion facultative d'une adresse XMPP qui suit l'identifiant de domaine jusqu'au caractère "/" séparateur (pour les détails, se référer au paragraphe 3.4 de la [RFC3920]) ; cette utilisation du terme "identifiant de ressource" ne doit pas être confondue avec les significations de "ressource" et "identifiant" fournies au paragraphe 1.1 de la [RFC3986].

Les IRI et URI XMPP sont définis principalement pour les besoins de l'identification plutôt que d'interaction (concernant cette distinction, voir le paragraphe 1.2.2 de la [RFC3986]). La "ressource Internet" identifiée par un IRI ou URI XMPP est une entité qui peut communiquer via XMPP sur un réseau. Un IRI ou URI XMPP peut contenir des informations supplémentaires au-dessus et au-delà de la ressource identifiée ; en particulier, comme décrit au paragraphe 2.5 un composant d'interrogation peut être inclus pour spécifier la sémantique suggérée pour une interaction avec la ressource identifiée. Il est envisagé que quand une application XMPP résout un IRI ou URI XMPP contenant la sémantique d'interaction suggérée, l'application génère une stance XMPP et l'envoi à la ressource identifiée, où la stance générée peut inclure des entrées d'utilisateur ou d'application cohérentes avec la sémantique d'interaction suggérée (pour les détails, voir le paragraphe 2.8.1).

2.2 Forme

Comme décrit dans la [RFC3920], une adresse XMPP utilisée de façon native sur un réseau XMPP est une chaîne de caractères Unicode qui (1) se conforme à un certain ensemble de profils stringprep [RFC3454] et de restrictions d'IDNA [RFC3490], (2) suit un certain ensemble de règles de syntaxe, et (3) est codée en UTF-8 [RFC3629]. La forme d'une telle adresse peut être représentée en forme Backus-Naur augmenté [RFC5234] comme :

```
[ nœud "@" ] domaine [ "/" ressource ]
```

Dans ce contexte, les règles "nœud" et "ressource" s'appuient sur des profils distincts de stringprep [RFC3454], et la règle "domaine" s'appuie sur le concept d'un nom de domaine internationalisé comme décrit dans la [RFC3490]. (Note : il n'est pas besoin de se référer au punycode dans la syntaxe d'IRI elle-même, car toute représentation de punycode va seulement se produire dans une application XMPP afin de représenter les noms de domaine internationalisés. Cependant, il est de la responsabilité de l'application traitante de convertir la syntaxe d'IRI [RFC3987] en syntaxe IDNA [RFC3490] avant d'adresser des stances XML à l'entité spécifiée sur un réseau XMPP.)

Certains caractères sont permis dans les identifiants de nœud XMPP et les identifiants de ressource XMPP mais pas dans la portion pertinente d'un IRI ou URI. Les caractères sont les suivants :

Dans les identifiants de nœud : [\] ^ ` { | }

Dans les identifiants de ressource : " < > [\] ^ ` { | }

Les caractères d'identifiant de nœud ne sont pas permis dans userinfo par la règle sub-delims et les caractères d'identifiant de ressource ne sont pas permis dans segment par la règle pchar. Ces caractères DOIT être codés en pourcentage quand on transforme une adresse XMPP en IRI ou URI XMPP.

Naturellement, afin d'être convertie en IRI ou URI, une adresse XMPP doit être précédée d'un schéma (spécifiquement, le schéma xmpp) et peut aussi devoir subir des transformations qui respectent les règles définies dans les [RFC3987] et [RFC3986]. De plus, afin de permettre une interaction avec une entité XMPP plus poussée qu'une simple identification, il est souhaitable de tirer parti des aspects supplémentaires de la syntaxe et sémantique d'URI, tels que les composants d'autorité, les composants d'interrogation, et les composants d'identifiant de fragment.

Donc, la syntaxe d'ABNF pour un IRI XMPP est définie comme montré ci-dessous en utilisant la forme Backus-Naur augmentée spécifiée par la [RFC5234], où les règles "ifragment", "ihost", et "iunreserved" sont définies dans la [RFC3987] et la règle "pct-encoded" est définie dans la [RFC3986] :

```
xmppiri = "xmpp" ":" ihierxmpp
          [ "?" iquerycomp ]
          [ "#" ifragment ]
ihierxmpp = iauthpath / ipathxmpp
iauthpath = "/" iauthxmpp [ "/" ipathxmpp ]
iauthxmpp = inodeid "@" ihost
```

```

ipathxmpp = [ inodeid "@" ] ihost [ "/" iresid ]
inodeid = *( iunreserved / pct-encoded / nodeallow )
nodeallow = "! " / "$" / "(" / ")" / "*" / "+" / "," / ";" / "="
iresid = *( iunreserved / pct-encoded / resallow )
resallow = "! " / "$" / "&" / "'" / "(" / ")" / "*" / "+" / "," / ":" / ";" / "="
iquerycomp = iquerytype [ *ipair ]
iquerytype = *iunreserved
ipair = ";" ikey "=" ivalue
ikey = *iunreserved
ivalue = *( iunreserved / pct-encoded )

```

Cependant, la syntaxe ci-dessus n'est pas appropriée pour l'inclusion dans l'enregistrement du schéma d'URI xmpp, car l'IANA reconnaît seulement les schémas d'URI et pas les schémas d'IRI. Donc, la syntaxe ABNF pour un URI XMPP plutôt que pour un IRI est définie comme montré au paragraphe 3.3 de ce document. Si il est nécessaire de convertir la syntaxe d'IRI en syntaxe d'URI, une application DOIT respecter la procédure de transposition spécifiée au paragraphe 3.1 de la [RFC3987].

Voici un exemple d'un IRI/URI XMPP de base utilisé pour identifier un nœud associé à un serveur XMPP :

```
xmpp:nœud@exemple.com
```

Les descriptions des divers composants d'un IRI/URI XMPP sont fournies dans les paragraphes qui suivent.

2.3 Composant d'autorité

Comme expliqué au paragraphe 2.8 de ce document, en l'absence d'un composant d'autorité, l'application traitante va s'authentifier comme un utilisateur configuré auprès d'un serveur XMPP configuré. C'est-à-dire que la section composant d'autorité n'est pas nécessaire et devrait être ignorée si l'application traitante a été configurée avec un ensemble d'accréditifs par défaut.

Conformément au paragraphe 3.2 de la [RFC3986], le composant d'autorité est précédé d'une double barre oblique ("/") et est terminée par le prochain caractère barre oblique ("/"), point d'interrogation ("?"), ou signe numéro("#") ou par la fin de l'IRI/URI. Comme expliqué plus en détails au paragraphe 2.8.1 de ce document, la présence d'un composant d'autorité signale à l'application traitante de s'authentifier comme le nœud@domaine spécifié dans le composant d'autorité plutôt que comme un nœud@domaine configuré (voir à la Section "Considérations sur la sécurité" de ce document ce qui concerne l'authentification). (Bien qu'il soit peu probable que le composant d'autorité soit inclus dans la plupart des IRI ou URI XMPP, le schéma permet cette inclusion, si elle est appropriée.) Donc, l'IRI/URI XMPP suivant indique de s'authentifier comme "guest@exemple.com" :

```
xmpp://guest@exemple.com
```

Noter bien que c'est assez différent de l'IRI/URI XMPP suivant, qui identifie un nœud "guest@exemple.com" mais ne signale pas à l'application traitante de s'authentifier comme ce nœud :

```
xmpp:guest@exemple.com
```

De même, l'utilisation d'un possible composant d'interrogation de "?message" pour déclencher l'envoi d'un message d'une interface, l'IRI/URI XMPP suivant signale à l'application traitante de s'authentifier comme "guest@exemple.com" et d'envoyer un message à "support@exemple.com" :

```
xmpp://guest@exemple.com/support@exemple.com?message
```

À l'opposé, l'IRI/URI XMPP suivant signale à l'application traitante de s'authentifier comme son compte configuré par défaut et d'envoyer un message à "support@exemple.com" :

```
xmpp:support@exemple.com?message
```

2.4 Composant de chemin

Le composant de chemin d'un IRI/URI XMPP identifie une adresse XMPP ou spécifie l'adresse XMPP à laquelle une stance XML devra être dirigée à la fin du traitement de l'IRI/URI.

Par exemple, l'IRI/URI XMPP suivant identifie un nœud associé à un serveur XMPP :

```
xmpp:exemple-nœud@exemple.com
```

L'IRI/URI XMPP suivant identifie un nœud associé à un serveur XMPP avec un identifiant de ressource XMPP particulier associé à ce nœud :

```
xmpp:exemple-nœud@exemple.com/une-ressource
```

L'inclusion d'un nœud est facultative dans les adresses XMPP, de sorte que l'IRI/URI XMPP suivant identifie simplement un serveur XMPP :

```
xmpp:exemple.com
```

2.5 Composant d'interrogation

Il y a de nombreux cas d'utilisation potentiels de l'encapsulation d'informations dans le composant d'interrogation d'un IRI/URI XMPP afin de spécifier la sémantique d'interaction suggérée (voir le paragraphe 2.1) ; les exemples incluent, mais ne se limitent pas à :

- o l'envoi d'une stance de message XMPP (voir la [RFC3921]),
- o l'ajout d'un élément répertoire (voir la [RFC3921]),
- o l'envoi d'un abonnement de présence (voir la [RFC3921]),
- o le sondage d'informations de présence actuelles (voir la [RFC3921]),
- o le déclenchement d'un appel de procédure distante (voir [XEP-0009]),
- o la découverte de l'identité ou des capacités d'une autre entité (voir [XEP-0030]),
- o la jonction à une discussion de texte fondée sur XMPP (voir [XEP-0045]),
- o l'interaction avec des canaux de publication-abonnement (voir [XEP-0060]),
- o la fourniture d'une interface SOAP (voir [XEP-0072]), et
- o l'enregistrement auprès d'une autre entité (voir [XEP-0077]).

Beaucoup de ces cas d'utilisation potentiels sont spécifiques de l'application, et la gamme complète de ces applications ne peut pas être prévue étant donnée la continuelle expansion du développement de XMPP. Cependant, il y a un consensus au sein de la communauté des développeurs Jabber/XMPP sur le fait que toutes les utilisations envisagées aujourd'hui peuvent être encapsulées via un "type query", complété facultativement par une ou plusieurs paires de "clé-valeur" (c'est similaire au type MIME "application/x-www-form-urlencoded" décrit dans [HTML]).

Par exemple, un IRI/URI XMPP destiné à lancer une interface pour l'envoi d'un message à l'entité XMPP "exemple-nœud@exemple.com" pourrait être représenté comme suit :

```
xmpp:exemple-nœud@exemple.com?message
```

De même, un IRI/URI XMPP destiné à lancer une interface pour l'envoi d'un message à l'entité XMPP "exemple-nœud@exemple.com" avec un sujet particulier pourrait être représenté comme suit :

```
xmpp:exemple-nœud@exemple.com?message;sujet=Hello%20World
```

Si l'application traitante ne comprend pas les composants d'interrogation ou le type d'interrogation spécifié, elle DOIT ignorer le composant d'interrogation et traiter l'IRI/URI comme consistant, par exemple, en <xmpp:exemple-nœud@exemple.com> plutôt que <xmpp:exemple-nœud@exemple.com?query>. Si l'application traitante ne comprend pas une clé particulière dans le composant d'interrogation, elle DOIT ignorer cette clé et sa valeur associée.

Comme on l'a noté, il existe de nombreuses sortes d'applications XMPP (actuelles et potentielles) et ces applications peuvent définir des types et clés d'interrogation à utiliser dans la portion composant d'interrogation des URI XMPP. La fonction de registre XMPP (voir [XEP-0053]) de la "XMPP Standards Foundation" tient un registre de ces types et clés d'interrogation à <<http://www.xmpp.org/registrar/querytypes.html>>. Pour aider à assurer l'interopérabilité, toute application qui utilise les formats définis dans ce document DEVRAIT soumettre tous les types et clés d'interrogation associés à ce registre en accord avec les procédures spécifiées dans [XEP-0147].

Note : le délimiteur entre paires de clé-valeur est le caractère ";" au lieu du caractère "&" utilisé dans de nombreux autres schémas d'URI. Ce délimiteur a été choisi afin d'éviter des problèmes avec l'échappement du caractère & dans les applications HTML et XML.

2.6 Composant d'identifiant de fragment

Comme indiqué au paragraphe 3.5 de la [RFC3986], "Le composant d'identifiant de fragment d'un URI permet une identification indirecte d'une ressource secondaire par référence à une ressource principale et des informations d'identification supplémentaires. "Parce que la ressource identifiée par un IRI/URI XMPP ne rend pas disponible de type de support (voir la [RFC2046]) et donc (dans la terminologie de la [RFC3986]) aucune représentation n'existe d'une ressource XMPP, la sémantique du composant d'identifiant de fragment dans les IRI/URI XMPP est à "considérer comme inconnue et, effectivement sans contrainte" (ibid.). Des applications XMPP particulières PEUVENT utiliser le composant d'identifiant de fragment à leurs propres fins. Cependant, si une application traitante ne comprend pas des composants d'identifiant de fragment ou la syntaxe d'un composant d'identifiant de fragment particulier inclus dans un IRI/URI XMPP, il DOIT ignorer le composant d'identifiant de fragment.

2.7 Génération des IRI/URI XMPP

2.7.1 Méthode de génération

Afin de former un IRI XMPP à partir d'un identifiant de nœud, identifiant de domaine, et identifiant de ressource XMPP, l'application génératrice DOIT d'abord s'assurer que l'adresse XMPP se conforme aux règles spécifiées dans la [RFC3920], incluant le codage comme chaîne UTF-8 [RFC3629] et l'application des profils stringprep pertinents [RFC3454]. Parce que la syntaxe d'IRI [RFC3987] spécifie que les caractères dans un IRI sont les caractères Unicode originaux eux-mêmes [UNICODE], quand elle génère un IRI XMPP, l'application génératrice DOIT alors décoder les caractères UTF-8 [RFC3629] d'une adresse XMPP native en leur forme Unicode originale. L'application génératrice DOIT alors enchaîner ce qui suit :

1. Le schéma "xmpp" et le caractère ":".
2. Facultativement (si un composant d'autorité est à inclure avant l'identifiant de nœud) les caractères "/", un composant d'autorité de la forme nœud@domaine, et le caractère "/".
3. Facultativement (si l'adresse XMPP contenait un "identifiant de nœud" XMPP) une chaîne de caractères Unicode qui se conforme à la règle "inodid", suivie par le caractère "@".
4. Une chaîne de caractères Unicode qui se conforme à la règle "ihost".
5. Facultativement (si l'adresse XMPP contenait un "identifiant de ressource" XMPP) le caractère "/" et une chaîne de caractères Unicode qui se conforme à la règle "iresid".
6. Facultativement (si un composant d'interrogation doit être inclus) le caractère "?" et un composant d'interrogation.
7. Facultativement (si un composant d'identifiant de fragment doit être inclus) le caractère "#" et le composant d'identifiant de fragment.

Pour former un URI XMPP à partir de l'IRI résultant, une application DOIT respecter la procédure de transposition spécifiée au paragraphe 3.1 de la [RFC3987].

2.7.2 Notes sur la génération

Certains caractères sont permis dans les portions identifiant de nœud, identifiant de domaine, et identifiant de ressource d'une adresse XMPP native mais interdits par les règles "inodid", "ihost", et "iresid" d'un IRI XMPP. Spécifiquement, les caractères "#" et "?" sont permis dans les identifiants de nœud, et les caractères "/", "?", "#", et "@" sont permis dans les identifiants de ressource, mais ces caractères sont utilisés comme délimiteurs dans les IRI XMPP. De plus, le caractère " " (espace US-ASCII) est permis dans les identifiants de ressource mais interdit dans les IRI. Donc, tous les caractères ci-dessus DOIVENT être codés en pourcentage quand on transforme une adresse XMPP en IRI XMPP.

Considérons le nœud maléfisant suivant dans une adresse XMPP :

```
maléfisant!#$%()*+,-.:=?[ \^`'{}~nœud@exemple.com
```

Cette adresse serait transformée en l'IRI XMPP suivant :

```
xmpp:maléfisant!%23$%25()*+,-.:=%3F%5B%5C%5D%5E_%60%7B%7C%7D~nœud@exemple.com
```

Considérons la ressource repoussante suivante dans une adresse XMPP :

nœud@exemple.com/repoussante !#"\$\$%&'()*+,-./:;<=>?@[\\]^_`{|}~ressource

Cette adresse serait transformée en l'IRI XMPP suivant (présenté sur deux lignes aux fins d'affichage) :

xmpp:nœud@exemple.com/repoussante%20!%23%22\$%25&'()*+,-.%2F:;%3C=%3E%3F%40%5B%5C%5D%5E_%60%7B%7C%7D~ressource

De plus, virtuellement tout caractère en dehors de la gamme US-ASCII [US-ASCII] est permis dans une adresse XMPP et donc aussi dans un IRI XMPP, mais la syntaxe d'URI interdit ces caractères directement et spécifie qu'ils DOIVENT être codés en pourcentage. Pour déterminer l'URI associé à un IRI XMPP, une application DOIT respecter la procédure de transposition spécifiée au paragraphe 3.1 de la [RFC3987].

Le tableau suivant peut aider les mises en œuvre à comprendre les codages respectifs et "les unités porteuses" des identifiants discutés dans ce document, à savoir : (1) les adresses XMPP natives, (2) les IRI, et (3) les URI. Pour les détails, voir le paragraphe 3.5 de ce document ainsi que la Section 3 de la [RFC3920], le paragraphe 6.4 de la [RFC3987], et la Section 2 de la [RFC3986].

Identifiant	Codage	Unités
adresse XMPP	UTF-8	octets
IRI	Unicode	valeurs de 16/32 bits
URI	UTF-8 codé en pourcentage	US-ASCII

2.7.3 Exemple de génération

Considérons l'adresse XMPP suivante : <jiři@čechy.exemple/v Prazе>

Note : la chaîne "ř" indique le caractère Unicode LATIN SMALL LETTER R WITH CARON, et la chaîne "č" indique le caractère Unicode LATIN SMALL LETTER C WITH CARON. La forme "&#x..." est utilisée dans ce document comme appareil notationnel pour représenter les caractères Unicode, suivant la "Notation XML" utilisée dans la [RFC3987] pour représenter des caractères qui ne peuvent pas être rendus dans des documents seulement ASCII. Un IRI XMPP DOIT contenir les caractères Unicode eux-mêmes, et non leur représentation en notation XML (en particulier, noter que le caractère "#" est interdit dans la syntaxe d'IRI). Un URI XMPP DOIT échapper convenablement de tels caractères, comme décrit ci-dessous. Les caractères '<' et '>' ne font pas partie de l'adresse elle-même mais sont fournis pour délimiter l'adresse de façon lisible. (Pour ceux qui ne comprennent pas le tchèque, cet exemple pourrait être francisé en "george@czech-ville.exemple/à Prague".)

En accord avec le processus spécifié ci-dessus, l'application génératrice serait ce qui suit pour générer un IRI XMPP valide à partir de cette adresse :

1. S'assurer que l'adresse XMPP se conforme aux règles spécifiées dans la [RFC3920], incluant l'application des profils stringprep pertinents [RFC3454] et le codage comme chaîne UTF-8 [RFC3629].
2. Enchaîner ce qui suit :
 1. Le schéma "xmpp" et le caractère ":".
 2. Un "composant d'autorité" si inclus (non montré dans cet exemple).
 3. Une chaîne de caractères Unicode qui représente l'adresse XMPP, transformée en accord avec les règles "inodid", "ihost", et "iresid".
 4. Le caractère "?" suivi par un "composant d'interrogation" si c'est approprié pour l'application (non montré).
 5. Le caractère "#" suivi par un "composant d'identifiant de fragment" si c'est approprié pour l'application (non montré).

Le résultat est l'IRI XMPP suivant (noter encore que, en accord avec la "Notation XML" utilisée dans la [RFC3987], la chaîne "ř" indique le caractère Unicode LATIN SMALL LETTER R WITH CARON et la chaîne "č" indique le caractère Unicode LATIN SMALL LETTER C WITH CARON ; un IRI XMPP contiendrait les caractères Unicode eux-mêmes).

<xmpp:jiři@čechy.exemple/v%20Prazе>

Afin de générer un URI XMPP valide pour l'IRI ci-dessus, l'application DOIT respecter la procédure spécifiée au paragraphe 3.1 de la [RFC3987], résultant en l'URI suivant :

<xmpp:ji%C5%99i@%C4%8Dechy.exemple/v%20Prazе>

2.8 Traitement des IRI/URI XMPP

2.8.1 Méthode de traitement

Si un URI XMPP et non un IRI XMPP est présenté à une application traitante, elle DOIT d'abord convertir l'URI en IRI en suivant la procédure spécifiée au paragraphe 3.2 de la [RFC3987].

Afin de décomposer un IRI XMPP pour interaction avec l'entité qu'il identifie, une application traitante DOIT séparer :

1. Le schéma "xmpp" et le caractère ":".
2. Le composant d'autorité, si il est inclus (la chaîne de caractères Unicode entre les caractères "/" et le prochain caractère "/", "?", "#", ou la fin de l'IRI).
3. Une chaîne de caractères Unicode qui représente une adresse XMPP comme transformée en accord avec les règles "inodeid", "ihost", et "iresid".
4. Facultativement le composant d'interrogation, si il est inclus, en utilisant le caractère "?" comme séparateur.
5. Facultativement le composant d'identifiant de fragment, si il est inclus, en utilisant le caractère "#" comme séparateur.

À ce point, l'application traitante DOIT s'assurer que l'adresse XMPP résultante se conforme aux règles spécifiées dans la [RFC3920], incluant l'application des profils stringprep pertinents [RFC3454]. L'application traitante va alors soit (1) compléter elle-même le traitement XMPP, soit (2) invoquer une application d'aide pour compléter le traitement XMPP ; un tel traitement XMPP va très probablement consister en les étapes suivantes :

1. Si elle n'est pas déjà connectée à un serveur XMPP, se connecter soit comme l'utilisateur spécifié dans le composant d'autorité, soit comme l'utilisateur configuré auprès du serveur XMPP configuré, normalement en respectant les procédures de connexion à XMPP définies dans la [RFC3920]. (Note : l'application traitante DEVRAIT ignorer le composant d'autorité si il a été configuré avec un ensemble d'accréditifs par défaut.)
2. Facultativement, déterminer la nature du receveur prévu (par exemple, via [XEP-0030]).
3. Facultativement, présenter une interface appropriée à un utilisateur sur la base de la nature du receveur prévu et/ou du contenu du composant d'interrogation.
4. Générer une stance XMPP qui traduise toutes les entrées d'utilisateur ou d'application en leurs équivalents XMPP correspondants.
5. Envoyer la stance XMPP via la connexion de serveur authentifiée pour livraison au receveur prévu.

2.8.2 Notes sur le traitement

Il peut aider les mises en œuvre de noter que les deux premières étapes de la "suite du traitement XMPP", comme décrit à la fin du paragraphe 2.8.1, sont similaires à l'authentification HTTP [RFC2617], tandis que les trois étapes suivantes sont similaires au traitement des URI mailto: [RFC2368].

Comme noté au paragraphe 2.7.2 de ce document, certains caractères sont permis dans les portions identifiant de nœud, identifiant de domaine, et identifiant de ressource d'une adresse XMPP native mais interdits par les règles "inodeid", "ihost", et "iresid" d'un IRI XMPP. Les octets codés en pourcentage correspondant à ces caractères dans les IRI XMPP DOIVENT être transformés en les caractères permis dans les adresses XMPP lors du traitement d'un IRI XMPP pour interaction avec l'entité XMPP représentée.

Considérons le vilain nœud suivant dans un IRI XMPP :

```
xmpp:vilain!%23$%25()*+,-.:=%3F%5B%5C%5D%5E_%60%7B%7C%7D~nœud@exemple.com
```

Cet IRI serait transformé en l'adresse XMPP suivante :

```
vilain!#$%()*+,-.:=?[\\^_`{}~nœud@exemple.com
```

Considérons la ressource repoussante suivante dans un IRI XMPP (mis sur deux lignes pour la lisibilité) :

```
xmpp:nœud@exemple.com/repoussante%20!%23%22$%25&'()*+,-.%2F;%3C
=%3E%3F%40%5B%5C%5D%5E_%60%7B%7C%7D~ressource
```

Cet IRI serait transformé en l'adresse XMPP suivante :

nœud@exemple.com/repoussante!#\$%&'()*+,-./:;<=>@[\\]^_`{|}~ressource

2.8.3 Exemple de traitement

Considérons l'URI XMPP qui résultait de l'exemple précédent (voir le paragraphe 2.7.3) :

```
<xmpp:ji%C5%99i@%C4%8Dechy.exemple/v%20Praze>
```

Afin de générer un IRI XMPP valide à partir de cet URI, l'application DOIT respecter la procédure spécifiée au paragraphe 3.2 de la [RFC3987], résultant en l'IRI suivant :

```
<xmpp:ji&#x159;i@&#x10D;echy.exemple/v%20Praze>
```

En accord avec le processus spécifié ci-dessus, l'application traitante va supprimer le schéma "xmpp" et le caractère ":" pour extraire l'adresse XMPP de cet IRI XMPP, convertissant tout octet codé en pourcentage à partir des règles "inodeid", "ihost", et "iresid" en leurs caractères équivalents (par exemple, "%20" en le caractère espace).

Le résultat est cette adresse XMPP :

```
<ji&#x159;i@&#x10D;echy.exemple/v Praze>
```

2.9 Internationalisation

Parce que les adresses XMPP sont des chaînes UTF-8 [RFC3629] et parce que les octets en dehors de la gamme US-ASCII [US-ASCII] au sein des adresses XMPP peuvent être facilement convertis en octets codés en pourcentage, les adresses XMPP sont conçues pour bien fonctionner avec les identifiants de ressource internationalisés [RFC3987]. En particulier, à l'exception de la vérification stringprep, la conversion de caractères US-ASCII pertinents pour la syntaxe (par exemple, "?") et la conversion d'octets codés en pourcentage à partir des règles "inodeid", "ihost", et "iresid" en leurs caractères équivalents (par exemple, "%20" en le caractère US-ASCII espace) un IRI XMPP peut être construit directement en ajoutant devant une adresse XMPP le schéma "xmpp" et le caractère ":". De plus, un IRI XMPP peut être converti en syntaxe d'URI en respectant la procédure spécifiée au paragraphe 3.1 de la [RFC3987], et un URI XMPP peut être converti en syntaxe d'IRI en respectant la procédure spécifiée au paragraphe 3.2 de la [RFC3987], assurant donc l'interopérabilité avec les applications qui sont capables de traiter les URI mais incapables de traiter les IRI.

3. Enregistrement par l'IANA du schéma d'URI xmpp

En accord avec la [RFC4395], cette section donne les informations requises pour enregistrer le schéma d'URI xmpp.

3.1 Nom du schéma d'URI

xmpp

3.2 Statut

Permanent

3.3 Syntaxe du schéma d'URI

La syntaxe pour un URI xmpp est définie ci-dessous en utilisant la forme Backus-Naur augmentée comme spécifié par la [RFC5234], où les règles "fragment", "host", "pct-encoded", et "unreserved" sont définies dans la [RFC3986] :

```
xmppuri = "xmpp" ":" hierxmpp [ "?" querycomp ] [ "#" fragment ]
hierxmpp = authpath / pathxmpp
authpath = "/" authxmpp [ "/" pathxmpp ]
authxmpp = nœudid "@" host
pathxmpp = [ nodeid "@" ] host [ "/" resid ]
nodeid = *( unreserved / pct-encoded / nodeallow )
nodeallow = "!" / "$" / "(" / ")" / "*" / "+" / "," / ";" / "="
```

```

resid = *( unreserved / pct-encoded / resallow )
resallow = "!"/"$"/"&"/""/"("/)" / "*" / "+" / "," / ":" / ";" / "="
querycomp = querytype [ *pair ]
querytype = *( unreserved / pct-encoded )
pair = ";" key "=" value
key = *( unreserved / pct-encoded )
value = *( unreserved / pct-encoded )

```

3.4 Sémantique du schéma d'URI

Le schéma d'URI xmpp identifie des entités qui communiquent de façon native en utilisant le protocole extensible de messagerie et de présence (XMPP, *Extensible Messaging et Presence Protocol*) et est principalement utilisé pour l'identification plutôt que pour la localisation de ressource. Cependant, si une application qui traite un URI xmpp permet une interaction avec l'adresse XMPP identifiée par l'URI, elle DOIT suivre la méthodologie définie à la Section 2 du présent document, utiliser les IRI et URI XMPP, reconstruire l'adresse XMPP encapsulée, se connecter à un serveur XMPP approprié, et envoyer une "stance" XMPP (fragment XML) appropriée à l'adresse XMPP. (Note : aucun type MIME n'est associé au schéma d'URI xmpp.)

3.5 Considérations de codage

En plus des URI XMPP, il y a aussi des identifiants de ressource internationalisée (IRI) XMPP. Avant de convertir une adresse XMPP en IRI (et en accord avec la [RFC3920]) l'adresse XMPP doit être représentée comme une chaîne de caractères UTF-8 [RFC3629] par l'application génératrice (par exemple, en transformant la représentation interne d'une application de l'adresse comme chaîne UTF-16 en chaîne UTF-8). Parce que la syntaxe d'IRI [RFC3987] spécifie que les caractères dans un IRI sont les caractères Unicode originaux eux-mêmes [UNICODE], quand elle génère un IRI XMPP, l'application génératrice DOIT décoder les caractères UTF-8 d'une adresse XMPP native en leur forme Unicode originale. Parce que la syntaxe d'URI [RFC3986] spécifie que les caractères dans un URI sont seulement des caractères US-ASCII [US-ASCII], quand elle génère un URI XMPP, l'application génératrice DOIT échapper les caractères Unicode d'un IRI XMPP en caractères US-ASCII en respectant la procédure spécifiée dans la [RFC3987].

3.6 Applications/protocoles qui utilisent ce nom de schéma d'URI

Le schéma d'URI xmpp est destiné à être utilisé par des interfaces à un réseau XMPP provenant d'agents d'utilisateur non natifs, comme des navigateurs de la Toile, ainsi que par des applications non natives qui ont besoin d'identifier des entités XMPP comme URI ou IRI complets.

3.7 Considérations d'interopérabilité

Il n'y a pas de problème d'interopérabilité connu en rapport avec l'utilisation du schéma d'URI xmpp. Afin d'aider à assurer l'interopérabilité, la fonction de registraire XMPP de la "XMPP Standards Foundation" tient un registre des types et clés d'interrogation qui peut être utilisé dans les composants d'interrogation des URI et IRI XMPP, situé à <http://www.xmpp.org/registrar/querytypes.html>.

3.8 Considérations sur la sécurité

Voir la Section 5 du présent document, Considérations sur la sécurité.

3.9 Contact

Peter Saint-Andre [mailto:stpeter@jabber.org, xmpp:stpeter@jabber.org]

3.10 Auteur/contrôleur des changements

Ce schéma est enregistré sous l'arborescence de l'IETF. À ce titre, l'IETF contrôle les changements.

3.11 Références

[RFC3920]

4. Considérations relatives à l'IANA

Le présent document rend obsolète l'enregistrement de schéma d'URI créé par la RFC 4622. Le gabarit d'enregistrement se trouve à la Section 3 du présent document. Afin d'aider à assurer l'interopérabilité, la fonction de registraire XMPP de la "XMPP Standards Foundation" tient un registre des types et clés d'interrogation qui peut être utilisé dans les composants d'interrogation des URI et IRI XMPP, situé à <<http://www.xmpp.org/registrar/querytypes.html>>.

5. Considérations sur la sécurité

Fournir une interface aux services XMPP à partir d'applications non natives n'introduit pas de nouveau problème de sécurité. Les considérations sur la sécurité discutées dans les [RFC3987], [RFC3986], et [RFC3920] s'appliquent aux IRI XMPP, et les considérations sur la sécurité discutées dans les [RFC3986] et [RFC3920] s'appliquent aux URI XMPP. Conformément au paragraphe 2.7 de la [RFC4395] et à la Section 7 de la [RFC3986], des considérations sur la sécurité particulières sont spécifiées dans les paragraphes qui suivent.

5.1 Fiabilité et cohérence

Étant donné que les adresses XMPP de forme `nœud@domaine.tld` sont normalement créées via l'enregistrement auprès d'un serveur XMPP ou provisionnées par un administrateur d'un tel serveur, il est possible que de telles adresses soient aussi désenregistrées ou déprovisionnées. Donc, l'IRI/URI XMPP qui identifie une telle adresse XMPP ne peut être associé de façon fiable et cohérente au même principal, propriétaire de compte, application, ou appareil.

Les adresses XMPP de la forme `nœud@domaine.tld/ressource` sont normalement encore plus éphémères (car un identifiant de ressource XMPP donné est normalement associé à une session temporaire particulière d'un client XMPP chez un serveur XMPP). Donc, l'IRI/URI XMPP qui identifie une telle adresse XMPP ne va probablement pas être associé de façon fiable et cohérente à la même session. Cependant, les procédures spécifiées à la Section 10 de la [RFC3920] éliminent effectivement toute confusion potentielle qui pourrait être introduite par le manque de fiabilité et cohérence de l'IRI/URI XMPP qui identifie une telle adresse XMPP.

Les adresses XMPP de la forme `domaine.tld` sont normalement des serveurs XMPP ou services associés à longue durée de vie. Bien que naturellement il soit possible aux administrateurs de serveur ou service de décommissionner le serveur ou service à tout moment, normalement les IRI/URI qui identifient ces serveurs ou services sont les plus fiables et cohérents des IRI/URI XMPP.

Les adresses XMPP de la forme `domaine.tld/ressource` ne sont pas encore courantes sur les réseaux XMPP ; cependant, la fiabilité et la cohérence des IRI/URI XMPP qui identifient de telles adresses XMPP vont probablement se situer quelque part entre celles qui identifient les adresses XMPP de la forme `domaine.tld` et celles qui identifient les adresses XMPP de la forme `nœud@domaine.tld`.

5.2 Construction malveillante

La construction malveillante des IRI/URI XMPP est rendue moins probable par l'interdiction des numéros d'accès dans les IRI/URI XMPP (car les numéros d'accès sont à découvrir en utilisant les enregistrements SRV du DNS [RFC2782], comme spécifié dans la [RFC3920]).

5.3 Transcodage d'extrémité arrière

Parce que le protocole de base XMPP est conçu pour mettre en œuvre l'échange de messages et d'informations de présence et non la restitution de fichiers ou l'invocation de fonctions système similaires, il est réputé peu probable que l'utilisation des IRI/URI XMPP résulte en dérèfèrencement dommageable. Cependant, si une extension du protocole XMPP définit des méthodes pour la restitution d'informations, elle DOIT définir les contrôles appropriés sur l'accès à ces informations. De plus, les serveurs XMPP NE DEVRAIENT PAS analyser d'eux-mêmes les IRI/URI XMPP mais plutôt DEVRAIENT accepter seulement le protocole réseau XML spécifié dans la [RFC3920] et toutes extensions qui y sont désirées.

5.4 Informations sensibles

La capacité d'interagir avec les entités XMPP via un navigateur de la Toile ou autre application non native peut exposer des informations sensibles (comme un support d'extensions de protocole d'application XMPP particulières) et par là rendre

possible le lancement d'attaques qui ne sont pas possibles ou peu probables sur un réseau XMPP natif. La décision de quelle information est appropriée pour la représentation dans les IRI ou URI XMPP doit être murement réfléchie.

En particulier, l'annonce des IRI/URI XMPP dans des localisations publiquement accessibles (par exemple, sur des sites de la Toile) peut faciliter à des utilisateurs malveillants la collecte d'adresses XMPP auprès des composants d'autorité et de chemin des IRI/URI XMPP et donc d'envoyer des communications en vrac non sollicitées aux utilisateurs ou applications représentées par ces adresses. La mise en balance des avantages d'un échange d'informations ouvert par rapport aux coûts potentiels de communications ne devrait pas être faite à la légère.

Pour aider à empêcher la fuite d'informations sensibles, les mots de passe et autres accreditifs d'utilisateur sont interdits dans le composant d'autorité des IRI/URI XMPP ; en fait ils ne sont pas nécessaires, car l'authentification dans XMPP se fait via l'authentification simple et couche de sécurité (SASL, *Simple Authentication et Security Layer*) [RFC4422] et rend possible l'utilisation du mécanisme SASL ANONYMOUS, si désiré.

5.5 Attaques sémantiques

En dépit de l'existence de schémas d'URI non hiérarchiques tels que de la [RFC2368], par association les utilisateurs humains peuvent s'attendre à ce que tous les URI incluent les caractères "/" après le nom de schéma et le caractère ":". Cependant, dans les IRI/URI XMPP, les caractères "/" précèdent le composant d'autorité plutôt que le composant de chemin. Donc, `xmpp://guest@exemple.com` indique de s'authentifier comme "guest@exemple.com", tandis que `xmpp:guest@exemple.com` identifie le nœud "guest@exemple.com". Les applications traitantes DOIVENT clairement différencier ces formes, et les agents d'utilisateur DEVRAIENT déconseiller aux utilisateurs humains d'inclure les caractères "/" dans les IRI/URI XMPP dans la mesure où l'utilisation du composant d'autorité n'est utile que dans des scénarios spécialisés, et non pas de façon générale.

5.6 Tromperie

La capacité à inclure effectivement la gamme complète des caractères Unicode dans un IRI XMPP peut rendre plus facile l'exécution de certaines formes d'imitation d'adresse (aussi appelé "usurpation"). Cependant, les IRI XMPP ne sont pas différents des autres IRI à cet égard, et les applications qui vont présenter des IRI XMPP aux utilisateurs humains doivent respecter les bonnes pratiques concernant l'imitation d'adresse afin d'aider à empêcher ces attaques qui résultent d'adresses usurpées (par exemple, le phénomène connu comme "hameçonnage"). Pour les détails, se reporter aux considérations sur la sécurité de la [RFC3987].

6. Remerciements

Merci à Martin Duerst, Lisa Dusseault, Frank Ellerman, Roy Fielding, Joe Hildebrand, et Ralph Meijer de leurs commentaires.

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](#))
- [RFC3920] P. Saint-Andre, éd., "[Protocole extensible de messagerie](#) et de présence (XMPP) : éléments centraux", octobre 2004. (P.S.) (Remplacée par [RFC6120](#))
- [RFC3986] T. Berners-Lee, R. Fielding et L. Masinter, "[Identifiant de ressource uniforme](#) (URI) : Syntaxe générique", STD 66, janvier 2005. (P.S. ; MàJ par [RFC8820](#))
- [RFC3987] M. Duerst et M. Suignard, "[Identifiant de ressource internationalisé](#) (IRI)", janvier 2005.
- [RFC5234] D. Crocker, P. Overell, "[BNF augmenté pour les spécifications de syntaxe](#) : ABNF", janvier 2008. ([STD0068](#))

7.2 Références pour information

- [HTML] Raggett, D., "HTML 4.0 Specification", W3C REC REC- html40-19980424, avril 1998.
- [RFC2046] N. Freed et N. Borenstein, "[Extensions de messagerie Internet](#) multi-objets (MIME) Partie 2 : Types de support", novembre 1996. (*D. S., MàJ par [2646](#), [3798](#), [5147](#), [6657](#), [8098](#)*)
- [RFC2368] P. Hoffman, L. Masinter, J. Zawinski, "Le schéma d'URL mailto", juillet 1998. (*P.S.) (Obsolète, voir la [RFC6068](#)*)
- [RFC2617] J. Franks et autres, "Authentification HTTP : [Authentification d'accès de base et par résumé](#)", juin 1999. (*DS.*)
- [RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la [localisation des services](#) (DNS SRV)", février 2000.
- [RFC3454] P. Hoffman et M. Blanchet, "[Préparation de chaînes internationalisées](#) ("stringprep")", décembre 2002. (*P.S.*)
- [RFC3490] P. Faltstrom et autres, "Internationalisation des noms de domaine dans les applications (IDNA)", mars 2003. (*Remplacée par les RFC[5890](#) et [5891](#), P.S.*)
- [RFC3629] F. Yergeau, "[UTF-8, un format de transformation](#) de la norme ISO 10646", STD 63, novembre 2003.
- [RFC3859] J. Peterson, "[Profil commun pour les services de présence](#) (CPP)", août 2004. (*P.S.*)
- [RFC3860] J. Peterson, "[Profil commun pour la messagerie instantanée](#) (CPIM)", août 2004. (*P.S.*)
- [RFC3921] P. Saint-Andre, éd., "Protocole extensible de messagerie et de présence (XMPP) : [messagerie instantanée et présence](#)", octobre 2004. (*P.S.) (Remplacée par RFC[6121](#)*)
- [RFC4395] T. Hansen et autres, "Lignes directrices et procédures d'enregistrement pour les nouveaux schémas d'URI", février 2006. (*Remplace [RFC2717](#), [RFC2718](#) ([BCP0115](#))*)
- [RFC4422] A. Melnikov et K. Zeilenga, éd., "[Authentification simple et couche de sécurité](#) (SASL)", juin 2006. (*P.S.*)
- [UNICODE] The Unicode Consortium, "The Unicode Standard, Version 3.2.0", 2000.
La norme Unicode, version 3.2.0 est définie par sa version 3.0 (Reading, MA, Addison-Wesley, 2000, ISBN 0-201-61633-5) telle qu'amendée par l'annexe n° 27 : Unicode 3.1 (<http://www.unicode.org/reports/tr27/>) et l'annexe n° 28 : Unicode 3.2 (<http://www.unicode.org/reports/tr28/>).
- [US-ASCII] American National Standards Institute, "Coded Character Set - 7-bit American Standard Code for Information Interchange", ANSI X3.4, 1986.
- [XEP-0009] Adams, D., "Jabber-RPC", XSF XEP 0009, février 2006.
- [XEP-0030] Hildebrand, J., Millard, P., Eatmon, R., et P. Saint-Andre, "Service Discovery", XSF XEP 0030, février 2007.
- [XEP-0045] Saint-Andre, P., "Multi-User Chat", XSF XEP 0045, avril 2007.
- [XEP-0053] Saint-Andre, P., "XMPP Registrar Function", XSF XEP 0053, décembre 2006.
- [XEP-0060] Millard, P., Saint-Andre, P., et R. Meijer, "Publish-Subscribe", XSF XEP 0060, septembre 2006.
- [XEP-0072] Forno, F. et P. Saint-Andre, "SOAP Over XMPP", XSF XEP 0072, décembre 2005.
- [XEP-0077] Saint-Andre, P., "In-Band Registration", XSF XEP 0077, janvier 2006.
- [XEP-0147] Saint-Andre, P., "XMPP URI Scheme Query Components", XSF XEP 0147, septembre 2006.

Appendice A. Différences avec la RFC 4622

Plusieurs erreurs ont été trouvées dans la RFC 4622. Le présent document corrige ces erreurs. Les différences en résultant sont les suivantes :

- o On spécifie que les caractères "[", "\", "]", "^", "'", "{", "|", et "}" sont permis dans les identifiants de nœud XMPP mais pas dans les IRI ou URI en accord avec la règle sub-delims.
- o On spécifie que les caractères '"', "<", ">", "[", "\", "]", "^", "'", "{", "|", et "}" sont permis dans les identifiants de ressource XMPP mais ne le sont pas dans les IRI ou URI en accord avec la règle pchar.
- o On spécifie que es caractères ci-dessus doivent être codés en pourcentage dans la construction d'un URI XMPP.
- o L'ABNF a été corrigé en conséquence.
- o Les exemples ont été mis à jour en conséquence.

Appendice B. Conditions de copie

Concernant ce document entier ou toute portion de celui-ci, l'auteur ne donne aucune garantie et ne peut être tenu pour responsable d'aucun dommage résultant de son utilisation. L'auteur accorde la permission irrévocable à quiconque de l'utiliser, modifier, et distribuer de toute façon qui ne diminue pas les droits de tout autre de l'utiliser, modifier, et distribuer, pourvu que les travaux dérivés redistribués ne contiennent pas d'information d'auteur ou de version trompeuses. Les travaux dérivés n'ont pas besoin d'être licenciés sous des termes similaires.

Adresse de l'auteur

Peter Saint-Andre
XMPP Standards Foundation

mél : stpeter@jabber.org

URI : <xmpp:stpeter@jabber.org>

Déclaration complète de droits de reproduction

Copyright (C) The IETF Trust (2008).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

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

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

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