Groupe de travail Réseau
Request for Comments : 5034
RFC rendue obsolète : 1734
RFC mise à jour : 2449
Catégorie : En cours de normalisation

R. Siemborski, Google, Inc.
A. Menon-Sen, Oryx Mail Systems GmbH
juillet 2007

Traduction Claude Brière de L'Isle

Mécanisme d'authentification simple et de couche de sécurité (SASL) du protocole Post Office (POP3)

Statut du présent mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussion et d 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 un profil d'authentification simple et de couche de sécurité (SASL, Simple Authentication and Security Layer) pour le protocole Post Office (POP3). Cette extension permet à un client POP3 d'indiquer un mécanisme d'authentification au serveur, effectue un échange de protocole d'authentification, et négocie facultativement une couche de sécurité pour les interactions de protocole ultérieures durant cette session.

Le présent document cherche à consolider les informations qui se rapportent à la commande AUTH de POP3 dans un seul document. À cette fin, le présent document rend obsolète la RFC 1734 et la remplace, et met à jour les informations contenues au paragraphe 6.3 de la RFC 2449.

1. Introduction

La commande POP3 (voir la [RFC1939]) AUTH (voir la [RFC1734]) a subi plusieurs problèmes dans sa spécification. Le premier est qu'elle est très similaire à un cadre de travail SASL défini par la [RFC4422], mais qui anticipait la spécification SASL initiale. Il y manquait donc quelques composants clés, tels qu'un moyen pour établir la liste des mécanismes d'authentification disponibles.

Plus tard, la [RFC2449] a essayé de remédier à cette situation en ajoutant la commande CAPA et en permettant une réponse de client initial avec la commande AUTH, mais il restait des problèmes quant à la clarté de la spécification sur le traitement de la réponse du client initial.

Tout cela mis bout à bout, il en résulte que la création d'une mise en œuvre complète de la commande AUTH de POP3 requiert une compréhension des matériaux dispersés dans cinq documents différents (et la [RFC3206] donne des codes de réponse différents qui sont à utiliser durant l'authentification).

Le présent document essaye de combiner les informations des [RFC1734] et [RFC2449] pour simplifier cette situation. Il vise, de plus, à clarifier et mettre à jour des spécifications plus anciennes lorsque c'est approprié.

2. Conventions utilisées dans le présent document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

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

La syntaxe formelle est définie par la [RFC4234].

3. La capacité SASL

La présente section se substitue à la définition de la capacité SASL du paragraphe 6.3 de la [RFC2449].

CAPA tag:
SASL

Arguments : Mécanismes SASL pris en charge

Commandes ajoutées : AUTH

Commandes standard affectées : Aucune

États annoncés / différences possibles : les deux / non

Commandes valides dans les états : AUTHORIZATION

Spécification de référence : Le présent document et la [RFC4422]

Discussion : La capacité SASL permet l'utilisation de la commande AUTH (telle que définie à la Section 4 du présent document) pour commencer une négociation SASL (comme défini dans la [RFC4422]). L'argument de la capacité SASL est une liste, séparée par des espaces, des mécanismes SASL qui sont pris en charge.

Si un serveur ne prend pas en charge la commande CAPA ou s'il n'affiche pas la capacité SASL, les clients NE DEVRAIENT PAS tenter la commande AUTH. Si un client tente la commande AUTH dans une telle situation, il NE DOIT PAS fournie le paramètre de réponse initial de client (pour la rétrocompatibilité avec la [RFC1734]).

Noter que la liste des mécanismes disponibles PEUT changer après la réussite d'une commande STLS (voir la [RFC2595]). Cependant, comme l'exige la [RFC2449], les mises en œuvre DOIVENT continuer d'inclure la capacité SASL même après l'achèvement d'une commande AUTH réussie (quand bien même aucune autre commande AUTH ne serait produite).

Exemple
S: +OK pop.example.com BlurdyBlurp POP3 server ready
C: CAPA
S: +OK List of capabilities follows
S: SASL PLAIN DIGEST-MD5 GSSAPI ANONYMOUS
S: STLS
S: IMPLEMENTATION BlurdyBlurp POP3 server
S: .

4. La commande AUTH

Mécanisme AUTH [initial-response]

Arguments : mécanisme : Une chaîne qui identifie un mécanisme d'authentification SASL.

initial-response : Réponse facultative du client initial, comme défini à la Section 3 de la [RFC4422]. Si présente, cette réponse DOIT être codée en Base64 (spécifié à la Section 4 de la [RFC4648]), ou comporter seulement le caractère "=", qui représente une réponse initiale vide.

Restrictions : Après qu'une commande AUTH a été menée à terme avec succès, aucune autre commande AUTH ne peut être produite dans la même session. Après l'achèvement réussi d'une commande AUTH, un serveur DOIT rejeter toute autre commande AUTH avec une réponse -ERR.

La commande AUTH ne peut être donnée que durant l'état AUTHORIZATION.

Discussion : La commande AUTH initialise un échange d'authentification SASL entre le client et le serveur. Le client identifie le mécanisme SASL à utiliser avec le premier paramètre de la commande AUTH. Si le serveur prend en charge le mécanisme d'authentification demandé, il effectue l'échange SASL pour authentifier l'utilisateur. Facultativement, il peut aussi négocier une couche de sécurité pour les interactions de protocole ultérieures durant cette session. Si le mécanisme d'authentification demandé n'est pas accepté, le serveur rejette la commande AUTH avec une réponse -ERR.

L'échange de protocole d'authentification comporte une série de mises en question du serveur et de réponses du client qui est spécifique du mécanisme SASL choisi.

Une mise en question du serveur est l'envoi d'une ligne qui consiste en un caractère "+", suivi par un seul espace et une chaîne codée en Base64, comme spécifié à la Section 4 de la [RFC4648]. Cette ligne NE DOIT PAS contenir de texte autre que la mise en question codée en BASE64.

Un réponse de client consiste une ligne qui contient une chaîne codée en Base64. Si le client souhaite annuler l'échange d'authentification, il produit une ligne avec un seul "*". Si le serveur reçoit une telle réponse, il DOIT rejeter la commande AUTH en envoyant une réponse -ERR.

L'argument facultatif initial-response à la commande AUTH est utilisé pour épargner un aller-retour en utilisant les mécanismes d'authentification qui acceptent une réponse initiale de client. Si l'argument de réponse initiale est omis et si le mécanisme choisi exige une réponse initiale de client, le serveur DOIT procéder en produisant une mise en question vide, comme défini à la Section 3 de la [RFC4422]. Dans POP3, une mise en question de serveur vide est définie comme une ligne avec seulement un "+", suivi d'un seul espace. Elle NE DOIT contenir aucune autre donnée.

Pour les besoins de la réponse initiale de client, la limite de 255 octets pour la longueur d'une seule commande, définie à la Section 4 de la [RFC2449], s'applique toujours. Si la spécification d'une réponse initiale devait causer le dépassement de cette longueur par la commande AUTH, le client NE DOIT PAS utiliser le paramètre de réponse initiale (et doit à la place procéder à l'envoi de sa réponse initiale après une mise en question vide de la part du serveur, comme dans la Section 3 de la [RFC4422]).

Si le client a besoin d'envoyer une réponse initiale de longueur zéro, il DOIT transmettre la réponse comme un seul signe égal ("="). Cela indique que la réponse est présente, mais ne contient pas de données.

Si le client utilise un argument de réponse initiale à la commande AUTH avec un mécanisme SASL qui n'accepte pas un envoi de client initial, le serveur DOIT rejeter la commande AUTH avec un réponse -ERR.

Si le server ne peut pas décoder la réponse du client en Base64, il DOIT rejeter la commande AUTH avec une réponse -ERR. Si le client ne peut pas décoder le Base64 de l'une des mises en question du serveur, il DOIT annuler l'authentification en utilisant la réponse "*". En particulier, serveurs et clients DOIVENT rejeter (et non pas ignorer) tout caractère non explicitement permis par l'alphabet Base64, et DOIVENT rejeter toute séquence de caractères Base64 qui contient le caractère de bourrage ('=') n'importe où ailleurs qu'à la fin d'une chaîne (par exemple, "=AAA" et "AAA=BBB" ne sont pas admis).

À l'exception de la réponse de client initiale, ces chaînes BASE64 peuvent être de longueur arbitraire, selon le mécanisme d'authentification utilisé. Clients et serveurs DOIVENT être capables de traiter les plus grandes mises en question et réponses codées générées par les mécanismes d'authentification qu'ils prennent en charge. Cette exigence est indépendante de toutes limitations de longueur de ligne que le client ou le serveur pourraient subir dans d'autres parties de cette mise en œuvre de protocole.

Si le serveur est incapable d'authentifier le client, il DOIT rejeter la commande AUTH avec une réponse -ERR. Si le client achève l'échange avec succès, le serveur produit une réponse +OK. De plus, en cas de succès, la session POP3 entre dans l'état TRANSACTION.

L'identité d'autorisation générée par l'échange SASL est un simple nom d'utilisateur, et DEVRAIT utiliser le profil SASLprep (voir la [RFC4013]) de l'algorithme StringPrep (voir la [RFC3454]) pour préparer la confrontation de ces noms. Si la préparation de l'identité d'autorisation échoue ou résulte en une chaîne vide (sauf si elle a été transmise comme chaîne vide), le serveur DOIT faire échec à l'authentification.

Si une couche de sécurité est négociée durant l'échange SASL, elle prend effet pour le client sur l'octet qui suit immédiatement le CRLF qui conclut la dernière réponse générée par le client. Pour le serveur, elle prend effet immédiatement à la suite du CRLF de sa réponse de succès.

Lorsqu'une couche de sécurité prend effet, le serveur DOIT éliminer toutes les informations précédemment obtenues du client, qu'il n'aurait pas obtenues de la négociation SASL elle-même. De même, le client DOIT élmimner toute information obtenue du serveur, comme la liste des extensions de service POP3 disponibles.

Lorsque la sécurité de la couche de transport (TLS) (voir la [RFC4346]) et la couche de sécurité SASL sont toutes deux en effet, le codage TLS DOIT être appliqué après le codage SASL lors de l'envoi des données. (Conformément à la [RFC2595], STLS ne peut en aucun cas être produit avant AUTH.)

Noter que POP3 ne permet pas que des données supplémentaires soient envoyées avec un message indiquant un résultat de succès (voir le paragraphe 3.6 de la [RFC4422]).

Le nom de service spécifié par ce profil de protocole de SASL est "pop".

Si une commande AUTH échoue, le client peut essayer un autre mécanisme d'authentification ou présenter des accréditifs différents en présentant une autre commande AUTH (ou en utilisant un des autres mécanismes d'authentification POP3). De même, le serveur DOIT se comporter comme si le client n'avait pas produit la commande AUTH.

Pour assurer l'interopérabilité, les mises en œuvre de client et de serveur de la présente extension DOIVENT mettre en œuvre le mécanisme SASL PLAIN [RFC4616] sur TLS [RFC2595].

Une mise en œuvre de serveur DOIT mettre en œuvre une configuration dans laquelle ellle ne rend public ou ne permet aucun mécanisme de mot de passe en clair, sauf si la commande STLS a été utilisée pour négocier une session TLS (voir la [RFC2595]). Comme décrit par la RFC 4616, cette configuration DEVRAIT être la configuration par défaut. Avant d'utiliser un mécanisme de mot de passe en clair sur une session TLS, les mises en œuvre de client DOIVENT vérifier le certificat du serveur TLS comme exigé par le paragraphe 2.4 de la RFC 25954. Les mises en œuvre de client et de serveur DEVRAIENT mettre en œuvre des mécanismes SASL supplémentaires qui n'envoient pas de mots de passe en clair, tels que le mécanisme GSSAPI [RFC4752].

5. Syntaxe formelle

La spécification de syntaxe formelle utilise la notation en forme Backus-Naur augmentée telle que spécifiée dans la [RFC4234]. Les règles CRLF, ALPHA, et DIGIT sont importées de la [RFC4234]. La règle sasl-mech vient de la [RFC4422].
Sauf notation contraire, tous les caractères alphabétiques sont insensibles à la casse. L'utilisation de caractères majuscules ou minuules pour définir les chaînes de jetons est seulemnt pour faciliter la lecture. Les mises en œuvre DOIVENT accepter ces chaînes de façon insensible à la casse.

```
auth-command     = "AUTH" SP sasl-mech [SP initial-response] *(CRLF [base64]) [CRLF cancel-response] CRLF

initial-response = base64 / "="

cancel-response  = "*"

base64           = base64-terminal / ( 1*(4base64-CHAR) [base64-terminal] )

base64-char      = ALPHA / DIGIT / "+" / "/"
                   ;; Case-sensitive

base64-terminal  = (2base64-char "==") / (3base64-char "=")

continue-req     = "+" SP [base64] CRLF
```

De plus, l'ABNF spécifié dans la [RFC2449] est mis à jour comme suit :

```
response         =/ continue-req
```

6. Exemples

Voici un exemple d'un client qui tente AUTH PLAIN (voir la [RFC4616]) sous TLS en faisant usage de la réponse de client initiale :

```
S: +OK pop.example.com BlurdyBlurp serveur POP3 prêt
C: CAPA
S: +OK Liste des capacités suit
S: SASL DIGEST-MD5 GSSAPI ANONYMOUS
S: STLS
S: IMPLEMENTATION BlurdyBlurp POP3 server
```

S: .
C: STLS
S: +OK Commencer maintenant le négociation TLS
(La négociation TLS a lieu, avec d'autres commandes protégées pas la couche TLS)
C: CAPA
S: +OK Liste des capacités suit
S: SASL PLAIN DIGEST-MD5 GSSAPI ANONYMOUS
S: IMPLEMENTATION BlurdyBlurp POP3 server
S: .
C: AUTH PLAIN dGVzdAB0ZXN0AHRlc3Q=
S: +OK Point de livraison de messagerie verrouillé et prêt

Voici un autre client qui tente AUTH PLAIN sous une couche TLS, cette fois, sans la réponse initiale. Des parties de la négociation avant l'établissement de la couche TLS ont été omises :

(La négociation TLS s'effectue, d'autres commandes sont protégées par la couche TLS)
C: CAPA
S: +OK Liste des capacités suit
S: SASL PLAIN DIGEST-MD5 GSSAPI ANONYMOUS
S: IMPLEMENTATION BlurdyBlurp POP3 server
S: .
C: AUTH PLAIN
(noter qu'il y a une espace qui suit le '+' sur la ligne suivante)
S: +
C: dGVzdAB0ZXN0AHRlc3Q=
S: +OK Point de livraison de messagerie verrouillé et prêt

Voici un exemple qui utilise un mécanisme dans lequel l'échange commence par une mise en question de serveur (les lignes longues sont coupées pour faciliter la lecture) :

S: +OK pop.example.com BlurdyBlurp serveur POP3 prêt
C: CAPA
S: +OK Liste des capacités suit
S: SASL DIGEST-MD5 GSSAPI ANONYMOUS
S: STLS
S: IMPLEMENTATION BlurdyBlurp POP3 server
S: .
C: AUTH DIGEST-MD5
S: + cmVhbG09ImVsd29vZC5pbm5vc29mdC5jb20iLG5vbmNlPSJPQTZNRzl0RVFHbTJoaCIscW9wPSJhd
XRoIixhbGdvcml0aG09bWQ1LXNlc3MsY2hhcnNldD11dGYtOA==
C: Y2hhcnNldD11dGYtOCx1c2VybmFtZT0iY2hyaXMiLHJlYWxtPSJlbHdvb2QuaW5ub3NvZnQuY29t
Iixub25jZT0iT0E2TUc5dEVRR20yaGgiLG5jPTAwMDAwMDAxLGNub25jZT0iT0E2TUhYaDZWcVRyUmsiLGRpZ2
VzdC11cmk9InBvcC9lbHdvb2QuaW5ub3NvZnQuY29tIixyZXNwb25zZT1iMGQ1NmQyZjA1NGMyNGI2MjA3MjMy
MjEwNjQ2OGRiOSxxb3A9YXV0aA==
S: + cnNwYXV0aD0wYjk3MTQ2MmNlZjVlOGY5MzBkYjlhMzNiMDJmYzlhMA==
C:
S: +OK Point de livraison de messagerie verrouillé et prêt

7. Considérations pour la sécurité

Les questions de sécurité sont discutées tout au long du présent document.

8. Considérations relatives à l'IANA

L'IANA a mis à jour son site pour se référer à la présente RFC au lieu de la [RFC1734] dans http://www.iana.org/assignments/pop3-extension-mechanism (le registre des extensions POP3), et aussi dans http://www.iana.org/assignments/gssapi-service-names (le registre des noms de service GSSAPI/SASL).

9. Remerciements

Les auteurs tiennent à remercier de leurs contributions John Myers, Randall Gellens, Chris Newman, Laurence Lundblade, et les autres contributeurs des RFC 1734 et RFC 2554, sur lesquelles le présent document s'appuie fortement.

Les auteurs tiennent aussi à remercier Ken Murchison, Randall Gellens, Alexey Melnikov, Mark Crispin, Arnt Gulbrandsen, Lisa Dusseault, Frank Ellermann, et Philip Guenther qui ont révisé le présent document.

10. Changements par rapport aux RFC 1734, RFC 2449.

1. Références mises à jour avec les versions les plus récentes des diverses spécifications, en particulier la RFC 4422.
2. La sémantique fondée sur SASL définie dans la RFC 2449 est maintenant normative pour l'extension AUTH.
3. Le comportement et le traitement appropriés des réponse de client initialsont définies, avec des exemples et des références à SASL.
4. Nouvelles exigences minimales de prise en charge pour TLS+PLAIN.
5. Le profil SASLprep DEVRAIT être utilisé pour préparer les identités d'autorisation.
6. Précise que le codage TLS devrait s'appliquer après tout codage appliqué par les couches de sécurité SASL.
7. Note que la liste des mécanismes peut changer après STLS.
8. Mentionne explicitement que "=" signifie une réponse initiale de longueur zéro.
9. Note que POP3 ne permet pas que des données supplémentaires soient envoyées avec +OK.

11. Références normatives

[RFC1939] J. Myers et M. Rose, "Protocole Post Office - version 3", STD 53, RFC 1939, mai 1996.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[RFC2449] R. Gellens, C. Newman et L. Lundblade, "Mécanisme d'extension de POP3", RFC 2449, novembre 1998.

[RFC2595] C. Newman, "Utilisation de TLS avec IMAP, POP3 et ACAP", RFC 2595, juin 1999.

[RFC3454] P. Hoffman et M. Blanchet, "Préparation des chaînes internationalisées ("stringprep")", RFC 3454, décembre 2002.

[RFC4013] K. Zeilenga, "SASLprep : Profil Stringprep pour les noms d'utilisateur et les mots de passe", RFC 4013, février 2005.

[RFC4234] D. Crocker, éd., et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", RFC 4234, octobre 2005.

[RFC4422] A. Melnikov, éd., et K. Zeilenga, éd., "Authentification simple et couche de sécurité (SASL)", RFC 4422, juin 2006.

[RFC4648] S. Josefsson, "Codages de données Base16, Base32, et Base64", RFC 4648, octobre 2006.

[RFC4616] K. Zeilenga, éd., "Mécanisme PLAIN d'authentification simple et de couche de sécurité (SASL)", RFC 4616, août 2006.

12. Références informatives

[RFC1734] J. Myers, "La commande AUTHentication de POP3", RFC 1734, décembre 1994.

[RFC3206] R. Gellens, "Codes de réponse SYS et AUTH de POP", RFC 3206, février 2002.

[RFC4346] T. Dierks et E. Rescorla, "Protocole Sécurité de la couche transport (TLS) version 1.1", RFC 4346, avril 2006.

[RFC4752] A. Melnikov, éd., "Mécanisme Kerberos V5 ("GSSAPI") d'authentification simple et de couche de sécurité (SASL)", RFC 4752, novembre 2006.

Adresse des auteurs

Robert Siemborski
Google, Inc.
1600 Ampitheatre Parkway
Mountain View, CA 94043
Phone: +1 650 623 6925
mèl : robsiemb@google.com

Abhijit Menon-Sen
Oryx Mail Systems GmbH
mèl : ams@oryx.com

Déclaration de copyright

Propriété intellectuelle

Remerciement

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