Groupe de travail Réseau
Request for Comments : 4314
RFC rendue obsolète : 2086
Catégorie : Sur la voie de la normalisation

A. Melnikov, Isode Ltd.
décembre 2005

Traduction Claude Brière de L'Isle

Extension Liste de contrôle d'accès (ACL) à IMAP4

Résumé
L'extension Liste de contrôle d'accès (ACL, *Access Control List*) (RFC2086) du protocole d'accès au message Internet (IMAP, *Internet Message Access Protocol*) permet de restituer et manipuler les listes de contrôle d'accès de boîtes aux lettres à l'aide du protocole IMAP.

Le présent document est une révision de la RFC 2086. Il définit plusieurs nouveaux droits de contrôle d'accès et précise quels droits sont exigés pour différentes commandes IMAP.

Table des matières

1. Introduction et généralités

L'extension ACL (liste de contrôle d'accès) du protocole d'accès au message Internet (IMAP4) [RFC3501] permet que les listes de contrôle d'accès aux boîtes aux lettres soient restituées et manipulées avec le protocole IMAP.

Le présent document est une révision de la [RFC2086]. Il essaye de préciser différentes ambiguïtés de la RFC 2086, en particulier, l'utilisation de UTF-8 [RFC3629] dans les identifiants d'accès, les droits exigés pour les différentes commandes IMAP4, et comment les codes de réponse READ-WRITE/READ-ONLY sont en relation avec ACL.

1.1 Conventions utilisées dans le document

Dans les exemples, "C:" et "S:" indiquent les lignes envoyées respectivement par le client et le serveur.

Dans tous les exemples, le caractère "/" est utilisé comme séparateur hiérarchique.

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].

La phrase "serveur ACL" est juste un raccourci pour dire "le serveur IMAP qui prend en charge l'extension ACL telle que définie dans le présent document".

2. Contrôle d'accès

L'extension ACL est présente dans toute mise en œuvre de IMAP4 qui retourne "ACL" dans les capacités prises en charge à la commande CAPABILITY.

Une mise en œuvre de serveur conforme au présent document DOIT aussi retourner des droits (voir ci-dessous) non définis au paragraphe 2.2 dans la capacité "RIGHTS=".

Une liste de contrôle d'accès est un ensemble de paires de <identifiants d'accès, droits>. Une ACL s'applique à un nom de boîte aux lettres.

Un identifiant d'accès (ou juste "identifiant") est une chaîne UTF-8 [RFC3629]. L'identifiant "tous" *(anyone)* est réservé pour se référer à l'identité universelle (toutes les authentifications, incluant les anonymes). Toutes les chaînes de nom d'utilisateur acceptée par les commandes LOGIN ou AUTHENTICATE pour authentifier le serveur IMAP sont réservées comme identifiants pour les utilisateurs correspondants. Les identifiants qui commencent par un tiret ("-") sont réservés pour les "droits négatifs", décrits ci dessous. Toutes les autres chaînes d'identifiant sont interprétées d'une façon qui est définie par la mise en œuvre.

Droits est une chaîne qui fait la liste (éventuellement vide) d'un ensemble de caractères alphanumériques, dont chacun fait la liste d'un ensemble d'opérations qui sont contrôlées. Les lettres minuscules sont réservées aux droits "standard" dont la liste figure au paragraphe 2.1. (Noter que pour la compatibilité avec les clients et serveurs déployés, les droits en majuscules ne sont pas permis.) L'ensemble des droits standard ne peut être étendu que par un document sur la voie de la normalisation. Les chiffres sont réservés aux droits définis par une mise en œuvre ou site.

Une mise en œuvre PEUT lier ensemble des droits ou PEUT forcer des droits à être toujours ou jamais accordés à des identifiants particuliers. Par exemple, dans une mise en œuvre qui utilise les bits de mode UNIX, les droits "swite" sont liés, le droit "a" est toujours accordé au propriétaires d'une boîte aux lettres, et jamais accordé à un autre utilisateur. Si les droits sont liés dans une mise en œuvre, celle ci doit être prudente dans l'octroi de droits en réponse à des commandes SETACL -- sauf si tous les droits dans un ensemble lié sont spécifiés, aucun droit de cet ensemble ne devrait être inclus dans l'entrée d'ACL pour cet identifiant. Un client peut découvrir l'ensemble des droits qui peuvent être accordés à un certain identifiant dans l'ACL pour un certain nom de boîte aux lettres en utilisant la commande LISTRIGHTS.

Il est possible que plusieurs identifiants dans une liste de contrôle d'accès s'appliquent à un certain utilisateur. Par exemple, une ACL peut inclure des droits à accorder à l'identifiant qui correspond à l'utilisateur, à un ou plusieurs identifiants définis par la mise en œuvre correspondants aux groupes qui incluent l'utilisateur, et/ou l'identifiant "tous". Comment ces droits

sont combinés pour déterminer l'accès de l'utilisateur est défini par la mise en œuvre. Une mise en œuvre peut choisir, par exemple, d'utiliser l'union des droits accordés aux identifiants applicables. Une mise en œuvre peut à la place choisir, par exemple, d'utiliser seulement les droits accordés à l'identifiant le plus spécifique présent dans l'ACL. Un client peut déterminer l'ensemble de droits accordés à l'utilisateur enregistré pour un certain nom de boîte aux lettres en utilisant la commande MYRIGHTS.

Quand un identifiant dans une ACL commence par un tiret ("-"), cela indique que les droits associés sont à retirer de l'identifiant qui a le tiret en préfixe. C'est ce qu'on appelle un "droit négatif". Cela diffère de DELETEACL en ce que un droit négatif est ajouté à l'ACL et fait partie du calcul des droits.

Supposons qu'un identifiant "fred" se réfère à un utilisateur dont le nom de connexion est "fred". Si le droit "w" est accordé à l'identifiant "-fred", cela indique que le droit "w" est à retirer des utilisateurs qui correspondent à l'identifiant "fred", bien que l'utilisateur "fred" puisse avoir le droit "w" par suite de quelque autre identifiant dans l'ACL. Une DELETEACL de "fred" supprime simplement l'identifiant "fred" de l'ACL ; elle n'affecte aucun des droits que l'utilisateur "fred" pourrait obtenir d'une autre entrée dans l'ACL, en particulier, elle n'affecte pas les droits accordés à l'identifiant "-fred".

Les mises en œuvre de serveur ne sont pas obligées de prendre en charge les identifiants de "droit négatif".

2.1 Droits standard

Les droits standard actuellement définis sont (noter que la liste ci-dessous ne donne pas toutes les commandes qui utilisent un droit particulier) :

l - recherche (la boîte aux lettres est visible pour les commandes LIST/LSUB, SOUSCRIT à la boîte aux lettres)
r - lire (CHOISIT la boîte aux lettres, effectue STATUS)
s - garde les informations vues/non vues à travers les sessions (établit ou supprime le fanion \VU via MÉMORISER, établit aussi VU durant AJOUTE/COPIE/ALLER CHERCHER LE CORPS[...])
w - écrire (établit ou supprime les fanions autres que \VU et \SUPPRIMÉ via MÉMORISER, les établit aussi durant AJOUTE/COPIE)
i - insérer (effectue AJOUTE/COPIE dans la boîte aux lettres)
p - envoyer (envoie la messagerie à l'adresse de soumission pour les boîtes aux lettres, non appliqué par IMAP4 lui-même)
k - crée des boîtes aux lettres (CRÉE de nouvelles sous boîtes aux lettres dans toute hiérarchie définie par la mise en œuvre, la boîte au lettres parente pour le nom de la nouvelle boîte aux lettres dans RENOMME)
x - supprime la boite aux lettres (SUPPRIME la boîte aux lettres, le nom de la vieille boîte aux lettres dans RENOMME)
t - supprime les messages (établit ou supprime le fanion \SUPPRIMÉ via MÉMORISER, établit le fanion \SUPPRIMÉ durant AJOUTE/COPIE)
e - effectue PURGE et purge au titre de CLOTURE
a - administre (effectue SETACL/DELETEACL/GETACL/LISTRIGHTS)

2.1.1 Droits obsolètes

Du fait d'une ambiguïté de la RFC 2086, certaines mises en œuvre existantes de serveur utilisent le droit "c" pour contrôler la commande DELETE. D'autres choisissent d'utiliser le droit "d" pour ce faire. Pour le premier groupe, on définit le droit "créer" comme l'union des droits "k" et "x", et le droit "supprime" comme l'union des droits "e" et "t". Pour le dernier groupe, on définit les droits "créer" comme synonymes du droit "k", et le droit "supprime" comme l'union des droits "e", "t", et "x".

Pour la compatibilité avec la RFC 2086, ce paragraphe définit deux droits virtuels "d" et "c".

Si un client inclut le droit "d" dans une liste de droits, il DOIT alors être traité comme si le client avait inclus chaque membre du droit "supprime". (Ce n'est pas une erreur pour un client de spécifier à la fois le droit "d" et un ou plusieurs membres du droit "supprime", mais l'effet n'est pas différent de si il avait été juste spécifié le droit "d" ou tous les membres du droit "supprime".)

Quand un des droits membres de "supprime" est établi dans une liste de droits, le serveur DOIT aussi inclure le droit "d" quand il retourne la liste dans une réponse MYRIGHTS ou ACL. C'est pour permettre aux clients plus anciens qui se conforment à la RFC 2086 de travailler avec les serveurs plus récents. (*)

Exemple :
C: A001 SeTacl INBOX/Drafts David lrswida
S: A001 OK Setacl complete

Le client a spécifié le droit "d" dans la commande SETACL et il l'étend à "et" sur le serveur :
C: A002 getacl INBOX/Drafts
S: * ACL INBOX/Drafts Fred rwipslxcetda David lrswideta
S: A002 OK Getacl complete

Si l'identifiant spécifié dans la commande LISTRIGHTS peut recevoir tous les droits de membre "supprimer" sur une boîte aux lettres, le serveur DOIT alors inclure le droit "d" dans la réponse LISTRIGHTS correspondante. (*) Si les droits de membre ne sont pas liés à des droits de non membre, alors le droit "d" est retourné par lui-même dans la réponse LISTRIGHTS. Si un des droits de membre a besoin d'être lié à un (ou plusieurs) droits de non membre, le droit "d" et tous les droits de membre doivent alors être liés au ou aux mêmes droits de non membre (**).

Si un client inclut le droit "c" dans une liste de droits, il DOIT alors être traité comme si le client avait inclus tous les membres du droit "créer". (Ce n'est pas une erreur pour un client de spécifier à la fois le droit "c" et un ou plusieurs membres du droit "créer", mais l'effet n'est pas différent de si juste le droit "c" ou tous les membres du droit "créer" avaient été spécifiés.)

Quand un des droits de membre "créer" est établi dans une liste de droits, le serveur DOIT aussi inclure le droit "c" quand il retourne la liste dans une réponse MYRIGHTS ou ACL. C'est pour permettre aux clients plus anciens qui se conforment à la RFC 2086 de travailler avec des serveurs plus récents. (*)

Exemple :
C: A003 Setacl INBOX/Drafts Byron lrswikda
S: A001 OK Setacl complete
C: A002 getAcl INBOX/Drafts
S: * ACL INBOX/Drafts Fred rwipslxcetda Byron lrswikcdeta
S: A002 OK Getacl complete

Le client a spécifié le droit "d" dans la commande SETACL et il l'étend à "et" sur le serveur : comme le client a spécifié le droit "k" (qui est un membre du droit "c") le serveur retourne aussi le droit "c".

Si il peut être accordé à l'identifiant spécifié dans la commande LISTRIGHTS un des droits de membre "créer" sur une boîte aux lettres, le serveur DOIT alors inclure le droit "c" dans la réponse LISTRIGHTS correspondante. (*) Si les droits de membre ne sont pas liés aux droits de non membre, le droit "c" est alors retourné par lui-même dans la réponse LISTRIGHTS. Si un des droits de membre a besoin d'être lié à un (ou plusieurs) droits de non membre, le droit "c" et tous les droits de membre doivent alors être liés aux mêmes droits de non membre (**).

Exemple : le serveur qui lie les droits comme suit :
lr s w i p k x t
et c=k
va retourner :
S: * LISTRIGHTS archive/imap anyone "" lr s w i p k x t c d

Exemple : le serveur qui lie les droits comme suit :
lr s w i p k xte
et c=k
va retourner :
S: * LISTRIGHTS archive/imap anyone "" lr s w i p k xte c d

Exemple : le serveur qui lie les droits comme suit :
lr s w i p k x te
et c=k
va retourner :
S: * LISTRIGHTS archive/imap anyone "" lr s w i p k c x te d

Exemple : le serveur qui lie les droits comme suit :
lr swte i p k x
et c=kx

va retourner :
S: * LISTRIGHTS archive/imap anyone "" lr swted i p k x c

(*) Les clients qui se conforment au présent document DOIVENT ignorer les droits virtuels "d" et "c" dans les réponses MYRIGHTS, ACL, et LISTRIGHTS.

(**) Le groupe de travail IMAPEXT a débattu longuement de cette question et après avoir examiné les mises en œuvre existantes d'ACL a conclu qu'il s'agit d'une restriction raisonnable.

2.2 Droits définis dans la RFC 2086

La capacité "RIGHTS=" NE DOIT PAS inclure de droits définis dans la RFC 2086 : "l", "r", "s", "w", "i", "p", "a", "c", "d", et des chiffres ("0" .. "9").

3. Commandes et réponses de gestion de contrôle d'accès

Les serveurs, quand ils traitent une commande qui a un identifiant comme paramètre (c'est-à-dire, une des commandes SETACL, DELETEACL, et LISTRIGHTS) DEVRAIT d'abord préparer l'identifiant reçu en utilisant le profil "SASLprep" [RFC4013] de l'algorithme "stringprep" [RFC3454]. Si la préparation de l'identifiant échoue ou résulte en une chaîne vide, le serveur DOIT refuser d'effectuer la commande avec une réponse BAD. Noter que la Section 6 recommande des étapes supplémentaires de vérification d'identifiant.

3.1 Commande SETACL

Arguments : nom de boîte aux lettres ; identifiant ; modification de droits d'accès

Données : pas de données spécifiques pour cette commande

Résultat : OK - setacl achevé
NO - échec de setacl : ne peut pas établir acl
BAD - arguments invalides

La commande SETACL change la liste de contrôle d'accès sur la boîte aux lettres spécifiée afin que l'identifiant spécifié reçoivent les permissions spécifiées dans le troisième argument.

Le troisième argument est une chaîne contenant un préfixe plus ("+") ou moins ("-") facultatif, suivi par zéro, un, ou plusieurs caractères de droits. Si la chaîne commence par un plus, les droits suivants sont ajoutés à tous les droits existants pour l'identifiant. Si la chaîne commence par un moins, les droits suivants sont retirés de tous droits existants pour l'identifiant. Si la chaîne ne commence pas par un plus ou un moins, les droits remplacent tous les droits existants pour l'identifiant.

Noter qu'un droit non reconnu DOIT causer le retour de la réponse BAD par la commande. En particulier, le serveur NE DOIT PAS ignorer en silence des droits non reconnus.

Exemple :
C: A001 GETACL INBOX/Drafts
S: * ACL INBOX/Drafts Fred rwipslxetad Chris lrswi
S: A001 OK Getacl complete
C: A002 SETACL INBOX/Drafts Chris +cda
S: A002 OK Setacl complete
C: A003 GETACL INBOX/Drafts
S: * ACL INBOX/Drafts Fred rwipslxetad Chris lrswicdakxet
S: A003 OK Getacl complete
C: A035 SETACL INBOX/Drafts John lrQswicda
S: A035 BAD les droits en majuscules ne sont pas permis
C: A036 SETACL INBOX/Drafts John lrqswicda
S: A036 BAD le droit q n'est pas accepté

3.2 Commande DELETEACL

Arguments : nom de boîte aux lettres ; identifiant

Données : pas de données spécifiques pour cette commande

Résultat : OK - deleteacl achevé
NO - échec de deleteacl : acl n'a pas pu être supprimé
BAD - arguments invalides

La commande DELETEACL supprime toute paire <identifiant, droits> pour l'identifiant spécifié de la liste de contrôle d'accès pour la boîte aux lettres spécifiée.

Exemple :
C: B001 getacl INBOX
S: * ACL INBOX Fred rwipslxetad -Fred wetd $team w
S: B001 OK Getacl achevé
C: B002 DeleteAcl INBOX Fred
S: B002 OK Deleteacl achevé
C: B003 GETACL INBOX
S: * ACL INBOX -Fred wetd $team w
S: B003 OK Getacl achevé

3.3 Commande GETACL

Arguments : nom de boîte aux lettres

Données : réponses non étiquetées : ACL

Résultat : OK - getacl achevé
NO - échec de getacl : acl n'a pas pu être obtenu
BAD - arguments invalides

La commande GETACL retourne la liste de contrôle d'accès pour la boîte aux lettres dans une réponse ACL non étiquetée.

Certaines mises en œuvre PEUVENT permettre plusieurs formes d'un identifiant pour référencer le même compte IMAP. Généralement, de telles mises en œuvre vont avoir une forme canonique qui est mémorisée en interne. Une réponse ACL causée par une commande GETACL PEUT inclure une forme canonique de l'identifiant qui soit différente de celle utilisée dans la commande SETACL correspondante.

Exemple :
C: A002 GETACL INBOX
S: * ACL INBOX Fred rwipsldexta
S: A002 OK Getacl achevé

3.4 Commande LISTRIGHTS

Arguments : nom de boîte aux lettres ; identifiant

Données : réponses non étiquetées : LISTRIGHTS

Résultat : OK - listrights achevé
NO - échec de listrights : la liste des droits n'a pas pu être obtenue
BAD - arguments invalides

La commande LISTRIGHTS prend un nom de boîte aux lettres et un identifiant et retourne des informations sur les droits qui peuvent être accordés à l'identifiant dans l'ACL pour la boîte aux lettres.

Certaines mises en œuvre PEUVENT permettre plusieurs formes d'un identifiant pour référencer le même compte IMAP. Généralement, de telles mises en œuvre vont avoir une forme canonique qui est mémorisée en interne. Une réponse

LISTRIGHTS causée par une commande LISTRIGHTS DOIT toujours retourner la même forme d'un identifiant comme elle est spécifiée par le client. C'est pour permettre au client de corréler la réponse avec la commande.

Exemple :
C: a001 LISTRIGHTS ~/Messages/sauvegardés smith
S: * LISTRIGHTS ~/Messages/sauvegardés smith la r swicdkxte
S: a001 OK Listrights achevé

Exemple :
C: a005 listrights archive/imap anyone
S: * LISTRIGHTS archive.imap anyone "" l r s w i p k x t e c d a 0 1 2 3 4 5 6 7 8 9
S: a005 Listrights réussi

3.5 Commande MYRIGHTS

Arguments : nom de boîte aux lettres

Données : réponses non étiquetées : MYRIGHTS

Résultat : OK - myrights achevé
NO - échec de myrights : les droits n'ont pas pu être obtenus
BAD - arguments invalides

La commande MYRIGHTS retourne l'ensemble des droits que l'utilisateur a sur la boîte aux lettres dans une réponse MYRIGHTS non étiquetée.

Exemple :
C: A003 MYRIGHTS INBOX
S: * MYRIGHTS INBOX rwiptsldaex
S: A003 OK Myrights achevé

3.6 Réponse à ACL

Données : nom de boîte aux lettres ; zéro, une ou plusieurs paires d'identifiant et de droits

La réponse ACL se produit par suite d'une commande GETACL. La première chaîne est le nom de la boîte aux lettres pour laquelle ACL s'applique. Elle est suivie par zéro, une ou plusieurs paires de chaînes ; chaque paire contient l'identifiant pour lequel l'entrée s'applique suivi par l'ensemble des droits qu'a l'identifiant.

Le paragraphe 2.1.1 détaille les exigences supplémentaires de serveur qui se rapportent au traitement des droits virtuels "d" et "c".

3.7 Réponse à LISTRIGHTS

Données : nom de boîte aux lettres ; identifiant ; droits requis ; liste des droits facultatifs

La réponse LISTRIGHTS se produit par suite d'une commande LISTRIGHTS. Les deux premières chaînes sont le nom de boîte aux lettres et l'identifiant pour lequel cette liste de droits s'applique. Après l'identifiant, il y a une chaîne qui contient l'ensemble (éventuellement vide) de droits qui seront toujours attribués à l'identifiant sur la boîte aux lettres. Ensuite se trouvent zéro, une ou plusieurs chaînes contenant chacune un ensemble de droits qui peuvent être accordés à l'identifiant sur la boîte aux lettres. Les droits mentionnés dans la même chaîne sont liés. Le serveur DOIT soit accorder à l'identifiant tous les droits liés sur la boîte aux lettres, soit n'en accorder aucun. Le paragraphe 2.1.1 détaille les exigences supplémentaires de serveur qui se rapportent au traitement des droits virtuels "d" et "c".

Le même droit NE DOIT PAS figurer plus d'une fois dans la commande LISTRIGHTS.

3.8 Réponse à MYRIGHTS

Données : nom de boîte aux lettres ; droits

La réponse MYRIGHTS survient suite à une commande MYRIGHTS. La première chaîne est le nom de la boîte aux lettres pour laquelle ces droits s'appliquent. La seconde chaîne est l'ensemble des droits qu'a le client.

Le paragraphe 2.1.1 détaille les exigences supplémentaires de serveur qui se rapportent au traitement des droits virtuels "d" et "c".

4. Droits requis pour effectuer différentes commandes IMAP4rev1

Avant d'exécuter une commande, un serveur conforme à ACL DOIT vérifier quels droits sont exigés pour l'exécuter. Cette section groupe les commandes par fonctions effectuées et listes de droits exigés. Elle donne aussi la description détaillée de tout traitement spécial requis.

Dans cette section la contrepartie en UID d'une commande est considérée comme étant la même commande, par exemple, les deux commandes UID COPY et COPY exigent le même ensemble de droits.

Le tableau ci-dessous résume les différents droits ou leurs combinaisons qui sont requis afin d'effectuer différentes opérations IMAP. Comme il n'est pas toujours possible d'exprimer des vérifications et interactions complexes de droits, la description après le tableau devrait être utilisée comme référence principale.

Opérations\droits	l	r	s	w	i	k	x	t	e	a	Tous	Aucun
commandes dans l'état authentifié												
LIST	+											
SUBSCRIBE	*											*
UNSUBSCRIBE												+
LSUB	*											*
CREATE (pour parent)						+						
DELETE		?					+	?	?			
RENAME						+	+					
SELECT/EXAMINE		+										
STATUS		+										
SETACL/DELETEACL										+		
GETACL/LISTRIGHTS										+		
MYRIGHTS											+	
APPEND			?	?	+			?				
commandes dans l'état choisi												
COPY			?	?	+			?				
EXPUNGE									+			
CLOSE									?			
FETCH			?									
Fanions STORE			?	?				?				

Note : pour toutes les commandes dans l'état choisi, le droit "r" est implicite, parce qu'il est exigé de SELECT/EXAMINE une boîte aux lettres. Les serveurs ne sont pas obligés de vérifier la présence du droit "r" une fois que le chois d'une boîte aux lettres est réussi.

Légende :
+ - le droit est requis
* - seulement un des droits marqués * est requis (voir la description ci-dessous)
? - le droit est FACULTATIF (voir la description ci-dessous)
"Tous" - au moins un des droits "l", "r", "i", "k", "x", "a" est requis
"Aucun" - aucun droit n'est exigé pour effectuer la commande

Liste et abonnement/désabonnement aux boîtes aux lettres :
LIST - le droit "l" est requis. Cependant, à la différence des autres commandes (par exemple, SELECT) le serveur NE DOIT PAS retourner une réponse NO si il peut mettre une boîte aux lettres sur la liste.

Noter que si l'utilisateur a le droit "l" sur une boîte aux lettres "A/B", mais pas sur sa boîte aux lettres parente "A", la commande LIST devrait se comporter comme si la boîte aux lettres "A" n'existait pas, par exemple :
C: A777 LIST "" *
S: * LIST (\NoInferiors) "/" "A/B"
S: * LIST () "/" "C"
S: * LIST (\NoInferiors) "/" "C/D"
S: A777 OK LIST achevée

SUBSCRIBE - le droit "l" n'est exigé que si le serveur vérifie l'existence de la boîte aux lettres quand il effectue SUBSCRIBE.

UNSUBSCRIBE - aucun droit n'est exigé pour effectuer cette opération.

LSUB - le droit "l" n'est exigé que si le serveur vérifie l'existence de la boîte aux lettres quand il effectue SUBSCRIBE. Cependant, à la différence des autres commandes (par exemple, SELECT) le serveur NE DOIT PAS retourner une réponse NO si il ne peut afficher un abonnement de boîte aux lettres.

Gestion de boîte aux lettres :
CREATE - le droit "k" sur une boîte aux lettres parente existante proche. Quand une nouvelle boîte aux lettres est créée, elle DEVRAIT hériter de l'ACL provenant de la boîte aux lettres parente (si il en existe une) dans la hiérarchie.

DELETE - le droit "x" sur la boîte aux lettres. Noter que certains serveurs ne permettent pas de supprimer une boîte aux lettres non vide. Si c'est le cas, l'utilisateur va aussi avoir besoin des droits "r", "e", et "t" afin d'ouvrir la boîte aux lettres et de la vider. La commande DELETE DOIT supprimer l'ACL associée à la boîte aux lettres supprimée.

RENAME - déplacer une boîte aux lettres d'un parent à un autre exige le droit "x" sur la boîte aux lettres elle-même et le droit "k" pour le nouveau parent. Par exemple, si l'utilisateur veut renommer la boîte aux lettres appelée "A/B/C" en "D/E", l'utilisateur doit avoir le droit "x" sur la boîte aux lettres "A/B/C" et le droit "k" sur la boîte aux lettres "D". La commande RENAME NE DEVRAIT PAS changer les ACL sur la boîte aux lettres renommée et sur les sous boîtes aux lettres.

Copie ou ajout de messages :
Avant d'effectuer une commande COPY/APPEND, le serveur DOIT vérifier si l'utilisateur a le droit "i" pour la boîte aux lettres cible. Si l'utilisateur n'a pas le droit "i", l'opération échoue. Autrement pour chaque message copié/ajouté, le serveur DOIT vérifier si l'utilisateur a le droit "t" - quand le message a le fanion \Deleted établi ; le droit "s" - quand le message a le fanion \Seen établi ; le droit "w" - pour tous les autres fanions de message. C'est seulement quand l'utilisateur a un droit particulier que les fanions correspondants sont mémorisés pour le nouveau message créé. Le serveur NE DOIT PAS faire échouer une commande COPY/APPEND si l'utilisateur n'a pas de droits pour établir un fanion particulier.

Exemple :
C: A003 MYRIGHTS TargetMailbox
S: * MYRIGHTS TargetMailbox rwis
S: A003 OK Myrights complete
C: A004 FETCH 1:3 (FLAGS)
S: * 1 FETCH (FLAGS (\Draft \Deleted)
S: * 2 FETCH (FLAGS (\Answered)
S: * 3 FETCH (FLAGS ($Forwarded \Seen)
S: A004 OK Fetch Completed
C: A005 COPY 1:3 TargetMailbox
S: A005 OK Copy completed
C: A006 SELECT TargetMailbox
...
S: A006 Select Completed

Supposons que les messages copiés ont reçu les numéros de message 77:79.
C: A007 FETCH 77:79 (FLAGS)
S: * 77 FETCH (FLAGS (\Draft))
S: * 78 FETCH (FLAGS (\Answered))
S: * 79 FETCH (FLAGS ($Forwarded \Seen))
S: A007 OK Le fanion Fetch Completed\Deleted a été perdu sur COPY, car l'utilisateur n'a pas de droit "t" sur la boîte aux lettre cible.

Si la commande MYRIGHTS avec l'étiquette A003 avait été retournée :
S: * MYRIGHTS TargetMailbox rsti
la réponse du FETCH avec l'étiquette A007 aurait été :
C: A007 FETCH 77:79 (FLAGS)
S: * 77 FETCH (FLAGS (\Deleted))
S: * 78 FETCH (FLAGS ())
S: * 79 FETCH (FLAGS (\Seen))
S: A007 OK Fetch Completed

Dans ce dernier cas, les fanions \Answered, $Forwarded, et \Draft ont été perdus sur COPY, car l'utilisateur n'a pas de droit "w" sur la boîte aux lettres cible.

Purge de la boîte aux lettres choisie :
EXPUNGE - droit "e" sur la boîte aux lettres choisie.

CLOSE - droit "e" sur la boîte aux lettres choisie. Si le serveur est dans l'incapacité de purger la boîte aux lettres parce que l'utilisateur n'a pas le droit "e", le serveur DOIT ignorer la demande de purge, clore la boîte aux lettres, et retourner la réponse OK étiquetée.

Aller chercher les informations sur une boîte aux lettre et ses messages :
SELECT/EXAMINE/STATUS - droit "r" sur la boîte aux lettres.

FETCH - une demande FETCH qui implique d'établir le fanion \Seen NE DOIT PAS l'établir, si l'utilisateur actuel n'a pas le droit "s".

Changement de fanions :
STORE - le serveur DOIT vérifier si l'utilisateur a le droit "t" quand l'utilisateur modifie le fanion \Deleted ; le droit "s" quand l'utilisateur modifie le fanion \Seen ; le droit "w" pour tous les autres fanions de message.
L'opération STORE NE DEVRAIT PAS échouer si l'utilisateur a le droit de modifier au moins un fanion spécifié dans le STORE, car la réponse étiquetée NO à une commande STORE n'est pas très bien traitée par les clients en service.

Changement des ACL :
SETACL/DELETEACL - droit "a" sur la boîte aux lettres.

Lecture des ACL :
GETACL - droit "a" sur la boîte aux lettres.

MYRIGHTS - n'importe lequel des droits suivants est requis pour effectuer l'opération : "l", "r", "i", "k", "x", "a".

LISTRIGHTS - droit "a" sur la boîte aux lettres.

5. Autres considérations

5.1 Exigences supplémentaires et notes de mise en œuvre

5.1.1 Serveurs

Le présent document définit une capacité supplémentaire qui est utilisée pour annoncer la liste des droits supplémentaires (à l'exclusion de ceux définis dans la RFC 2086) pris en charge par le serveur. L'ensemble des droits DOIT inclure "t", "e", "x", et "k". Noter que les droits supplémentaires peuvent apparaître dans n'importe quel ordre.

Exemple :
C: 1 capability
S: * CAPABILITY IMAP4REV1 STARTTLS LITERAL+ ACL RIGHTS=texk
S: 1 OK completed

Tout serveur qui met en œuvre une extension ACL DOIT refléter précisément les droits de l'utilisateur actuel dans les réponses FLAGS et PERMANENTFLAGS.

Exemple :
C: A142 SELECT INBOX
S: * 172 EXISTS
S: * 1 RECENT
S: * OK [UNSEEN 12] Message 12 is first unseen
S: * OK [UIDVALIDITY 3857529045] UIDs valid
S: * OK [UIDNEXT 4392] Predicted next UID
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * OK [PERMANENTFLAGS (\Seen \Answered \Flagged *)] L
S: A142 OK [READ-WRITE] SELECT completed
C: A143 MYRIGHTS INBOX
S: * MYRIGHTS INBOX lrwis
S: A143 OK completed

Noter que pour avoir de meilleures performances, le client PEUT traiter en parallèle les commandes SELECT et MYRIGHTS :
C: A142 SELECT INBOX
C: A143 MYRIGHTS INBOX
S: * 172 EXISTS
S: * 1 RECENT
S: * OK [UNSEEN 12] Message 12 is first unseen
S: * OK [UIDVALIDITY 3857529045] UIDs valid
S: * OK [UIDNEXT 4392] Predicted next UID
S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
S: * OK [PERMANENTFLAGS (\Seen \Answered \Flagged *)] L
S: A142 OK [READ-WRITE] SELECT completed
S: * MYRIGHTS INBOX lrwis
S: A143 OK completed

Les serveurs PEUVENT mettre en antémémoire les droits qu'a un utilisateur sur une boîte aux lettres quand elle est choisie, de sorte que si les droits d'un utilisateur sur une boîte aux lettres sont changés avec SETACL ou DELETEACL, les commandes spécifiques de l'état choisi (par exemple, STORE, EXPUNGE) peuvent ne pas refléter les droits changés jusqu'à ce que la boîte aux lettres soit choisie à nouveau. Si le serveur vérifie les droits sur chaque commande, il DEVRAIT alors envoyer les réponses FLAGS et PERMANENTFLAGS si ils ont changé. Si un tel serveur détecte que l'utilisateur n'a plus l'accès en lecture sur la boîte aux lettres, il PEUT envoyer une réponse BYE non étiquetée et clore la connexion. Il PEUT aussi refuser d'exécuter toutes les commandes spécifiques de l'état choisi jusqu'à ce que la boîte aux lettres soit fermée ; cependant, les mises en œuvre de serveur devraient noter que la plupart des clients ne traitent pas très bien les réponses NO.

Un serveur ACL PEUT modifier une ou plusieurs ACL pour un ou plusieurs identifiants comme effet collatéral de la modification de l'ACL spécifiée dans une SETACL/DELETEACL. Si le serveur fait cela, il DOIT envoyer une réponse d'ACL non étiquetée pour notifier au client les changements faits.

Une mise en œuvre de serveur ACL DOIT traiter les commandes de modification d'ACL reçues comme une possible ambiguïté par rapport aux commandes suivantes affectées par l'ACL, comme décrit au paragraphe 5.5 de la [RFC3501]. Donc un traitement en parallèle de SETACL + MYRIGHTS est une ambiguïté par rapport au serveur, ce qui signifie que le serveur doit exécuter la commande SETACL jusqu'à achèvement avant le MYRIGHTS. Cependant, il est permis aux clients d'envoyer un tel traitement en parallèle.

5.1.2 Clients

Les exigences suivantes s'imposent aux clients afin de permettre une future extensibilité. Une mise en œuvre de client qui permet à un utilisateur de lire et mettre à jour les ACL DOIT préserver les droits non reconnus qu'elle ne permet pas à l'utilisateur de changer. C'est-à-dire, si le client
1) peut lire les ACL et
2) peut mettre à jour les ACL, mais
3) ne permet pas à l'utilisateur de changer les droits que le client ne reconnaît pas, il DOIT alors préserver les droits non reconnus.
Autrement, le client risquerait de supprimer involontairement des permissions qu'il ne comprend pas.

5.2 Transposition des droits d'ACL en codes de réponse READ-WRITE et READ-ONLY

Une mise en œuvre particulière de serveur ACL PEUT permettre un "accès multi utilisateurs partagé" à certaines boîtes aux lettres. "Accès multi utilisateurs partagé" à une boîte aux lettres signifie que plusieurs utilisateurs différents sont capables d'accéder à la même boîte aux lettres, si ils ont les droits d'accès appropriés. "Accès multi utilisateurs partagé" à la boîte aux lettres ne signifie pas que l'ACL pour la boîte aux lettres est actuellement réglé à permettre l'accès par plusieurs utilisateurs. On note un "accès multi utilisateurs partagé en écriture" comme un "accès multi utilisateurs partagé" quand il peut être accordé à l'utilisateur les droits de modification de fanions ("w", "s", ou "t").

La Section 4 décrit quels droits sont exigés pour modifier les différents fanions.

Si le serveur ACL met en œuvre des fanions partagés par une boîte aux lettres (c'est-à-dire si l'ACL pour la boîte aux lettres PEUT être établie de façon à ce que les changements de ces fanions soient visibles pour un autre utilisateur) on appelle l'ensemble de droits associés à ces fanions (comme décrit à la Section 4) pour cette boîte aux lettres comme collectivement des "droits de fanions partagés". Noter que l'ensemble de "droits de fanions partagés" PEUT être différent pour des boîtes aux lettres différentes.

Si le serveur ne prend pas en charge "l'accès partagé multi utilisateur en écriture" à une boîte aux lettres ou ne met pas en œuvre les fanions partagés sur la boîte aux lettres, "les droits de fanions partagés" pour la boîte aux lettres sont définis comme étant l'ensemble vide.

Exemple 1 :
La boîte aux lettres "banan" permet "l'accès partagé multi utilisateurs en écriture" et met en œuvre les fanions \Deleted, \Answered, et $MDNSent comme fanions partagés. Les "droits de fanions partagés" pour la boîte aux lettres "banan" sont un ensemble contenant les fanions "t" (parce que le fanion système \Deleted exige le droit "t") et "w" (parce que les deux fanions \Answered et $MDNSent exigent le droit "w").

Exemple 2 :
La boîte aux lettres "apple" permet "accès partagé multi utilisateurs en écriture" et met en œuvre le fanion système \Seen comme fanion partagé. "Droits de fanions partagés" pour la boîte aux lettres "apple" contient le droit "s" parce que le fanion système \Seen exige le droit "s".

Exemple 3 :
La boîte aux lettres "pear" permet "l'accès partagé multi utilisateurs en écriture" et met en œuvre les fanions \Seen, \Draft comme fanions partagés. Les "droits de fanions partagés" pour la boîte aux lettres "apple" sont un ensemble contenant les fanions "s" (parce que le fanion système \Seen exige le droit "s") et "w" (parce que le fanion système \Draft exige le droit "w").

Le serveur DOIT inclure un code de réponse READ-ONLY *(lecture seule)* dans la réponse OK étiquetée à une commande SELECT si aucun des droits suivants n'est accordé à l'utilisateur actuel : "i", "e", et "droits de fanions partagés" (***).

Le serveur DEVRAIT inclure un code de réponse READ-WRITE *(lecture écriture)* dans la réponse OK étiquetée si au moins un des droits "i", "e", o "droits de fanions partagés" (***) est accordé à l'utilisateur en cours.

(***) Noter qu'une future extension au présent document pourrait étendre la liste des droits qui amènent le serveur à retourner le code de réponse READ-WRITE.

Exemple 1 (suite) :
L'utilisateur a les droits "lrs" sur la boîte aux lettres "banan". Le serveur retourne le code de réponse READ-ONLY sur SELECT, car aucun des droits "iewt" n'est accordé à l'utilisateur.

Exemple 2 (suite) :
L'utilisateur a les droits "rit" sur la boîte aux lettres "apple". Le serveur retourne de code de réponse READ-WRITE sur SELECT, car l'utilisateur a le droit "i".

Exemple 3 (suite) :
L'utilisateur a les droits "rset" sur la boîte aux lettres "pear". Le serveur retourne le code de réponse READ-WRITE sur SELECT, car l'utilisateur a les droits "e" et "s".

6. Considérations sur la sécurité

Une mise en œuvre DOIT s'assurer que, par des ACL restreintes de façon appropriée, les commandes ACL elles-mêmes ne donnent pas d'informations sur les boîtes aux lettres. Par exemple, quand un agent d'utilisateur exécute une commande GETACL sur une boîte aux lettres pour laquelle l'utilisateur n'a pas de permission pour LIST, le serveur va répondre à cette demande avec la même erreur qu'il aurait utilisé si la boîte aux lettres n'avait pas existé, ne révélant ainsi aucune information d'existence, beaucoup moins que l'ACL de la boîte aux lettres.

Les clients IMAP qui mettent en œuvre ACL et sont capables de modifier les ACL DEVRAIENT avertir un utilisateur qui veut donner un plein accès (ou même juste le droit "a") à l'identifiant spécial "tous" *(anyone)*.

Le présent document s'appuie sur la [RFC4013] pour décrire les étapes requises pour effectuer la canonisation (préparation) d'identifiant. L'algorithme de préparation dans SASLprep a été spécifiquement conçu de façon que son résultat soit canonique, et qu'il soit bien formé. Cependant, du fait d'une anomalie [PR29] dans la spécification de la normalisation Unicode, l'équivalence canonique n'est pas garantie pour quelques séquences de caractères choisies. Les identifiants préparés avec SASLprep peuvent être mémorisés et retournés par un serveur ACL. L'anomalie affecte la manipulation d'ACL et l'évaluation des identifiants contenant les séquences de caractères choisies. Ces séquences, n'apparaissent cependant pas dans le texte bien formé. Afin de régler ce problème, un serveur ACL PEUT rejeter les identifiants qui contiennent les séquences décrites dans [PR29] en envoyant la réponse BAD étiquetée. Ceci est en plus de l'exigence de rejet des identifiants qui échouent à la préparation SASLprep comme décrit à la Section 3.

Les autres considérations de sécurité décrites dans la [RFC3501] sont pertinentes pour le présent document. En particulier, les informations d'ACL sont envoyées en clair sur le réseau sauf si la protection de la confidentialité est négociée. Cela peut se faire soit en utilisant STARTTLS, en négociant la protection de la confidentialité dans la commande AUTHENTICATE, soit par quelque autre mécanisme de protection.

7. Syntaxe formelle

La syntaxe formelle est définie en utilisant l'ABNF [RFC4234], en étendant les règles d'ABNF de la Section 9 de la [RFC3501]. Les éléments non définis ici se trouvent dans la [RFC4234] et dans la [RFC3501].

Sauf notation contraire, tous les caractères alphabétiques sont insensibles à la casse. L'utilisation de caractères majuscules ou minuscules pour définir des chaînes de jetons est seulement pour la facilité de lecture. Les mises en œuvre DOIVENT accepter ces chaînes sans tenir compte de la casse.

```
LOWER-ALPHA  =  %x61-7A   ;; a-z
acl-data  = "ACL" SP boîte aux lettres *(SP identifiant SP droits)
capability =/ droits-capa                    ;;capability est défini dans la [RFC3501]
command-auth  =/ setacl / deleteacl / getacl / listrights / myrights      ;;command-auth est défini dans la [RFC3501]
deleteacl  = "DELETEACL" SP boîte aux lettres SP identifiant
getacl  = "GETACL" SP boîte aux lettres
identifiant = astring
listrights = "LISTRIGHTS" SP boîte aux lettres SP identifiant
listrights-data = "LISTRIGHTS" SP boîte aux lettres SP identifiant SP droits *(SP droits)
boîte aux lettres-data =/ acl-data / listrights-data / myrights-data          ;;boîte aux lettres-data est défini dans la [RFC3501]
mod-droits = astring                    ;; +droits d'ajouter, -droits de supprimer ; droits de remplacer
myrights = "MYRIGHTS" SP boîte aux lettres
myrights-data = "MYRIGHTS" SP boîte aux lettres SP droits
nouveaux-droits = 1*LOWER-ALPHA
                        ;; DOIT inclure "t", "e", "x", et "k".
                        ;; NE DOIT PAS inclure de droits standard listés au paragraphe 2.2
droits = astring                    ;; seules les lettres ASCII en minuscules et les chiffres sont permis
droits-capa = "RIGHTS=" nouveaux-droits                    ;; RIGHTS=... capability
setacl  = "SETACL" SP boîte aux lettres SP identifiant SP mod-droits
```

8. Considérations relatives à l'IANA

Les capacités IMAP4 sont enregistrées en publiant une RFC sur la voie de la normalisation ou une RFC expérimentale approuvée par l'IESG. Le registre est actuellement situé à : http://www.iana.org/assignments/imap4-capabilities

Le présent document définit la capacité RIGHTS= IMAP. L'IANA a ajouté cette capacité au registre.

9. Considérations d'internationalisation

La Section 3 déclare les exigences pour les serveurs concernant l'internationalisation des identifiants.

Appendice A. Changements par rapport à la RFC 2086

1. Changement du jeu de caractère de "identifiant" de US-ASCII en UTF-8.
2. Spécifié que la suppression de boîte aux lettres est contrôlée par le droit "x" et EXPUNGE par le droit "e".
3. Ajout du droit "t" qui contrôle STORE \Deleted. Redéfinition du droit "d" comme une macro pour "e", "t", et éventuellement "x".
4. Ajout du droit "k" qui contrôle CREATE. Redéfinition du droit "c" comme une macro pour "k" et éventuellement "x".
5. Spécifié que le droit "a" contrôle aussi DELETEACL.
6. Spécifié que le droit "r" contrôle aussi STATUS.
7. Suppression de l'exigence de vérification du droit "r" pour CHECK, SEARCH et FETCH, car c'est exigé pour que SELECT/EXAMINE réussisse.
8. LISTRIGHTS exige le droit "a" sur la boîte aux lettres (comme SETACL).
9. Suppression de "PARTIAL", qui est une caractéristique déconseillée de la RFC 1730.
10. Spécifié que le droit "w" contrôle le réglage des fanions autres que \Seen et \Deleted sur APPEND. Spécifié aussi que le droit "s" contrôle le fanion \Seen et que le droit "t" contrôle le fanion \Deleted.
11. Spécifié que SUBSCRIBE N'EST PAS permis avec le droit "r".
12. Spécifié que le droit "l" contrôle SUBSCRIBE.
13. GETACL N'EST PAS permis avec le droit "r", même si il y a plusieurs mises en œuvre qui le permettent. Si un utilisateur a seulement le droit "r", GETACL peut divulguer des informations sur les identifiants existants sur le système.
14. Précision que RENAME exige le droit "k" pour le nouveau parent et le droit "x" pour l'ancien nom.
15. Ajout d'un nouveau paragraphe qui décrit quels droits sont requis et/ou vérifiés lors de l'exécution de diverses commandes IMAP.
16. Ajout des considérations de sécurité de client de messagerie lors du traitement avec l'identifiant spécial "tous".
17. Précisé que des droits négatifs ne sont pas la même chose que DELETEACL.
18. Ajout de la Section "Compatibilité avec la RFC 2086".
19. Ajout d'un paragraphe sur la transposition des droits d'ACL en codes de réponse READ-WRITE et READ-ONLY.
20. Changement de BNF en ABNF.
21. Ajout de la section "Notes de mise en œuvre".
22. Mise à jour de la Section "Références".
23. Ajout d'exemples.
24. Précisé quand les droits virtuels "c" et "d" sont retournés dans les réponses ACL, MYRIGHTS, et LISTRIGHTS.

Appendice B. Compatibilité avec la RFC 2086

Cet appendice non normatif donne des lignes directrices sur la façon dont une mise en œuvre de serveur existante de la RFC 2086 peut être mise à jour pour se conformer au présent document.

Le présent document partage le droit "d" en plusieurs nouveaux droits différents : "t", "e", et éventuellement "x" (voir les détails au paragraphe 2.1.1). Le droit "d" reste pour la rétro compatibilité, mais c'est un droit virtuel. Il y a deux approches pour que les mises en œuvre de la RFC 2086 traitent le droit "d" et les nouveaux droits qui l'ont remplacé :

a. lier ensemble "t", "e" (et éventuellement "x") - presque pas de changements.
b. Mettre en œuvre séparément "x", "t" et "e". Retourner le droit "d" dans une réponse MYRIGHTS ou une réponse d'ACL contenant les informations d'ACL quand un des droits "t", "e" (et "x") est accordé.

De la même façon, le présent document partage le droit "c" en plusieurs nouveaux droits différents : "k" et éventuellement "x" (voir les détails au paragraphe 2.1.1). Le droit "c" reste pour la rétro compatibilité, mais c'est un droit virtuel. Là encore les mises en œuvre de serveur de la RFC 2086 peuvent choisir de lier les droits ou de mettre en œuvre des droits séparés, comme décrit ci-dessus.

Voir aussi les paragraphes 5.1.1 et 5.1.2, ainsi que l'Appendice A, pour les autres changements requis. Les mises en œuvre de serveurs devraient vérifier quels droits sont requis pour invoquer différentes commandes IMAP4 comme décrit à la Section 4.

Appendice C. Déficiences connues

La présente spécification a certaines déficiences connues qui incluent :

1. Il n'est pas adéquat de fournir un accès complet en lecture écriture aux boîtes aux lettres protégées par des bits de droits de style Unix parce que il n'y a pas d'équivalent aux commandes "chown" et "chgrp" et il n'y a pas de bon moyen pour découvrir que de telles limitations sont présentes.
2. Parce que la présente extension laisse la sémantique spécifique de comment les droits sont combinés par le serveur comme définis par la mise en œuvre, la capacité de construire une interface facile pour l'utilisateur est limitée.
3. Les identifiants d'utilisateurs, de groupes, et spéciaux (par exemple, tous) existent dans le même espace de noms.

Le travail en cours "extension ACL2" est destiné à revoir la conception de cette extension pour traiter ces déficiences sans la contrainte de la rétro compatibilité et pourra peut-être se substituer à cette facilité.

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)

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

[RFC3501] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", mars 2003. *(P.S. ; Remplace* RFC2060 *; MàJ par* RFC4466, 4469, 4551, 5032, 5182, 7817, 8314, 8437, 8474)

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

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

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

Références pour information

[RFC2086] J. Myers, "Extension IMAP4 ACL", janvier 1997. (*Obsolète, voir* RFC4314) *(P.S.)*

[PR29] "Public Review Issue #29: Normalization Issue", février 2004, <http://www.unicode.org/review/pr-29.html>

Adresse de l'auteur

Alexey Melnikov
Isode Ltd.
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
GB
mél : alexey.melnikov@isode.com

Déclaration de droits de reproduction

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