Groupe de travail Réseau
Request for Comments : 3323
Catégorie : En cours de normalisation

J. Peterson, Neustar
novembre 2002
Traduction Claude Brière de L'Isle

Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP)

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

Résumé
Le présent document définit de nouveaux mécanismes pour le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) pour la prise en charge de la confidentialité. Précisément, des lignes directrices sont fournies pour la création de messages qui ne divulguent pas les informations d'identité personnelle. Un nouveau rôle logique de "service de confidentialité" pour les intermédiaires est défini pour répondre à certaines exigences de confidentialité que les agents d'utilisateur ne peuvent satisfaire eux-mêmes. Enfin sont présentés des moyens par lesquels un utilisateur peut demander des fonctions particulières à un service de confidentialité.

Table des matières

1. Introduction

Le présent document donne les exigences et les mécanismes de confidentialité pour le protocole d'initialisation de session (SIP, *Session Initiation Protocol*).

La confidentialité est définie dans le présent document comme la dissimulation de l'identité d'une personne (et des informations personnelles qui s'y rapportent) à une ou plusieurs parties dans un échange de communications, et

précisément un dialogue SIP. Ces parties incluent éventuellement la ou les destinations des messages et/ou tous intermédiaires qui traitent ces messages. Comme est définie l'identité dans le présent document, la dissimulation de l'identité d'un usager va, entre autres choses, rendre les autres parties au dialogue incapables d'envoyer de nouvelles demandes SIP à l'usager en dehors du contexte du dialogue en cours.

Dans SIP, l'identité est le plus couramment portée sous la forme d'un URI SIP et d'un nom d'affichage facultatif. Une address-of-record SIP a une forme similaire à une adresse de messagerie électronique avec un schéma d'URI SIP (par exemple, sip:alice@atlanta.com). Un nom d'affichage est une chaîne qui contient un nom pour l'usager identifié (par exemple, "Alice"). Les identités SIP de cette forme apparaissent communément dans les champs d'en-tête To et From des demandes et réponses SIP. Un usager peut avoir de nombreuses identités pour des contextes différents.

Il y a de nombreux autres endroits dans les messages SIP qui peuvent révéler des informations en rapport avec l'identité. Par exemple, le champ d'en-tête Contact contient un URI SIP, qui est couramment aussi révélateur que l'address-of-record de l'en-tête From. Dans certains en-têtes, l'agent d'utilisateur d'origine peut dissimuler des informations sur l'identité au titre de la politique locale sans affecter le fonctionnement du protocole SIP. Cependant, certains en-têtes sont utilisés dans l'acheminement des messages ultérieurs dans un dialogue, et doivent donc être remplis avec des données fonctionnelles.

Le problème de la confidentialité est encore compliqué par les serveurs mandataires (aussi appelés dans le présent document "intermédiaires" ou "le réseau") qui ajoutent des en-têtes de leur cru, tels que les en-têtes Record-Route et Via. Les informations dans ces en-têtes pourraient révéler par inadvertance quelque chose sur l'origine d'un message ; par exemple, un en-tête Via peut révéler le fournisseur de service par lequel l'usager a envoyé les demandes, ce qui peut à son tour être une forte indication de l'identité de l'envoyeur pour certains receveurs. Pour ces raisons, la participation des intermédiaires est aussi cruciale pour la fourniture de la confidentialité dans SIP.

Deux principes complémentaires ont guidé la conception de ce mécanisme de confidentialité : les usagers ont le pouvoir de cacher leur identité et les informations personnelles qui s'y rapportent lorsqu'ils produisent des demandes, mais les intermédiaires et les receveurs désignés des demandes sont fondés à rejeter les demandes dont l'origine ne peut être identifiée.

Le présent document ne discute des propriétés de confidentialité que des en-têtes spécifiques énumérés dans la spécification SIP principale ([1]), par opposition aux en-têtes définis par toute extension existante ou prévue – cependant, les mécanismes de confidentialité décrits dans le présent document peuvent être étendus pour prendre en charge les extensions.

Il y a pour SIP d'autres aspects du problème général de la confidentialité qui ne sont pas traités par le présent document. Parmi les plus significatifs, les mécanismes de gestion de la confidentialité des en-têtes et corps SIP, ainsi que la sécurité du trafic de session, ne sont pas reconsidérés ici. Ces problèmes sont suffisamment bien traités dans la spécification SIP de base et dans les documents qui s'y rapportent, et aucun nouveau mécanisme n'est nécessaire.

Le présent document commence par une section qui fournit un cadre général et une architecture pour la confidentialité dans SIP (Section 3), suivie par des sections qui détaillent le comportement d'agent d'utilisateur (Section 4) et le comportement du service de confidentialité (Section 5).

2. Terminologie

Les termes en majuscules "DOIT", "DEVRAIT", "PEUT", "NE DEVRAIT PAS", "NE DOIT PAS", et "RECOMMANDE" sont utilisés selon la définition de la RFC 2119, BCP 14 [2] et indiquent les niveaux d'exigence pour les mises en œuvre conformes à SIP.

3. Variétés de confidentialité

Un usager peut posséder de nombreuses identités qui sont utilisées dans divers contextes ; généralement, les identités sont des adresses d'enregistrement qui sont liées à des registres particuliers (que font fonctionner les administrateurs d'un domaine) avec lesquels les agents d'utilisateur SIP s'enregistrent. Les opérateurs de ces domaines peuvent être des employeurs, des fournisseurs de service, ou des usagers non affiliés eux-mêmes.

Lorsqu'un usager affiche volontairement son identité dans une demande, il affirme qu'il peut recevoir des demandes envoyées à cette identité dans ce domaine. Strictement parlant, la confidentialité entraîne des restrictions à la distribution d'une identité spécifique et des informations personnelles qui s'y rapportent pour certaines parties qui sont des receveurs potentiels du message. En particulier, il y a des scénarios dans lesquels une partie qui désire l'anonymat peut :

- envoyer un message et dissimuler une identité à la ou aux destinations finales tout en communiquant quand même une

identité à un ou plusieurs intermédiaires
- envoyer un message et dissimuler son identité à certains ou à tous les intermédiaires, mais communiquer quand même une identité de bout en bout à la ou aux destinations finales
- dissimuler son identité aussi bien aux intermédiaires qu'à la ou aux destinations finales

Le résultat de la dissimulation d'une identité est que les parties en question seront incapables, par exemple, d'essayer d'initier ultérieurement un nouveau dialogue avec la partie anonyme. Cependant, la partie anonyme doit toujours être capable de recevoir des réponses et de nouvelles demandes durant le dialogue auquel elle participe.

Il peut être souhaitable de restreindre les informations sur l'identité à la fois sur les demandes et les réponses. Au départ, il peut sembler inhabituel de suggérer qu'une réponse a des problèmes de confidentialité – on peut présumer que l'origine de la demande sait qui il a essayé de contacter – de sorte que l'identité de celui qui répond peut difficilement être confidentielle. Cependant, certaines informations personnelles dans les réponses (telles que l'adresse de contact à laquelle celui qui répond est réellement enregistré) posent des problèmes de confidentialité et peuvent être traitées par ces mécanismes.

3.1 Quand la confidentialité est-elle nécessaire ?

Les usagers peuvent souhaiter que des informations sur l'identité soient dissimulées à une partie donnée pour un certain nombre de raisons, par exemple :

- Les usagers peuvent vouloir contacter une certaine partie sans révéler leur identité afin de transmettre des informations auxquelles ils n'aimeraient pas être associés.

- Les usagers peuvent craindre que la divulgation de leur identité ou d'informations personnelles sur des réseaux ou à des destinations qui feraient d'eux des cibles de publicités importunes, d'une censure légale ou d'autres conséquences inopportunes.

- Les usagers peuvent vouloir dissimuler aux participants à une session l'identité sous laquelle ils sont connus des intermédiaires du réseau pour les besoins de la comptabilité et la facturation.

Lorsqu'un agent d'utilisateur décide d'envoyer une demande par l'intermédiaire d'un serveur mandataire, il peut être difficile pour l'origine d'anticiper la destination finale de ce message. Pour cette raison, il est conseillé aux utilisateurs de ne pas fonder l'estimation de leurs besoins de confidentialité sur la destination attendue d'un message. Par exemple, si un usager envoie une demande à un numéro de téléphone, il peut croire que la destination finale de la demande sera une station sur le réseau téléphonique public commuté (RTPC) qui sera incapable d'inspecter, disons les en-têtes Contact de SIP, et suppose donc qu'il peut en toute sécurité laisser de tels en-têtes en clair ; cependant, une telle demande pourrait très bien finir par être redirigée par le réseau sur un authentique point d'extrémité SIP pour lequel les en-têtes Contact sont parfaitement lisibles.

Le présent document décrit trois degrés de confidentialité – un niveau de confidentialité fournie par l'utilisateur, et deux niveaux de confidentialité fournie par le réseau (confidentialité d'en-tête et confidentialité de session). Quelle quantité de confidentialité est nécessaire à un usager pour une session donnée ? En général, si un utilisateur recherche la confidentialité, il va en avoir besoin d'autant qu'il peut en obtenir. Cependant, si un utilisateur ne connaît pas de service de confidentialité, il se contentera de la seule confidentialité fournie par l'utilisateur. De même, si un usager connaît un service d'anonymat qui peut fournir la confidentialité de session, mais s'il est incapable de sécuriser le trafic de session pour empêcher ce service d'anonymat d'éventuellement espionner la session, il pourrait juger la perte de la confidentialité de session un moindre mal. L'usager peut aussi être conscient de conditions exceptionnelles au sujet de l'architecture dans laquelle l'agent d'utilisateur se trouve qui pourraient obvier à un ou plusieurs problèmes de confidentialité.

Un usager peut n'être pas toujours le meilleur juge du moment où la confidentialité est nécessaire même dans des circonstances idéales, et donc dans certaines architectures la confidentialité peut être appliquée par des intermédiaires sans une demande explicite de l'usager message par message. En envoyant une demande par des intermédiaires qui peuvent jouer un rôle en matière de confidentialité, l'usager permet tacitement que des fonctions de confidentialité soient invoquées en tant que de besoin.

Il est aussi important que les usagers comprennent que les intermédiaires peuvent être incapables de fournir les fonctions de confidentialité demandées par les usagers. Les demandes de confidentialité peuvent n'être pas honorées du fait de contraintes légales, de dispositifs non mis en œuvre ou mal configurés, ou autres conditions exceptionnelles.

Noter que comme c'est simplement la prérogative d'un usager de dissimuler son identité, il doit aussi être la prérogative des

serveurs mandataires et des autres usagers de refuser de traiter des demandes d'utilisateurs qu'ils ne peuvent pas identifier. Donc les usagers ne devraient pas simplement dissimuler automatiquement leur identité pour toutes les demandes et réponses – l'incapacité à certifier l'identité de l'origine de la demande sera souvent le fondement d'un rejet. La confidentialité ne devrait être demandée que lorsque l'usager en a besoin.

De plus sur ce point, la dissimulation de certaines informations dans la signalisation peut n'être pas nécessaire pour tous les agents d'utilisateur pour assurer la confidentialité. Par exemple, les agents d'utilisateur peuvent acquérir leurs adresses IP et leurs noms d'hôte par des moyens dynamiques, et ces adresses dynamiques peuvent ne révéler aucune information sur l'usager quel qu'il soit. Dans ces cas, restreindre l'accès aux noms d'hôtes (comme décrit au paragraphe 4.1.1.3) n'est pas nécessaire.

3.2 Confidentialité fournie par l'utilisateur

Il y a une certaine quantité de confidentialité qu'un agent d'utilisateur peut fournir lui-même. Par exemple, la spécification SIP de base permet à un agent d'utilisateur de remplir le champ d'en-tête From d'une demande avec une valeur anonyme. Les usagers peuvent prendre des mesures similaires pour éviter de révéler n'importe quelles autres informations non nécessaires sur l'identité dans les en-têtes SIP qui s'y rapportent (ceci est discuté plus en détail au paragraphe 4.1.1).

Un usager peut avoir des besoins de confidentialité différents pour un message si il traverse des intermédiaires plutôt que d'aller directement de bout en bout. Un usager peut tenter de dissimuler aux intermédiaires des choses qui ne seront pas cachées à la destination finale, et vice versa. Par exemple, en utilisant les mécanismes de base de SIP, un agent d'utilisateur peut chiffrer les corps SIP de bout en bout afin d'empêcher les intermédiaires de les inspecter. Si un message SIP ne passe pas à travers des intermédiaires, cette étape peut cependant n'être pas nécessaire (c'est-à-dire, la sécurité de couche inférieure, sans l'ajout de la sécurité pour les corps SIP, pourrait être suffisante).

Noter aussi que si un dialogue va directement de bout en bout entre les participants, il ne sera cependant pas possible de dissimuler les adresses réseau des participants.

3.3 Confidentialité fournie par le réseau

Si un usager envoie une demande par un intermédiaires, un agent d'utilisateur ne peut dissimuler son identité que dans une certaine mesure sans la coopération des intermédiaires. Aussi, certaines informations ne peuvent être dissimulées aux points d'extrémité de destination que si un intermédiaire est chargé de les retirer.

Pour ces raisons, un usager doit avoir un moyen de demander la confidentialité aux intermédiaires, un moyen qui lui permette à la fois de signaler certaines indications des services de confidentialité désirés, et d'assurer que son appel est acheminé par un intermédiaire qui soit capable de fournir ces services. Un usager peut connaître un hôte tiers spécifique capable de fournir l'anonymat, avec lequel il a eu des relations préexistantes, ou bien l'usager peut demander que leur domaine administratif local fournisse les services de confidentialité.

Les intermédiaires peuvent aussi avoir le pouvoir d'appliquer la confidentialité à un message sans aucune signalisation explicite de la part de l'usager d'origine, car les agents d'utilisateur peuvent n'avoir pas toujours connaissance ou n'être pas capables de demander la confidentialité quand elle est nécessaire.

4. Comportement de l'agent d'utilisateur

Il y a trois façons différentes par lesquelles un agent d'utilisateur peut contribuer à la confidentialité d'une demande – en remplissant les en-têtes avec des valeurs qui reflètent les exigences de confidentialité, en demandant d'autres services de confidentialité au réseau, et en utilisant la confidentialité cryptographique pour sécuriser les en-têtes et les corps. Noter que cette dernière est en dehors du domaine d'application du présent document.

Les mécanismes décrits dans cette section supposent qu'un agent d'utilisateur est suffisamment configurable pour qu'un usager puisse choisir des valeurs d'en-tête et fournir des préférences de confidentialité (dans l'idéal, appel par appel). Si ce n'est pas le cas, il est possible qu'un usager puisse acheminer son appel à travers un service de confidentialité qui soit configuré pour assister la signalisation de cet agent d'utilisateur afin de fournir certaines des fonctions décrites ci-dessous (voir à la Section 5).

4.1 Construction de messages confidentiels

La confidentialité commence avec l'agent d'utilisateur. Le gros des étapes nécessaires pour dissimuler les informations privées sur l'expéditeur d'un message sont, assez opportunément, de la responsabilité de l'envoyeur.

Les en-têtes SIP suivants, lorsqu'ils sont générés par un agent d'utilisateur, peuvent directement ou indirectement révéler des informations sur l'identité de celui qui est à l'origine d'un message : From, Contact, Reply-To, Via, Call-Info, User-Agent, Organization, Server, Subject, Call-ID, In-Reply-To et Warning. Noter que l'utilisation d'un système d'authentification (tel que la méthode d'authentification par résumé de SIP décrite dans [1]) a aussi pour résultat habituel de révéler l'identité à une ou plusieurs parties ; voir à la Section 6 des informations complémentaires.

La première étape, la plus évidente, est que les agents d'utilisateur NE DEVRAIENT PAS inclure d'en-têtes facultatifs qui pourraient divulguer des informations personnelles ; il n'y a certainement aucune raison pour qu'un usager qui recherche la confidentialité remplisse un champ d'en-tête Call-Info. Ensuite, l'usager DEVRAIT remplir les URI tout au long du message conformément aux lignes directrices du paragraphe 4.1.1. Par exemple, les usagers DEVRAIENT créer un champ d'en-tête From anonyme pour la demande. Finalement, les usagers PEUVENT aussi avoir besoin de demander certaines fonctions de confidentialité au réseau, comme décrit au paragraphe 4.2.

L'en-tête Call-ID, qui est fréquemment construit d'une manière qui révèle l'adresse IP ou le nom d'hôte du client d'origine, requiert une mention particulière. Les agents d'utilisateur DEVRAIENT substituer à l'adresse IP ou nom d'hôte qui est fréquemment ajouté à la valeur du Call-ID une valeur aléatoire de longueur convenable (la valeur utilisée comme "étiquette pour l'en-tête From de la demande pourrait même être réutilisée).

Noter que si l'usager veut dissimuler l'un des en-têtes ci-dessus aux seuls intermédiaires, sans les cacher à la destination finale du message, il PEUT aussi placer des valeurs légitimes pour ces en-têtes dans des corps S/MIME encapsulés 'message/sip' comme décrit à la Section 23 de [1].

4.1.1 URI, noms d'affichage et confidentialité

On peut obtenir une certaine confidentialité en choisissant de remplir les en-têtes SIP avec des URI et des noms d'affichage qui ne révèlent aucune information sur l'identité. Dans certains des champs d'en-tête (par exemple, les en-têtes Reply-To et From) les URI ne sont pas utilisés dans les signalisations au sein des dialogues en cours. Dans d'autres, comme l'en-tête Contact, un URI inapproprié résultera en un échec de l'acheminement des demandes ultérieures au sein du dialogue.

4.1.1.1 Noms d'affichage

Il est de pratique relativement courante dans la messagerie électronique et autres applications d'utiliser un nom d'emprunt dans le composant de nom d'affichage du champ d'en-tête From. En dehors d'un contexte professionnel (en particulier dans des applications telles que la messagerie instantanée ou les jeux sur Internet) l'utilisation de tels alias est peu susceptible d'être une cause de défiance.

Il est RECOMMANDÉ que les agents d'utilisateur recherchent l'anonymat utilisent un nom d'affichage de "Anonyme".

4.1.1.2 URI en forme de nom d'utilisateur

La structure d'un URI elle-même peut révéler ou dissimuler une quantité considérable d'informations personnelles. Considérer la différence entre sip:jon.peterson@neustar.biz et sip:a0017@anonymous-sip.com

Dans le premier, le nom complet et l'employeur de la partie en question peuvent facilement être devinés. Du second, vous n'apprenez rien d'autre que cette personne désire l'anonymat. Dans certains cas, un anonymat suffisant peut être obtenu en choisissant un URI oblique. Aujourd'hui, la spécification SIP recommande un URI avec "anonyme" dans la portion usager de l'en-tête From.

Dans certains URI, tels que ceux qui apparaissent dans les en-têtes Contact, il PEUT aussi y avoir un sens à omettre aussi le nom d'utilisateur, et à fournir seulement un nom d'hôte, comme : sip:anonymous-sip.com

4.1.1.3 URI en forme de nom d'hôte et d'adresse IP

On suppose dans le présent document que l'usager qui demande la confidentialité souhaite recevoir de futures demandes et réponses dans ce dialogue, mais ne souhaite pas révéler une identité qui pourrait être utilisée pour lui envoyer de nouvelles demandes en dehors du domaine d'application de ce dialogue. Pour cette raison, un traitement différent doit être recommandé pour les URI qui sont utilisés dans le contexte de l'acheminement de demandes ultérieures dans le dialogue, par opposition à l'acheminement de nouvelles demandes en dehors du contexte du dialogue.

Pour les en-têtes qui indiquent comment l'usager aimerait être contacté lors des sessions à venir (telles que l'en-tête From), la nécessité de changer le nom d'hôte peut n'être pas immédiatement évidente – si le nom d'utilisateur est 'anonyme', les demandes ne seront pas acheminables à l'utilisateur anonyme.

Parfois, le simple changement du nom d'utilisateur ne sera pas suffisant pour dissimuler l'identité de l'usager. Un fournisseur de service SIP d'un usager peut révéler de façon décisive l'identité d'un usager (si il réfléchit quelque chose comme une petite société ou un domaine personnel). Aussi dans ce cas, quand bien même l'URI de l'en-tête From ne ferait pas référence à l'utilisateur anonyme, un humain pourrait facilement deviner l'identité de l'usager et connaître la forme appropriée de son adresse d'enregistrement.

Pour ces raisons, la valeur 'anonymous.invalid' de nom d'hôte DEVRAIT être utilisée pour les URI anonymes (voir [3] pour des informations complémentaires sur le TLD DNS 'invalid' réservé). La forme recommandée complète de l'en-tête From (noter que cet en-tête From, comme tous les autres, DOIT contenir un paramètre 'tag=' valide et unique) pour l'anonymat est :

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=1928301774

Pour les en-têtes qui indiquent comment devraient être acheminées les demandes ultérieures dans le dialogue en cours (à savoir l'en-tête Contact, l'en-tête Via, et les informations de session dans le SDP) il semble qu'un usager ne puisse pas faire grand chose pour déguiser l'URI existant, parce que l'usager DOIT fournir une valeur qui lui permettra de recevoir les demandes ultérieures. Dans certains cas, un déguisement ou manquer à fournir le nom d'utilisateur, comme décrit ci-dessus, peut créer un certain niveau de confidentialité, mais le nom d'hôte est un obstacle plus significatif.

Est-il ajouté beaucoup à la confidentialité en utilisant une adresse IP plutôt qu'un nom d'hôte ? Cela n'empêche personne de collecter des informations qu'on pourrait trouver par ailleurs par une inspection minutieuse d'un message. Cependant, la résolution inverse de telles adresses est généralement triviale, et substituer une adresse IP à un nom d'hôte pourrait introduire des complications, par exemple dues aux problèmes de traversée de NAT *(traducteur d'adresse réseau)* et de pare-feu. Les en-têtes utilisés pour l'acheminement peuvent aussi s'appuyer sur certaines pratiques du DNS pour fournir des services qui seraient perdus si une adresse IP est utilisée à la place d'un nom d'hôte.

Le présent document recommande donc que la portion hôte des URI qui sont utilisés pour l'acheminement des demandes ultérieures, tels que les URI qui apparaissent dans l'en-tête Contact, NE DEVRAIENT PAS être altérés par l'agent d'utilisateur pour des considérations de confidentialité. Si ces en-têtes requièrent l'anonymat, l'usager demande ce service à un intermédiaire, à savoir un service de confidentialité.

Noter que beaucoup des considérations ci-dessus concernant l'en-tête Contact s'appliquent également bien aux en-têtes SIP dans lesquelles un nom d'hôte, plutôt qu'un URI, est utilisé pour des besoins d'acheminement (à savoir l'en-tête Via).

4.2 Expression des préférences de confidentialité

Il y a certains en-têtes qu'un agent d'utilisateur ne peut pas dissimuler lui-même, parce qu'ils sont utilisés pour l'acheminement, et qui pourraient être dissimulés par un intermédiaire qui prend ensuite la responsabilité de diriger les messages de et vers l'utilisateur anonyme. L'agent d'utilisateur doit avoir un moyen de demander de tels services de confidentialité au réseau. À cette fin, le présent document définit un nouvel en-tête SIP, Privacy, qui peut être utilisé pour spécifier le traitement de confidentialité pour les demandes et réponses.

Privacy-hdr = "Privacy" HCOLON priv-value *(";" priv-value)

priv-value = "header" / "session" / "user" / "none" / "critical" / token

Les agents d'utilisateur DEVRAIENT inclure un en-tête Privacy lorsqu'ils requièrent la confidentialité fournie par le réseau (comme décrit au paragraphe 3.3). Noter que certains intermédiaires peuvent aussi ajouter l'en-tête Privacy aux messages, incluant des services de confidentialité. Cependant, de tels intermédiaires NE DEVRAIENT faire ainsi que sur ordre d'un usager, par exemple si un usager a un accord administratif avec l'opérateur de l'intermédiaire, il va ajouter un tel en-tête Privacy. Un intermédiaire NE DOIT modifier l'en-tête Privacy en aucune façon si la priv-value "none" est déjà spécifiée.

Aujourd'hui les valeurs de priv-value sont restreintes aux options ci-dessus, bien que d'autres options puissent être définies en tant que de besoin à l'avenir (voir la Section 7). Chaque priv-value légitime peut apparaître zéro ou une fois dans un en-tête Privacy. Les valeurs actuelles sont :

header :

L'usager demande qu'un service de confidentialité obscurcisse les en-têtes qui ne peuvent être complètement expurgés des informations d'identification sans l'assistance d'intermédiaires (tels que Via et Contact). Aussi, aucun en-tête non indispensable ne devrait être ajouté par le service qui puisse révéler des informations personnelles sur l'origine de la demande.

session :

L'usager demande qu'un service de confidentialité fournisse l'anonymat pour la ou les sessions (décrite, par exemple, dans un corps de protocole de description de session [5]) initiées par ce message. Cela va masquer l'adresse IP qui devrait normalement apparaître comme origine du trafic de la session. Lorsque la confidentialité de la session est demandée, les agents d'utilisateur NE DOIVENT PAS chiffrer les corps SDP dans les messages. Noter que demander la confidentialité de session en l'absence de tout chiffrement de bout en bout de la session soulève de sérieux problèmes de sécurité (voir au paragraphe 5.2).

user :

Ce niveau de confidentialité est normalement établi seulement par les intermédiaires, afin de faire savoir que les fonctions de confidentialité de niveau usager (comme exposé au paragraphe 5.3) doivent être fournies par le réseau, vraisemblablement parce que l'agent d'utilisateur n'est pas capable de les fournir. Les agents d'utilisateur PEUVENT cependant établir ce niveau de confidentialité pour les demandes REGISTER, mais NE DEVRAIENT PAS établir le niveau de confidentialité 'user' pour les autres demandes.

none :

L'usager demande qu'un service de confidentialité n'applique aucune fonctions de confidentialité à ce message, sans considération de tout profil pré-provisionné pour l'usager ou de comportement par défaut du service. Les agents d'utilisateur peuvent spécifier cette option lorsqu'ils sont forcés d’acheminer un message à travers un service de confidentialité qui va, si aucun en-tête Privacy n'est présent, appliquer des fonctions de confidentialité que l'usager ne désire pas pour ce message. Les intermédiaires NE DOIVENT PAS retirer ou altérer un en-tête Privacy dont la priv-value est 'none'. Les agents d'utilisateur NE DOIVENT PAS remplir d'autres priv-values (y compris 'critical') dans un en-tête Privacy qui contient une valeur de 'none'.

critical:

L'usager atteste que les services de confidentialité demandés pour ce message sont critiques, et que donc, si ces services de confidentialité ne peuvent être fournis par le réseau, cette demande devrait être rejetée. Le caractère critique ne peut pas être géré correctement pour les réponses.

Lorsqu'un en-tête Privacy est construit, il DOIT comporter soit la valeur 'none', soit une ou plusieurs des valeurs 'user', 'header' et 'session' (dont chacune ne DOIT apparaître qu'une fois au plus) qui PEUT à son tour être suivie par l'indicateur 'critical'.

Le tableau suivant spécifie les extensions au Tableau 2 de [1].

Champ d'en-tête	où	proxy	ACK	BYE	CAN	INV	OPT	REG
Privacy		amrd	o	o	o	o	o	o
Champ d'en-tête			SUB	NOT	PRK	IFO	UPD	MSG
Privacy			o	o	o	o	o	o

4.3 Acheminement des demandes sur les services de confidentialité

La façon la plus évidente pour qu'un agent d'utilisateur invoque la fonction de confidentialité est de diriger une demande par un intermédiaire connu pour agir comme service de confidentialité. Faire ainsi entraîne traditionnellement la configuration d'en-têtes Route pré chargés qui appellent le service de confidentialité.

Il est RECOMMANDÉ que les fournisseurs de service couplent la fonction de service de confidentialité avec un mandataire local de sortie. Les usagers peuvent ainsi envoyer leurs messages qui requièrent la confidentialité à travers leur chemin de sortie usuel. Les usagers ne devraient cependant pas supposer que le domaine administratif qui est la destination de la demande sera d'accord et capable d'effectuer la fonction de service de confidentialité en leur nom. Si l'usager d'origine souhaite garder secret son domaine administratif local, il doit alors utiliser un service d'anonymat tiers en dehors de tout domaine administratif principal associé à la session.

Il est fortement RECOMMANDÉ aux agents d'utilisateur d'utiliser la sécurité de la couche réseau ou transport, telle que TLS, en contactant un service de confidentialité. Dans l'idéal, les usagers DEVRAIENT établir une connexion directe (c'est-à-dire, un en-tête Route pré chargé) avec un service de confidentialité ; cela va à la fois permettre à l'usager d'inspecter un certificat présenté par le service de confidentialité, et cela va assurer la confidentialité des demandes en réduisant les chances que les informations que le service de confidentialité va masquer soient révélées avant qu'un message n'arrive au service de confidentialité. En établissant une connexion directe à un service de confidentialité, l'usager élimine aussi la possibilité que des intermédiaires puissent retirer des demandes de confidentialité. Si une connexion directe est impossible, les usagers DEVRAIENT utiliser un mécanisme comme SIPS pour garantir l'utilisation de la sécurité de couche inférieure sur tout le chemin vers le service de confidentialité.

Si un agent d'utilisateur pense qu'il envoie une demande directement à un service de confidentialité, il DEVRAIT inclure un en-tête Proxy-Require contenant une nouvelle option-tag, 'privacy', en particulier lorsque la priv-value 'critical' est présente dans l'en-tête Privacy. De cette façon, dans le cas peu vraisemblable où l'agent d'utilisateur enverrait une demande à un intermédiaire qu ne prend pas en charge les extensions décrites dans le présent document, la demande va échouer. Noter qu'à cause du comportement particulier du service de confidentialité (décrit à la Section 5), aucun intermédiaire ultérieur dans le chemin de signalisation de la demande n'aura aussi besoin de prendre en charge l'étiquette d'option 'privacy' - une fois que le service de confidentialité a accompli toutes les fonctions de confidentialité requises, l'étiquette d'option 'privacy' est retirée de l'en-tête Proxy-Require.

4.4 Acheminement des réponses aux services de confidentialité

S'assurer que les réponses vont passer par un service de confidentialité est un petit peu plus compliqué. Le chemin traversé par les réponses SIP est le même que le chemin sur lequel a voyagé la demande. Et donc, l'agent d'utilisateur qui répond ne peut, par exemple, forcer l'injection d'un service de confidentialité dans le chemin de réponse après qu'il a reçu une demande.

Ce que peut cependant faire un agent d'utilisateur qui répond est de s'assurer que le chemin par lequel les demandes l'atteignent traverse son service de confidentialité. Dans certaines architectures, la fonction de service de confidentialité sera remplie par le même serveur que celui auquel les demandes sont envoyées pour le domaine administratif local, et donc, il va automatiquement être sur le chemin des demandes entrantes. Cependant, si ce n'est pas le cas, l'usager devra s'assurer que les demandes sont dirigées à travers un service de confidentialité tiers.

Une façon de le faire est de procurer un URI 'anonymous callback' *(rappel anonyme)* provenant du service tiers et de le distribuer comme une address-of-record *(adresse d'enregistrement)*. Un fournisseur de service de confidentialité pourrait offrir ces URI de rappel anonyme aux usagers de la même façon qu'un fournisseur de service SIP ordinaire alloue des addresses-of-record. L'usager enregistrerait alors son address-of-record normale comme adresse de contact auprès du service tiers.

Autrement, un agent d'utilisateur pourrait envoyer des demandes REGISTER à travers un service de confidentialité avec une demande de confidentialité de niveau 'user'. Cela va permettre au service de confidentialité d'insérer des URI d'en-tête Contact anonymes. Les demandes envoyées à l'address-of-record conventionnelle de l'usager atteindront alors les appareils de l'usager sans révéler aucune adresse de contact utilisable.

Finalement, un usager pourrait générer un script CPL ([7]) qui va diriger les demandes sur un service d'anonymat.

Il est aussi conseillé aux usagers d'utiliser la sécurité de couche transport ou réseau sur le chemin de réponse. Cela peut impliquer d'enregistrer un URI SIPS et/ou de maintenir des connexions TLS persistantes sur lesquelles leur agent d'utilisateur recevra les demandes.

Les services de confidentialité PEUVENT à leur tour acheminer les demandes à travers d'autres services de confidentialité. Cela peut être nécessaire si un service de confidentialité ne prend pas en charge une fonction de confidentialité particulière, mais qu'il sait qu'un homologue le fait. Les services de confidentialité peuvent aussi se partager entre les réseaux qui échangent le trafic de session entre eux afin de mieux déguiser les participants à une session, bien qu'aucune architecture ou méthode spécifique pour ce faire ne soit décrite dans le présent document.

5. Comportement du service de confidentialité

Le présent document définit un nouveau rôle logique SIP appelé "service de confidentialité". Le rôle de service de confidentialité est instancié par un intermédiaire du réseau, fréquemment par des entités qui peuvent agir comme des serveurs mandataires SIP. La fonction d'un service de confidentialité est de fournir des fonctions de confidentialité pour les messages SIP qui ne peuvent pas être fournis par les agents d'utilisateur eux-mêmes.

Lorsque un message arrive à un serveur qui peut agir comme service de confidentialité, le service DEVRAIT évaluer le niveau de confidentialité demandé dans un en-tête Privacy. Habituellement, seuls les services explicitement demandés devraient être appliqués. Cependant, des services de confidentialité PEUVENT avoir des moyens en dehors de SIP pour vérifier les préférences de l'usager (telles qu'un profil d'usager prédéfini) et donc ils PEUVENT effectuer ces autres fonctions de confidentialité sans un en-tête Privacy explicite. Effectuer même une fonction de confidentialité de niveau usager dans un service de confidentialité pourrait être utile, par exemple, lorsque un usager envoie des messages à partir d'un client traditionnel qui accepte l'en-tête Privacy, ou d'un agent d'utilisateur qui ne permet pas à l'usager de configurer les valeurs des en-têtes qui pourraient révéler des informations personnelles. Cependant, si la valeur de l'en-tête Privacy de 'none' est spécifiée dans un message, les services de confidentialité NE DOIVENT PAS effectuer de fonction de confidentialité et NE DOIVENT PAS retirer ou modifier l'en-tête Privacy.

Les services de confidentialité DOIVENT mettre en œuvre la prise en charge des jetons de confidentialité 'none' et 'critical', et PEUVENT mettre en œuvre tous les autres niveaux de confidentialité décrits au paragraphe 4.2 aussi bien que toute extension qui ne serait pas précisée dans le présent document. Dans certains cas, le service de confidentialité ne sera pas capable de satisfaire le niveau de confidentialité demandé. Si le niveau de confidentialité 'critical' est présent dans l'en-tête Privacy d'une demande, et si le service de confidentialité est incapable d'effectuer tous les niveaux de confidentialité spécifiés dans l'en-tête Privacy, il DOIT alors rejeter la demande avec un code de réponse 500 (Erreur du serveur). La phrase de cause de la ligne status de la réponse DEVRAIT contenir le texte approprié indiquant qu'il y a eu une défaillance de confidentialité ainsi qu'une énumération de la ou des priv-value qui n'étaient pas acceptées par le service de confidentialité (la phrase de cause DEVRAIT aussi respecter tout en-tête Accept-Language dans la demande si possible).

Lorsque un service de confidentialité effectue une des fonctions correspondant à un niveau de confidentialité figurant sur la liste de l'en-tête Privacy, il DEVRAIT retirer la priv-value correspondante de l'en-tête Privacy - autrement, tout autre service de confidentialité impliqué dans l'acheminement de ce message pourrait inutilement appliquer la même fonction, ce qui dans de nombreux cas serait indésirable. Lorsque la dernière priv-value (en ne comptant pas 'critical') a été retirée de l'en-tête Privacy, le champ d'en-tête Privacy tout entier DOIT être retiré d'un message.

Lorsque le service de confidentialité retire l'en-tête Privacy tout entier, si le message est une demande, le service de confidentialité DOIT aussi retirer toute étiquette d'option 'privacy' du champ d'en-tête Proxy-Require de la demande.

5.1 En-tête de confidentialité

Si un niveau de confidentialité de 'header' est demandé, l'usager d'origine a alors demandé que le service de confidentialité l'aide à masquer les en-têtes qui pourraient sans cela révéler des informations sur l'origine de la demande. Cependant, les valeurs qui ont été ainsi masquées doivent être récupérables lorsque des messages ultérieurs dans le dialogue doivent être acheminés à l'agent d'utilisateur d'origine. Afin de fournir ces fonctions, le service de confidentialité doit fréquemment agir comme un agent d'utilisateur de boucle locale transparent (B2BUA).

Premièrement, une demande de confidentialité d'en-tête entraîne que le serveur NE DEVRAIT PAS ajouter d'en-tête au message qui révèlerait une identité ou des informations personnelles, y compris les suivants : Call-Info, Server, et Organization. Tous ceux-ci fournissent des informations facultatives qui pourraient révéler des faits concernant l'usager qui a demandé l'anonymat.

Les services de confidentialité travaillant sur les demandes DEVRAIENT retirer tous les en-têtes Via qui ont été ajoutés à la demande avant son arrivée au service de confidentialité (pratique appelée "nettoyage de Via") et DEVRAIENT ensuite ajouter un seul en-tête Via les représentant eux-mêmes. Noter que la dernière valeur d'un tel champ d'en-tête Via dans une demande contient une adresse IP ou nom d'hôte qui désigne le client d'origine, et les valeurs suivantes de champ d'en-tête Via peuvent indiquer les hôtes dans le même domaine administratif que le client. Aucun nettoyage de Via n'est exigé lors du traitement des réponses.

Les en-têtes Contact sont ajoutés par les agents d'utilisateur à la fois aux demandes et aux réponses. Un service de confidentialité DEVRAIT remplacer la valeur de l'en-tête Contact d'un message par un URI qui ne fasse pas référence à l'origine du message (tel que l'URI anonyme décrit au paragraphe 4.1.1.3). L'URI qui remplace la valeur existante du champ d'en-tête Contact DOIT faire référence au service de confidentialité.

De façon similaire au nettoyage de Via, un service de confidentialité DEVRAIT aussi nettoyer tous les en-têtes Record-Route qui ont été ajoutés à une demande avant qu'elle n'atteigne le service de confidentialité – noter toutefois qu'aucun de ces en-têtes ne sera présent si il y a seulement un bond entre l'agent d'utilisateur d'origine et le service de confidentialité, comme recommandé ci-dessus. De tels en-têtes Record-Route peuvent aussi divulguer des informations sur le domaine administratif du client.

Pour les besoins du présent document, on suppose que le service de confidentialité a conservé localement les valeurs de tous les en-têtes retirés, ce qui requiert du service de confidentialité qu'il conserve une quantité significative d'états dialogue par dialogue. Lorsque des demandes ou réponses ultérieures associées au dialogue atteignent le service de confidentialité, il DOIT restaurer les valeurs des en-têtes Via, Record-Route/Route ou Contact qu'il avait précédemment retirés au nom de la confidentialité. Il peut y avoir des solutions de remplacement (en dehors du domaine d'application du présent document) pour effectuer cette fonction qui n'exigent pas de conserver l'état dans le service de confidentialité (cela signifie habituellement d'utiliser le chiffrement et de trouver un moyen de conserver les valeurs dans la signalisation).

Les procédures suivantes sont RECOMMANDÉES pour le traitement du champ d'en-tête Record-Route des demandes et des réponses, qui posent des problèmes particuliers à un service de confidentialité :

Lorsqu'un service de confidentialité traite (au nom de l'expéditeur) une demande qui contient une ou plusieurs valeurs de champ d'en-tête Record-Route, le service de confidentialité doit nettoyer ces valeurs de la demande et se souvenir à la fois des identifiants de dialogue et des valeurs de champ d'en-tête Record-Route dans leur ordre. Comme décrit ci-dessus, il doit aussi remplacer le champ d'en-tête Contact par un URI qui l'indique lui-même. Lorsque une réponse arrive avec le même identifiant de dialogue au service de confidentialité, celui-ci doit ré appliquer toutes les valeurs de champ d'en-tête Record-Route à la réponse dans le même ordre, et il doit ensuite ajouter un URI le représentant lui-même au champ d'en-tête Record-Route de la réponse. Si la réponse contient des valeurs de champ d'en-tête Record-Route propres, elles doivent aussi être incluses (dans l'ordre) dans le champ d'en-tête Record-Route après l'URI représentant le service de confidentialité.

Noter que lorsque un service de confidentialité traite une demande et fournit la confidentialité au nom de la destination de la demande, fournir la confidentialité pour les en-têtes Record-Route vers l'aval du service de confidentialité est significativement plus compliqué. Le présent document ne recommande aucun moyen pour restaurer pleinement ces en-têtes si ils ont été enlevés.

5.2 Confidentialité de session

Si un niveau de confidentialité de 'session' est requis, l'usager a alors demandé que le service de confidentialité rende anonyme le trafic de session (par exemple, pour les appels téléphoniques SIP, le support audio) associé à ce dialogue.

La spécification SIP indique que les intermédiaires tels que les serveurs mandataires ne peuvent pas inspecter et modifier les corps de message. Le rôle logique de service de confidentialité DOIT donc agir comme agent d'utilisateur de boucle locale afin de fournir la confidentialité du support, en terminant effectivement et en générant à nouveau les messages qui initient une session (bien qu'à l'appui d'une confidentialité de session, le service de confidentialité n'ait pas besoin de modifier les en-têtes qui caractérisent l'origine ou la destination lorsque la demande est générée à nouveau). Afin d'introduire un "anonymiseur" de trafic de session, le service de confidentialité a besoin de contrôler un boîtier de médiation [8] qui puisse fournir une source apparente et un collecteur pour le trafic de session. Les détails de la mise en œuvre d'un "anonymiseur", et les modifications qui doivent être faites aux corps du protocole de description de session (SDP [5]) dans les messages qui initient une session sont dehors du domaine d'application du présent document.

Le risque, bien sûr, d'utiliser un tel "anonymiseur" est qu'il fait lui-même partie de la communication. Pour cette raison, demander la confidentialité de niveau session sans avoir recours à quelque sorte de sécurité de bout en bout pour le trafic de session (avec le support RTP [6], par exemple, SRTP [4]) N'EST PAS RECOMMANDÉ.

5.3 Application des fonctions de confidentialité de niveau utilisateur à un service de confidentialité

Si un niveau de confidentialité de 'user' est requis, l'usager d'origine a alors demandé que les services de confidentialité effectuent les fonctions de confidentialité de niveau usager décrites au paragraphe 4.1.

Noter que le service de confidentialité DOIT retirer tous les en-têtes d'information non essentiels qui ont pu être ajoutés par l'agent d'utilisateur, y compris Subject, Call-Info, Organization, User-Agent, Reply-To et In-Reply-To.

De façon significative, la confidentialité de niveau usager pourrait entraîner la modification de l'en-tête From, en changeant sa valeur d'origine en une valeur "anonymous". Avant la publication actuelle de la spécification SIP, la modification des valeurs des en-têtes To et From par les intermédiaires n'était pas permise, et aurait résulté en une mauvaise mise en correspondance des dialogues par les points d'extrémité. Actuellement; la mise en correspondance des dialogues utilise seulement les étiquettes dans les en-têtes To et From, plutôt que le champ d'en-tête entier. Et donc, avec les nouvelles règles les valeurs d'URI dans les en-têtes To et From eux-mêmes pourraient être altérées par les intermédiaires. Cependant, certains clients traditionnels peuvent considérer cela comme une condition d'erreur si la valeur de l'URI dans l'en-tête From a été altérée entre la demande et la réponse.

Aussi, effectuer la fonction de confidentialité de niveau usager PEUT entraîner la modification de l'en-tête Call-ID, car le Call-ID contient souvent un nom d'hôte ou l'adresse IP correspondant au client d'origine. Ce champ est essentiel à la mise en correspondance des dialogues, et il ne peut pas être altéré par les intermédiaires.

Donc, chaque fois qu'un service de confidentialité a besoin de modifier un des en-têtes de mise en correspondance du dialogue pour des raisons de confidentialité, il DEVRAIT agir comme un agent d'utilisateur de boucle locale transparent, et il DOIT conserver les anciennes valeurs des en-têtes de correspondance de dialogue. Ces valeurs DOIVENT être restaurées dans tout message envoyé à l'agent d'utilisateur d'origine.

6. Considérations pour la sécurité

Les messages qui demandent la confidentialité exigent la confidentialité et l'intégrité. Sans l'intégrité, les fonctions de confidentialité demandées pourraient être dégradées ou éliminées, exposant potentiellement les informations sur l'identité. Sans la confidentialité, l'espionnage sur le réseau (ou sur tout intermédiaire entre l'usager et le service de confidentialité) pourrait voir les informations très personnelles que l'usager a demandé au service de confidentialité de dissimuler.

Toutes les fonctions de confidentialité fournies par le réseau dans le présent document impliquent une grande quantité de confiance dans le service de confidentialité. Les usagers ne devraient faire confiance qu'aux services de confidentialité avec lesquels ils sont plus ou moins en relation.

Les opérateurs de services de confidentialité devraient être conscients qu'ils sont sous le regard des entités en aval, un service de confidentialité sera la seule source à laquelle puissent être rattachés les messages anonymes.

Noter que les mécanismes d'authentification, y compris la méthode d'authentification par résumé décrite dans la spécification SIP, sont en dehors du domaine d'application des considérations sur la confidentialité dans le présent document. Révéler l'identité à travers l'authentification est très sélectif, et peut ne pas résulter en la compromission d'informations privées. Évidemment, les usagers qui ne souhaitent pas révéler leur identité aux serveurs qui produisent des mises en cause d'authentification PEUVENT choisir de ne pas répondre à de telles mises en cause.

7. Considérations relatives à l'IANA

Le présent document définit un nouveau champ d'en-tête SIP appelé "Privacy" qui permet à un agent d'utilisateur de demander un certain degré de confidentialité pour un message. Le comportement associé à cet en-tête est spécifié au paragraphe 4.2. Cet en-tête a été ajouté au sous-registre des en-têtes à l'adresse http://www.iana.org/assignments/sip-parameters.

Nome d'en-tête : Privacy
Forme compacte : aucune n'est définie

Le présent document crée aussi un registre IANA pour les valeurs qui remplissent l'en-tête Privacy. Ce registre devrait être indexé par des jetons priv-value et devrait contenir une brève description sémantique de la nouvelle valeur. Les valeurs actuelles de l'en-tête "Privacy" sont les suivantes :

- o user : Demande que les services de confidentialité fournissent une fonction de confidentialité de niveau usager
- o header : Demande que les services de confidentialité modifient les en-têtes qui ne peuvent pas être réglés arbitrairement par l'usager (Contact/Via).
- o session : Demande que les services de confidentialité fournissent la confidentialité pour le support de session
- o none : Les services de confidentialité ne doivent effectuer aucune fonction de confidentialité
- o critical : le service de confidentialité doit effectuer les services spécifiés ou rejeter la demande

Les nouvelles valeurs pour l'en-tête "Privacy" ne peuvent être définies que par Consensus IETF incluant la publication de RFC (RFC2434). L'enregistrement auprès de l'IANA pour les valeurs de champ d'en-tête "Privacy" est exigé ainsi que la publication d'une RFC.

Les auteurs d'extensions au protocole SIP qui exposent des informations personnelles sur les participants à des sessions sont mis en garde contre l'extension de l'en-tête "Privacy" – il est préférable de créer de nouveaux mécanismes d'identité dont la confidentialité puisse être gérée par l'agent d'utilisateur sans intermédiaire.

Le présent document définit aussi une nouvelle étiquette d'option SIP, 'privacy', qui représente la prise en charge de l'extension définie dans le présent document.

Références normatives

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley et E. Schooler, "SIP : Protocole d'initialisation de session", RFC3261, juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393).

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

[3] D. Eastlake 3rd et A. Panitz, "Noms réservés de niveau supérieur du DNS", RFC2606, BCP 32, juin 1999.

Références informatives

[4] M. Baugher, D. McGrew, D. Oran, R. Blom, E. Carrara, M. Naslund et K. Normann, "Protocole de transport sécurisé en temps réel (SRTP)", RFC3711, mars 2004.

[5] M. Handley et V. Jacobson, "SDP : Protocole de description de session", RFC2327, avril 1998. *(Obsolète; voir RFC4566)*

[6] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : protocole de transport pour applications en temps réel", RFC1889, janvier 1996. *(Obsolète, voir* RFC3550 *STD64)*

[7] J. Lennox, X. Wu, H. Schulzrinne, "Langage de traitement d'appel (CPL) : un langage pour le contrôle d'usager des services de téléphonie Internet", RFC3880, octobre 2004.

[8] P. Srisuresh et autres, "Architecture et cadre de communication par boîtier de médiation", RFC3303, août 2002. *(Information)*

Adresse de l'auteur

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520 US
Téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz
URI : http://www.neustar.biz/

Remerciements

L'auteur tient à remercier Allison Mankin, Rohan Mahy, Eric Rescorla, Mark Watson, Cullen Jennings, Robert Sparks, Jonathan Rosenberg, Ben Campbell, Tom Gray et John Elwell de leurs commentaires.

Déclaration complète de droits de reproduction

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