Groupe de travail Réseau
Request for Comments : 5079
Catégorie : En cours de normalisation

J. Rosenberg, Cisco
décembre 2007
Traduction Claude Brière de L'Isle

Rejet des demandes anonymes dans le protocole d'initialisation de session (SIP)

Résumé

Le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) permet aux utilisateurs de faire des appels anonymes. Cependant, les usagers qui reçoivent de tels appels ont le droit de les rejeter parce qu'ils sont anonymes. SIP n'a pas de moyen pour indiquer à l'appelant que la raison du rejet de l'appel est son anonymat. Une telle indication est utile pour permettre que l'appel soit retenté sans l'anonymat. La présente spécification définit un nouveau code de réponse SIP pour répondre à ce besoin.

1. Introduction

Le protocole d'initialisation de session (SIP) [RFC3261] permet aux utilisateurs de faire des appels anonymes. Dans la RFC 3261, ceci est fait en incluant un champ From *(de)* dont le nom affiché a la valeur de "Anonyme". De plus grands niveau d'anonymat ont été ultérieurement définis dans la [RFC3323], qui a introduit le champ d'en-tête Privacy *(confidentialité)*. Le champ d'en-tête Privacy permet à un agent d'utilisateur (UA, *User Agent*) demandeur d'invoquer divers niveaux d'anonymat, y compris l'anonymat de niveau utilisateur, l'anonymat de niveau en-tête, et l'anonymat de niveau session. La [RFC3325] a en plus défini le champ d'en-tête P-Asserted-Identity, utilisé pour contenir une identité attestée. La RFC 3325 définissait aussi la valeur 'id' pour le champ d'en-tête Privacy, qui est utilisée pour demander au réseau de retirer le champ d'en-tête P-Asserted-Identity.

Bien que les utilisateurs aient besoin d'être capables de faire des appels anonymes, les usagers qui reçoivent de tels appels conservent le droit de rejeter l'appel à cause de son anonymat. SIP ne fournit pas de code de réponse qui permette au serveur d'agent d'utilisateur (UAS, *User Agent Server*), ou à un mandataire agissant en son nom, d'indiquer explicitement que la demande a été rejetée à cause de son anonymat. Le code de réponse le plus proche est 403 (Interdit), qui n'indique pas de raison spécifique. Alors qu'il est possible d'inclure une phrase de cause dans une réponse 403 qui indique à l'utilisateur humain que l'appel a été rejeté parce qu'il était anonyme, cette phrase de cause n'est pas utile pour un automate et ne peut pas être interprétée par un appelant d'une autre langue. Une indication qui puisse être comprise par un automate permettrait un traitement programmé, incluant des invites d'interface d'utilisateur, ou la conversion en codes d'erreur équivalents dans le réseau téléphonique public commuté (RTPC) lorsque le client est un routeur.

Pour y remédier, la présente spécification définit le code de réponse 433 (Anonymat interdit).

2. Terminologie

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

3. Comportement du serveur

Un serveur (agissant généralement au nom de l'appelant, bien que ce ne soit pas nécessairement le cas) PEUT générer une réponse 433 (Anonymat interdit) lorsqu'il reçoit une demande anonyme, et que le serveur refuse de satisfaire la demande

parce que le demandeur est anonyme. Une demande DEVRAIT être considérée comme anonyme lorsque l'identité de l'origine de la demande a été explicitement retirée par celui qui l'a générée. Ceci survient dans l'un des cas suivants :

- Le champ d'en-tête From contient une URI au sein du domaine anonymous.invalid.

- Le champ d'en-tête From contient un affichage de nom dont la valeur est 'Anonyme' ou 'anonyme'. Noter que les noms d'affichage n'ont qu'un choix assez pauvre pour indiquer l'anonymat, car ils sont destinés à la consommation humaine, et non aux automates. Et donc, les variations linguistiques et même une faute de frappe, peuvent amener un automate à manquer une indication dans le nom d'affichage. En dépit de ces problèmes, une vérification sur le nom d'affichage est incluse ici parce que la RFC 3261 déconseille explicitement l'utilisation du nom d'affichage comme moyen de déclarer l'anonymat.

- La demande contenait un champ d'en-tête Privacy dont la valeur indique que l'usager souhaite que son identité soit cachée. Les valeurs qui satisfont ce critère sont 'id' [RFC3325] ou 'user'.

- Le champ d'en-tête From contient un URI qui a une indication explicite d'anonymat. L'exemple d'un tel mécanisme satisfaisant de critère est [coexistence]. Ce critère est vrai même si la demande a un champ d'en-tête Identity validé [RFC4474], qui peut être utilisé de concert avec les champs d'en-tête From rendus anonymes.

L'absence d'une identité attestée par le réseau (telle qu'une champ d'en-tête P-Asserted-Identity) NE DEVRAIT PAS, par elle-même, être considérée comme une indication d'anonymat. Bien qu'une valeur de champ d'en-tête Privacy de 'id' cause la suppression d'une identité attestée par le réseau, il n'y a pas de moyen de différencier ce cas de celui dans lequel une identité attestée par le réseau n'a pas été acceptée par le domaine d'origine. Par conséquent, une demande sans une identité attestée par le réseau n'est considérée comme anonyme que lorsqu'il y a quelque autre indication de cela, comme un champ d'en-tête From avec un nom d'affichage de 'Anonyme'.

De plus, les demandes dans lesquelles l'identité du demandeur ne peut pas être déterminée ou validée, mais où ce n'est pas la conséquence d'une action explicite de la part du demandeur, ne sont pas considérée comme anonymes. Par exemple, si une demande contient un champ d'en-tête From non anonyme, avec les champs d'en-tête Identity et Identity-Info de la [RFC4474], mais si le certificat ne peut pas être obtenu de la référence dans le champ d'en-tête Identity-Info, elle n'est pas considérée comme une demande anonyme, et le code de réponse 433 NE DEVRAIT PAS être utilisé.

4. Comportement de l'UAC

Un client d'agent d'utilisateur (UAC, *User Agent Client*) qui reçoit une réponse 433 (Anonymat interdit) NE DOIT PAS réessayer la demande sans l'anonymat à moins qu'il n'obtienne confirmation de la part de l'usager que c'est souhaitable. Une telle confirmation devrait être obtenue à travers l'interface d'utilisateur, ou par en accédant à une politique définie par l'usager. Si l'usager a indiqué que c'est souhaitable, l'UAC PEUT réessayer la demande sans demander l'anonymat. Noter que si l'UAC devait réessayer automatiquement la demande sans l'anonymat en l'absence d'indication de la part de l'usager que ce traitement est souhaitable, les attentes de l'usager ne seraient alors pas satisfaites. Par conséquent, un usager pourrait penser qu'il a effectué un appel anonyme alors qu'en réalité il n'est pas anonyme.

La réception d'une réponse 433 à une demande de mi-dialogue NE DEVRAIT PAS causer la fin du dialogue, et NE DEVRAIT PAS causer l'interruption de cette utilisation spécifique de ce dialogue [RFC5057].

Un UAC qui ne comprend pas ou ne tient pas compte de la sémantique spécifique de la réponse 433 la traitera comme une réponse 400.

5. Définition de 433 (Anonymat interdit)

Cette réponse indique que le serveur refuse de satisfaire la demande parce que le demandeur est anonyme. Sa phrase de cause par défaut est "Anonymat interdit".

6. Considérations relatives à l'IANA

La présente section enregistre un nouveau code de réponse SIP conformément aux procédures de la RFC 3261.

Numéro de RFC : RFC 5079

Numéro de code de réponse : 433
Phrase de cause par défaut : Anonymat interdit

7. Considérations pour la sécurité

Le fait qu'une demande soit rejetée à cause de l'anonymat ne révèle pas d'information sur l'appelant – mais que l'appelé n'accepte pas les appels anonymes. Cette information peut être ou non sensible. Si elle l'est, un UAS DEVRAIT plutôt rejeter la demande avec une réponse 403.

Dans le réseau téléphonique public commuté (RTPC), le dispositif de rejet d'appel anonyme (ACR, *Anonymous Call Rejection*) est d'utilisation courante pour empêcher des appels indésirables de téléprospecteurs (appelés aussi polluposteurs). Comme les téléprospecteurs dissimulent fréquemment leur identité, le rejet des appels anonymes a l'effet désiré dans de nombreux cas (mais pas tous). Il est important de noter que le code de réponse décrit ici sera vraisemblablement inefficace pour bloquer les pourriels fondés sur SIP. La raison en est qu'un appelant malveillant peut inclure un champ d'en-tête From et un nom d'affichage qui ne sont pas anonymes, mais sont sans signification et invalides. Sans un champ d'en-tête Privacy, une telle demande ne paraîtra pas anonyme et donc ne sera pas bloquée par un service de recherche de messages anonymes. Le traitement des pourriels fondés sur SIP n'est pas un problème simple. Le lecteur est invité à se référer à [sipping-spam] pour un exposé du problème.

Lorsque des services d'anonymat sont fournis en conséquence d'une fonction d'anonymat qui agit comme un agent d'utilisateur de boucle locale (B2BUA, *back-to-back user agent*) [RFC3323], et que le demandeur anonyme reçoit une réponse 433, le demandeur anonyme NE DOIT PAS réessayer la demande sans anonymat sauf s'il a été explicitement configuré par l'utilisateur pour faire ainsi. Par nature, les mêmes règles qui s'appliquent à un UA pour le traitement d'une réponse 433 s'appliquent à un fonction d'anonymat fondée sur le réseau, et pour les mêmes raisons.

8. Remerciements

La motivation du présent document se fonde sur les exigences figurant dans [tispan-req], et il a bénéficié des concepts développés dans [hautakorpi]. Merci à Keith Drage, Paul Kyzivat et John Elwell pour leurs relectures du document.

9. Références

9.1 Références normatives

[RFC3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley et E. Schooler, "SIP : Protocole d'initialisation de session", RFC 3261, juin 2002.

[RFC3323] J. Peterson, "Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)", RFC 3323, novembre 2002.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les exigences de niveau", BCP 14, RFC 2119, mars 1997.

[RFC4474] J. Peterson et C. Jennings, "Améliorations de la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", RFC 4474, août 2006.

9.2 Références informatives

[RFC3325] C. Jennings, J. Peterson et M. Watson, "Extensions privées au protocole d'initialisation de session (SIP) pour les identités certifiées au sein des réseaux de confiance", RFC 3325, novembre 2002.

[coexistence] J. Rosenberg, "Coexistence de P-Asserted-ID et de l'identité SIP", Travail en cours, juin 2006.

[tispan-req] R. Jesske, "Exigences d'entrée pour le protocole d'initialisation de session (SIP) pour les besoins de l'Institut Européen de normalisation des Télécommunications", Travail en cours, juillet 2007.

[hautakorpi] J. Hautakorpi et G. Camarillo, "Extension de l'en-tête Raison du Protocole d'initialisation de session avec des codes d'avertissement", Travail en cours, octobre 2005.

[RFC5057] R. Sparks, "Utilisation de dialogues multiples dans le protocole d'initialisation de session", RFC 5057, novembre 2007.

[sipping-spam] C. Jennings et J. Rosenberg, "Protocole d'initialisation de session (SIP) et Spam", Travail en cours, août 2007.

Adresse de l'auteur

Jonathan Rosenberg
Cisco
Edison, NJ
US
mél : jdrosen@cisco.com
URI : http://www.jdrosen.net

Déclaration de copyright

Propriété intellectuelle