Groupe de travail Réseau
Request for Comments : 3725
BCP : 85
Catégorie : Bonnes pratiques actuelles
Traduction Claude Brière de L'Isle

J. Rosenberg, dynamicsoft
J. Peterson, Neustar
H. Schulzrinne, Columbia University
G. Camarillo, Ericsson
avril 2004

Bonnes pratiques actuelles pour le contrôle d'appel de tiers (3pcc) dans le protocole d'initialisation de session (SIP)

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright
Copyright (C) The Internet Society (2004).

Résumé
Le contrôle d'appel de tiers se réfère à la capacité d'une entité de créer un appel dans lequel la communication est en fait entre d'autres parties. Le contrôle d'appel de tiers est possible en utilisant les mécanismes spécifiés dans le protocole d'initialisation de session (SDP, *Session Initiation Protocol*). Cependant, il y a plusieurs approches possibles, dont chacune a des avantages et inconvénients différents. Le présent document discute des bonnes pratiques actuelles pour l'usage de SIP pour le contrôle d'appel de tiers.

Table des Matières

1. Introduction

Dans le contexte de la téléphonie traditionnelle, le contrôle d'appel de tiers permet à une entité (qu'on appelle le contrôleur)

d'établir et gérer une relation de communication entre deux, ou plus, autres parties. Le contrôle d'appel de tiers (en abrégé 3pcc) est souvent utilisé pour les services d'opérateur (où un opérateur crée un appel qui connecte ensemble deux participants) et pour les conférences.

De même, de nombreux services SIP sont possibles grâce au contrôle d'appel de tiers. Cela inclut les services traditionnels sur le RTPC, mais aussi des nouveaux, tels que de "cliquer pour numéroter". Cliquer pour numéroter permet à un usager de cliquer sur une page de la Toile lorsque il souhaite parler avec un représentant du service client. Le serveur de la Toile crée alors un appel entre l'usager et un représentant du service client. L'appel peut être entre deux téléphones, un téléphone et un hôte IP, ou deux hôtes IP.

Le contrôle d'appel de tiers est possible en utilisant seulement les mécanismes spécifiés dans la [RFC3261]. Bien sûr, de nombreux flux d'appel différents sont possibles, dont chacun va fonctionner avec des agents d'utilisateur conformes à SIP. Cependant, il y a des avantages et des inconvénients pour chacun de ces flux. L'usage du contrôle d'appel de tiers devient aussi plus complexe lorsque certaines parties de l'appel utilisent des extensions de SIP ou des caractéristiques facultatives de SIP. En particulier, l'usage de la [RFC3312] (utilisée pour le couplage de la signalisation à la réservation de ressources) avec le contrôle d'appel de tiers est non trivial, et est exposé à la Section 9. De même, l'usage d'un support précoce (où les données de session sont échangées avant que l'appel soit accepté) avec le contrôle d'appel de tiers n'est pas trivial ; tous les deux spécifient la façon dont les agents d'utilisateur génèrent et répondent à SDP, et la façon de le faire pour tous les deux en même temps n'est pas claire. C'est ce qui est exposé à la Section 8.

Le présent document sert de bonnes pratiques actuelles pour mettre en œuvre le contrôle d'appel de tiers sans usage d'aucune extension conçue spécifiquement pour cela. La Section 4 présente les flux d'appel connus qui peuvent utilisés pour réaliser le contrôle d'appel de tiers, et fournit des lignes directrices sur leur usage. La Section 9 discute des interactions de la [RFC3312] avec le contrôle d'appel de tiers. La Section 8 discute des interactions du support précoce avec le contrôle d'appel de tiers. La Section 10 donne des exemple d'applications qui utilisent les flux recommandés.

2. Terminologie

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 la [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

3. Définitions

Les termes suivants sont utilisés dans le présent document :

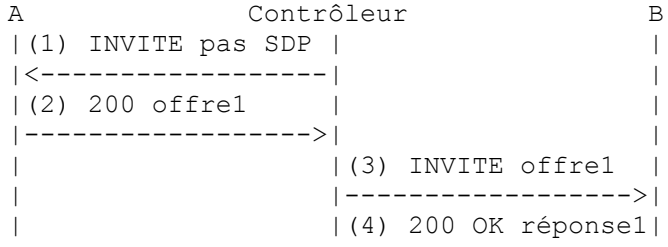
3pcc *(Third Party Call Control)* contrôle d'appel de tiers, qui se réfère à la capacité générale de manipuler des appels entre d'autres parties.

Contrôleur : c'est un agent d'utilisateur SIP qui souhaite créer une session entre deux autres agents d'utilisateur.

4. Établissement d'un appel 3pcc

L'opération primitive principale du contrôle d'appel de tiers est l'établissement d'une session entre les participants A et B. L'établissement de cette session est orchestré par un tiers, qu'on appelle le contrôleur.
Cette section documente trois flux d'appel que peut utiliser le contrôleur afin de réaliser cette opération primitive.

4.1 Flux I



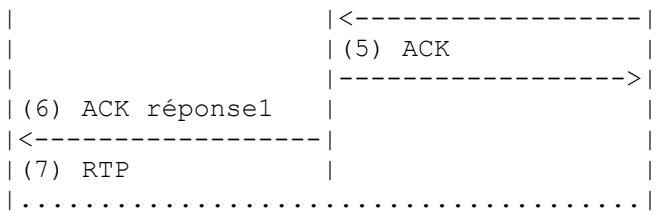


Figure 1

Le flux d'appel pour Flux I est montré à la Figure 1. Le contrôleur envoie d'abord un INVITE A (1). Cet INVITE n'a pas de description de session. Le téléphone de A sonne, et A répond. Il en résulte un 200 OK (2) qui contient une offre [RFC3264]. Le contrôleur doit envoyer sa réponse dans le ACK, comme exigé par la [RFC3261]. Pour obtenir la réponse, il envoie l'offre qu'il a obtenu de A (offre1) dans un INVITE à B (3). Le téléphone de B sonne. Lorsque B décroche, le 200 OK (4) contient la réponse à son offre, réponse1. Le contrôleur envoie un ACK à B (5), puis passe la réponse1 à A dans un ACK qu'il lui envoie (6). Parce que l'offre a été générée par A, et la réponse générée par B, la session support réelle est entre A et B. Donc, les supports s'écoulent entre eux (7).

Ce flux est simple, n'exige aucune manipulation de SDP par le contrôleur, et fonctionne pour tous les types de supports pris en charge par les deux points d'extrémité. Cependant, il y a un problème sérieux de fin de temporisation. L'utilisateur B peut ne pas répondre immédiatement à l'appel. Le résultat est que le contrôleur ne peut pas envoyer tout de suite le ACK à A. Cela amène A à retransmettre périodiquement la réponse 200 OK. Comme spécifié au paragraphe 13.3.1.4 de la [RFC3261], le 200 OK va être retransmis pendant 64*T1 secondes. Si un ACK n'est pas arrivé dans ce délai, l'appel est considéré comme ayant échoué. Cela limite l'applicabilité de ce flux aux scénarios où le contrôleur sait que B va répondre immédiatement à l'INVITE.

4.2 Flux II

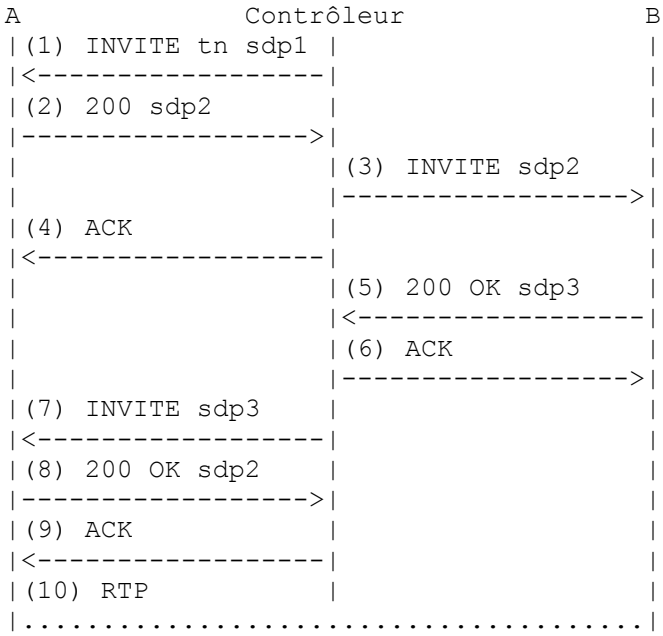


Figure 2

Un autre flux, Flux II, est montré à la Figure 2. Le contrôleur envoie d'abord un INVITE à l'usager A (1). C'est un INVITE standard contenant une offre (sdp1) avec une seule ligne de support audio, un codec, un numéro d'accès aléatoire (mais pas zéro) et une adresse de connexion de 0.0.0.0. Cela crée un flux de supports initial qui tombe dans un "trou noir" *(marqué "tn" dans les diagrammes)*, car aucun support (ou paquet RTCP [RFC3550]) ne va s'écouler de A. Le INVITE fait sonner le téléphone de A.

Noter que l'usage de 0.0.0.0, bien que recommandé par la [RFC3264], a de nombreux inconvénients. On prévoit qu'une future spécification recommandera l'usage d'un domaine au sein du domaine de niveau supérieur .invalide du DNS au lieu de l'adresse IP 0.0.0.0. Par suite, les mises en œuvre sont invitées à surveiller l'arrivée de tels développements.

Lorsque A répond (2), le 200 OK contient une réponse, sdp2, avec une adresse valide dans la ligne de connexion. Le contrôleur

envoie un ACK (4). Il génère alors un second INVITE (3). Cet INVITE est adressé à l'usager B, et il contient sdp2 comme offre à B. Noter que le rôle de sdp2 a changé. Dans le 200 OK (message 2), c'était une réponse, mais dans l'INVITE, c'est une offre. Heureusement, toutes les réponses valides sont des offres initiales valides. Cet INVITE fait sonner le téléphone de B. Quand il décroche, il génère un 200 OK (5) avec une réponse, sdp3. Le contrôleur génère alors un ACK (6). Ensuite, il envoie un re-INVITE à A (7) qui contient sdp3 comme offre. Une fois encore, il y a un renversement de rôle. sdp3 était une réponse, et maintenant c'est une offre. Heureusement, une réponse à une réponse refondue en offre est, à son tour, une offre valide. Ce re-INVITE génère un 200 OK (8) avec sdp2, en supposant que A ne décide pas de changer des aspects de la session par suite de ce re-INVITE. Ce 200 OK reçoit un accusé de réception (9), et ensuite les supports peuvent s'écouler de A vers B. Les supports de B vers A pourront déjà commencer à s'écouler une fois que le message 5 sera envoyé.

Ce flux a l'avantage que toutes les réponses finales sont immédiatement acquittées. Il ne souffre donc pas de problèmes de fin de temporisation et d'inefficacité de message du flux 1. Cependant, il a aussi des problèmes. D'abord, il exige que le contrôleur sache les types de support à utiliser pour l'appel (car il doit générer un "trou noir" SDP, qui exige des lignes de support). Ensuite, le premier INVITE à A (1) contient des supports avec une adresse de connexion de 0.0.0.0. Le contrôleur s'attend à ce que la réponse contienne une adresse de connexion valide, différente de zéro, pour A. Cependant, l'expérience a montré que de nombreux UA répondent à une offre d'une adresse de connexion 0.0.0.0 par une réponse contenant une adresse de connexion 0.0.0.0. La spécification d'offre/réponse de la [RFC3264] dit explicitement aux mises en œuvre de ne pas faire cela, mais au moment de la publication du présent document, de nombreuses mises en œuvre le font toujours. Si A devait répondre par une adresse de connexion 0.0.0.0 en sdp2, le flux ne fonctionnerait pas.

Cependant, la faute la plus sérieuse dans ce flux est l'hypothèse que le 200 OK au re-INVITE (message 8) contient le même SDP que dans le message 2. Il se peut que ce ne soit pas le cas. Si ce ne l'est pas, le contrôleur doit faire un re-INVITE à B avec ce SDP (disons, sdp4) qui peut avoir pour résultat un SDP différent, sdp5, dans le 200 OK provenant de B. Ensuite, le contrôleur a besoin de faire à nouveau un re-INVITE à A, et ainsi de suite. Le résultat est une boucle infinie de re-INVITE. Il est possible de casser ce cycle en ayant des UA très intelligents qui peuvent retourner le même SDP chaque fois que possible, ou des contrôleurs vraiment intelligents qui peuvent analyser le SDP pour déterminer si un re-INVITE est réellement nécessaire. Cependant, on souhaite que ce mécanisme reste simple, et éviter dans le contrôleur la capacité SDP. Par suite, ce flux ne fonctionne pas vraiment. Il est donc NON RECOMMANDÉ.

4.3 Flux III

Figure 3

La Figure 3 montre un troisième flux, Flux III.

D'abord, le contrôleur envoie un INVITE (1) à l'usager A sans aucun SDP (ce qui est bien, car cela signifie que le contrôleur n'a pas besoin de supposer quoi que ce soit sur la composition des supports de la session). Le téléphone de A sonne. Lorsque A décroche, un 200 OK est généré (2) qui contient son offre, offre1. Le contrôleur génère un ACK immédiat qui contient une réponse (3). Cette réponse est un "trou noir" SDP, avec son adresse de connexion égale à 0.0.0.0.

Le contrôleur envoie alors un INVITE à B sans SDP (4). Cela fait sonner le téléphone de B. Lorsque il décroche, un 200 OK est envoyé, contenant son offre, offre2 (5). Ce SDP est utilisé pour créer un re-INVITE en retour vers A (6). Ce re-INVITE se fonde sur l'offre2, mais peut avoir besoin d'être réorganisé pour correspondre aux lignes de support, ou pour garnir des lignes de support. Par exemple, si l'offre1 contenait une ligne audio et une ligne vidéo, dans cet ordre, mais si l'offre2 contenait juste une ligne audio, le contrôleur aurait besoin d'ajouter une ligne vidéo à l'offre (en réglant son accès à zéro) pour créer l'offre2'. Comme c'est un re-INVITE, il devrait s'achever rapidement dans le cas général. C'est bien parce que l'usager B retransmet son 200 OK, attendant un ACK. Le SDP dans le 200 OK (7) provenant de A, réponse2', peut aussi avoir besoin d'une réorganisation ou d'une garniture avant l'envoi dans le ACK pour B (8) comme réponse2. Finalement, un ACK est envoyé à A (9), et les supports peuvent ensuite s'écouler.

Ce flux a de nombreux avantages. D'abord, il va normalement fonctionner sans aucune retransmission parasite ni fin de temporisation (bien que cela puisse quand même arriver si on ne répond pas assez rapidement à un re-INVITE). Ensuite, il n'exige pas que le contrôleur devine le support qui sera utilisé par les participants.

Il y a quelques inconvénients. Le contrôleur a besoin d'effectuer des manipulations de SDP. Précisément, il doit prendre un SDP, et générer un autre SDP qui a la même composition de supports, mais a une adresse de connexion égale à 0.0.0.0. Ceci est nécessaire pour le message 3. Ensuite, il peut avoir besoin de réordonner et garnir le SDP X, afin que ses lignes de supports correspondent à celles d'un autre SDP, Y. Troisièmement, l'offre de B (offre2) peut n'avoir pas de codecs ou de flux de supports en commun avec l'offre de A (offre1). Le contrôleur va devoir détecter cette condition, et terminer l'appel. Finalement, le flux est beaucoup plus compliqué que le simple et élégant Flux I (Figure 1).

4.4 Flux IV

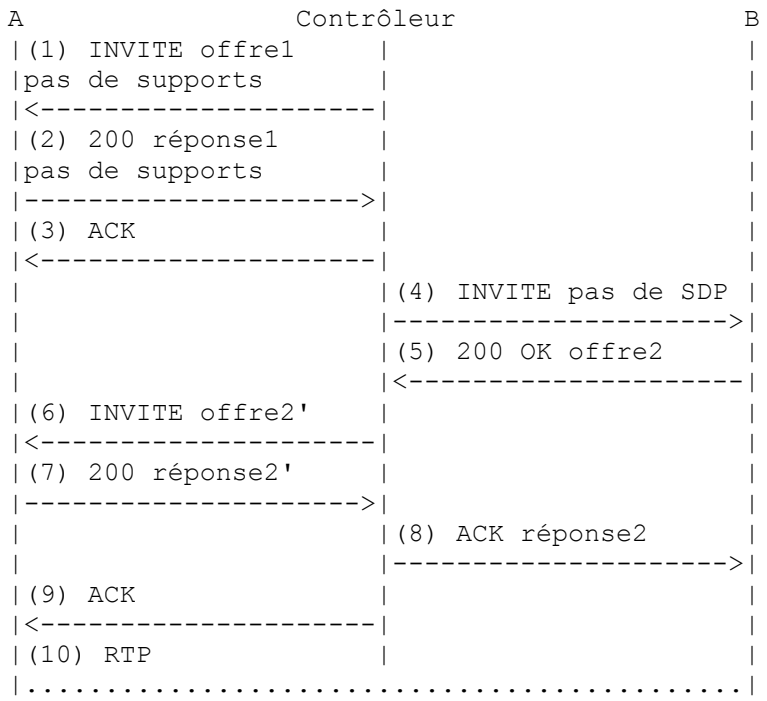


Figure 4

Le Flux IV montre une variation du Flux III qui réduit sa complexité. Le flux réel de messages est identique, mais le placement et la construction du SDP diffèrent. L'INVITE (1) initial contient un SDP sans aucun support, ce qui signifie qu'il n'y a pas de ligne m. Ceci est valide, et implique que la composition de supports de la session va être établie plus tard par un re-INVITE [RFC3264]]. Une fois que l'INVITE est reçu, l'usager A est alerté. Lorsque il répond à l'appel, le 200 OK (2) a une réponse qui n'a elle non plus pas de support. Le contrôleur en accuse réception (3). Le flux à partir de ce point est identique à celui du Flux III. Cependant, les manipulations requises pour convertir l'offre2 en offre2', et la réponse2' en réponse2, sont beaucoup plus simples. Bien sûr, aucune manipulation de support n'est nécessaire. Le seul changement nécessaire est de modifier les lignes d'origine, de sorte que la ligne d'origine dans l'offre2' est valide sur la base de la valeur dans l'offre1 (la validité exige que la version s'augmente de un, et que les autres restent inchangées).

Certaines limitations sont associées à ce flux. D'abord, l'usager A sera alerté sans qu'aucun support ait été encore établi. Cela signifie que l'usager A ne sera pas capable de rejeter ou accepter l'appel sur la base de sa composition en supports. Ensuite, A et B vont tous deux finir par répondre à l'appel (c'est-à-dire, générer un 200 OK) avant que soit connu si il y a des supports

compatibles. Si ils n'ont pas de supports en commun, l'appel peut être terminé ultérieurement par un BYE. Cependant, les utilisateurs auront déjà été alertés, d'où un dérangement des usagers et un éventuel événement de facturation.

5. Recommandations

Le Flux I (Figure 1) représente le flux le plus simple et le plus efficace. Ce flux DEVRAIT être utilisé par un contrôleur si il sait avec certitude que l'usager B est en fait un automate qui va répondre immédiatement à l'appel. C'est le cas pour les appareils comme des serveurs de supports, des serveurs de conférence, et des serveurs de messagerie, par exemple. Comme on s'attend à ce qu'un grand nombre de contrôles d'appel de tiers soient avec des automates, le cas spécial de ce scénario est raisonnable.

Pour des appels à des entités inconnues, ou à des entités connues pour représenter des gens, il est RECOMMANDÉ que le Flux IV (Figure 4) soit utilisé pour le contrôle d'appel de tiers. Le Flux III PEUT être utilisé à la place, mais il ne procure pas d'avantage supplémentaire par rapport au Flux IV. Cependant, le Flux II NE DEVRAIT PAS être utilisé, à cause du potentiel de ping-pong infini de re-INVITE.

Plusieurs de ces flux utilisent l'adresse de connexion "trou noir" de 0.0.0.0. C'est une adresse IPv4 qui a pour propriété que les paquets qui lui sont envoyés ne quittent jamais l'hôte qui les envoie ; ils sont juste éliminés. Ces flux sont donc spécifiques de IPv4. Pour les autres types de réseau ou d'adresses, une adresse ayant une propriété équivalente DEVRAIT être utilisée.
Dans la plupart des cas, y compris les flux recommandés, l'usager A va entendre un silence pendant que l'appel à B se réalise. Cela peut n'être pas toujours idéal. On peut y remédier en connectant l'appelant à une source de musique d'ambiance pendant que l'appel pour B se réalise.

6. Traitement des erreurs

Il y a de nombreux cas d'erreur qui méritent discussion.
Avec tous les flux d'appel de la Section 4, un appel est établi avec A, puis le contrôleur tente d'établir un appel pour B. Cependant, cette tentative d'appel peut échouer, pour toutes sortes de raisons. L'usager B peut être occupé (résultant en une réponse 486 à l'INVITE), il peut ne pas y avoir de support en commun, la demande peut arriver en fin de temporisation, et ainsi de suite. Si la tentative d'appel à B devait échouer, il est RECOMMANDÉ que le contrôleur envoie un BYE à A. Ce BYE DEVRAIT inclure un en-tête Reason [RFC3326] qui porte le code d'état provenant de la réponse d'erreur. Cela va informer A de la raison précise de l'échec. L'information est importante du point de vue de l'interface d'utilisateur. Par exemple, si A appelle d'un téléphone "noir", et si B a généré un 486, le BYE va contenir un code Reason de 486, et cela pourrait être utilisé pour générer un signal d'occupation local afin que A sache que B est occupé.

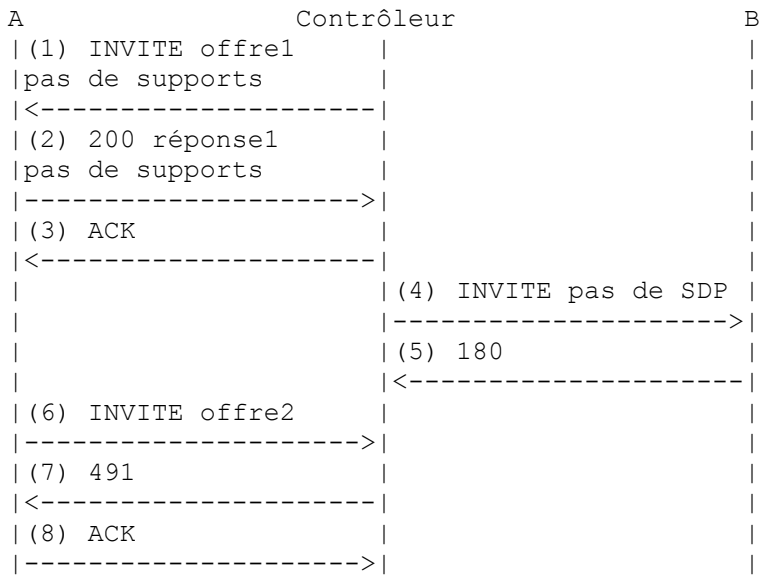


Figure 5

Une autre condition d'erreur qui vaut discussion est montré à la Figure 5. Après que le contrôleur a établi le dialogue avec A (messages 1 à 3) il tente de contacter B (message 4). Contacter B peut prendre un certain temps. Dans l'intervalle, A pourrait éventuellement tenter un re-INVITE, fournissant une offre mise à jour. Cependant, le contrôleur ne peut pas passer cette offre à

B, car il a une transaction INVITE en cours avec lui. Il en résulte que le contrôleur doit rejeter la demande. Il est RECOMMANDÉ qu'une réponse 491 soit utilisée. Ici, la situation est similaire à la condition de prise simultanée décrite dans la [RFC3261], et donc le même traitement d'erreur a du sens. Cependant, A va vraisemblablement réessayer sa demande (par suite de la 491) et cela peut se produire avant la fin de l'échange avec B. Dans ce cas, le contrôleur va répondre avec une autre 491.

7. Suite du traitement

Une fois les appels établis, les deux participants croient qu'ils sont dans un seul appel point à point. Cependant, ils échangent les supports directement d'un avec l'autre, plutôt qu'avec le contrôleur. Le contrôleur est impliqué dans deux dialogues, mais il ne voit aucun support.
Comme le contrôleur est toujours un point central pour la signalisation, il a maintenant le contrôle complet de l'appel. Si il reçoit un BYE d'un des participants, il peut créer un nouveau BYE et raccrocher avec l'autre participant. C'est ce que montre la Figure 6.

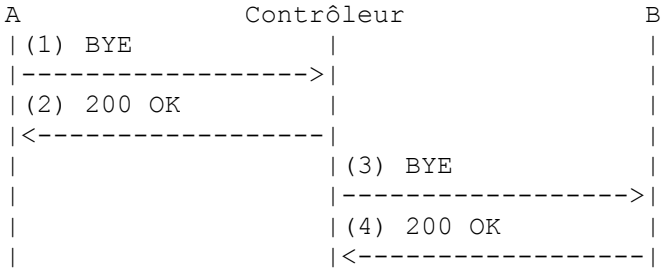


Figure 6

De façon similaire, si il reçoit un re-INVITE de l'un des participants, il peut le transmettre à l'autre participant. Selon le flux qui a été utilisé, cela peut exiger des manipulations sur le SDP avant de le passer.
Cependant, le contrôleur n'a pas besoin d'un "mandataire" pour les messages SIP reçus d'une des parties. Comme il est un agent d'utilisateur dos à dos (B2BUA, *Back-to-Back User Agent*), il peut invoquer tout mécanisme de signalisation sur chaque dialogue, comme il lui semble approprié. Par exemple, si le contrôleur reçoit un BYE de A, il peut générer un nouvel INVITE à un tiers, C, et connecter à la place B à ce participant. Un flux d'appel pour cela est montré à la Figure 7, en supposant le cas où C représente un utilisateur final, et non un automate. Noter que c'est juste le Flux IV.

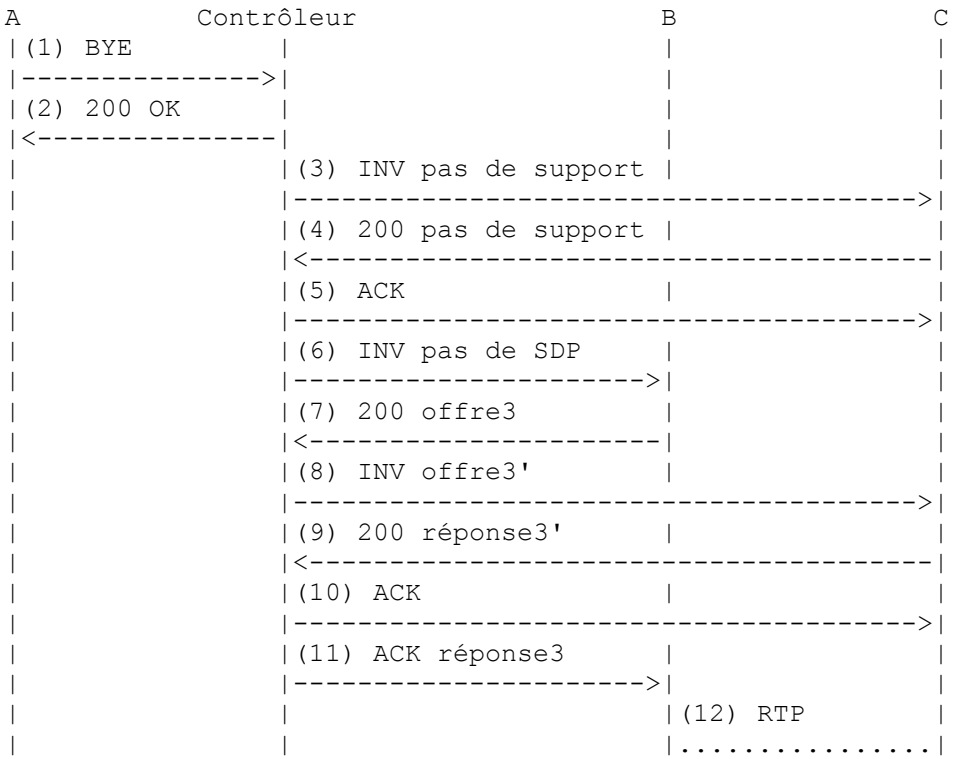


Figure 7

À partir d'ici, de nouvelles parties peuvent être ajoutées, retirées, transférées, et ainsi de suite, comme le contrôleur le trouve approprié. Dans de nombreux cas, le contrôleur va être obligé de modifier le SDP échangé entre les participants afin d'effectuer ces changements. En particulier, le numéro de version dans le SDP va devoir être changé par le contrôleur dans certains cas. Si le contrôleur doit produire une offre SDP de lui-même (par exemple, pour placer un appel en garde) il va avoir besoin d'incrémenter le numéro de version dans l'offre SDP. L'autre participant à l'appel ne saura pas que le contrôleur l'a fait, et toute offre suivante qu'il génère va avoir le mauvais numéro de version pour autant que son homologue soit concerné. Par suite, le contrôleur devra modifier le numéro de version dans les messages SDP pour correspondre à ce qu'attend le receveur.

Il est important de souligner que l'appel n'a pas besoin d'avoir été établi par le contrôleur pour que le traitement de cette section soit utilisé. Le contrôleur pourrait plutôt avoir agi comme un B2BUA durant un appel établi par A vers B (ou vice versa).

8. 3pcc et supports précoces

Les supports précoces représentent la condition où la session est établie (par suite de l'achèvement d'un échange offre/réponse) et que l'appel lui-même n'a pas été accepté. Ceci est habituellement utilisé pour convoyer des tonalités ou annonces concernant les progrès de l'appel. Le traitement des supports précoces dans un appel de tiers est tout simple.

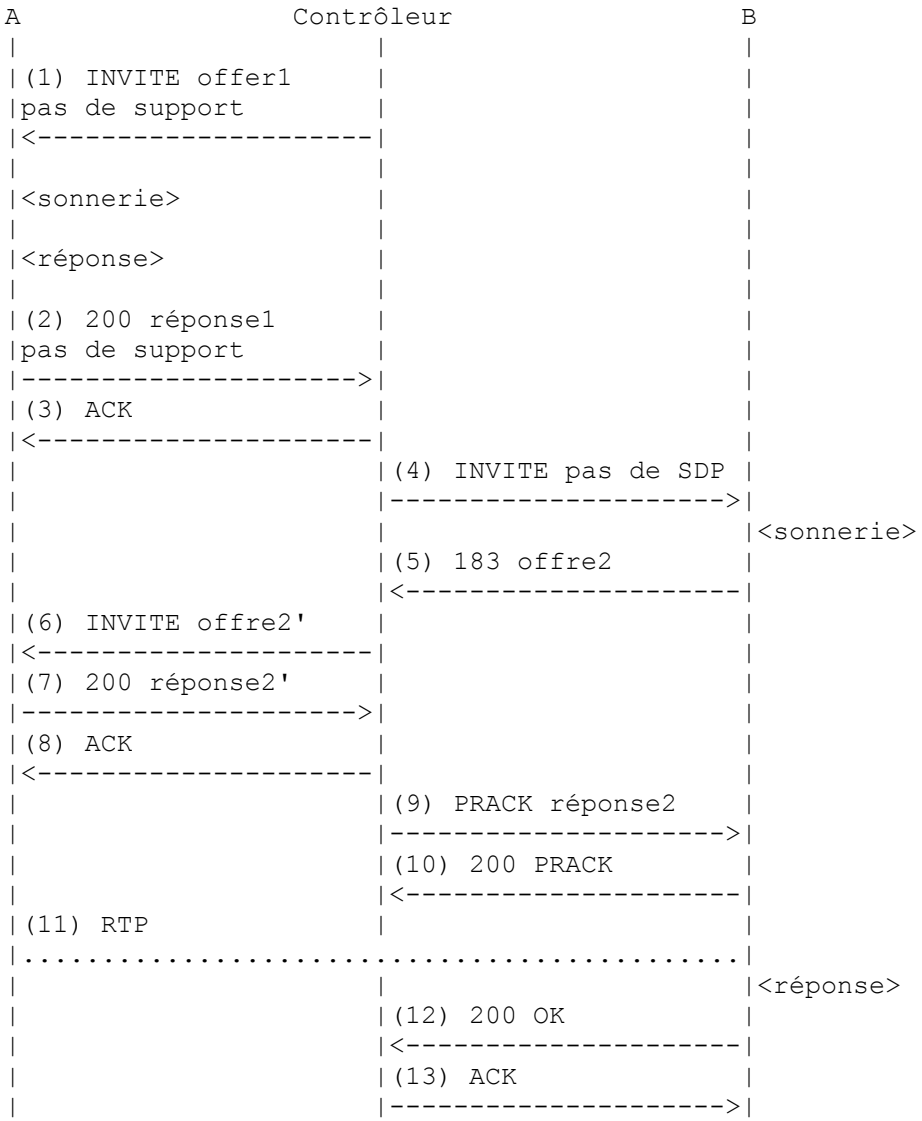


Figure 8

La Figure 8 montre le cas où l'usager B génère des supports précoces avant de répondre à l'appel. Le flux est presque identique à celui du Flux IV de la Figure 4. La seule différence est que l'usager B génère une réponse provisoire fiable (5) [RFC3262] au lieu d'une réponse finale, et la réponse2 est portée dans un PRACK (9) au lieu d'un ACK. Lorsque la partie B accepte

finalement l'appel (12), il n'y a pas de changement dans l'état de la session, et donc, aucune signalisation n'a besoin d'être faite avec l'usager A. Le contrôleur accuse simplement réception du 200 OK (13) pour confirmer le dialogue.

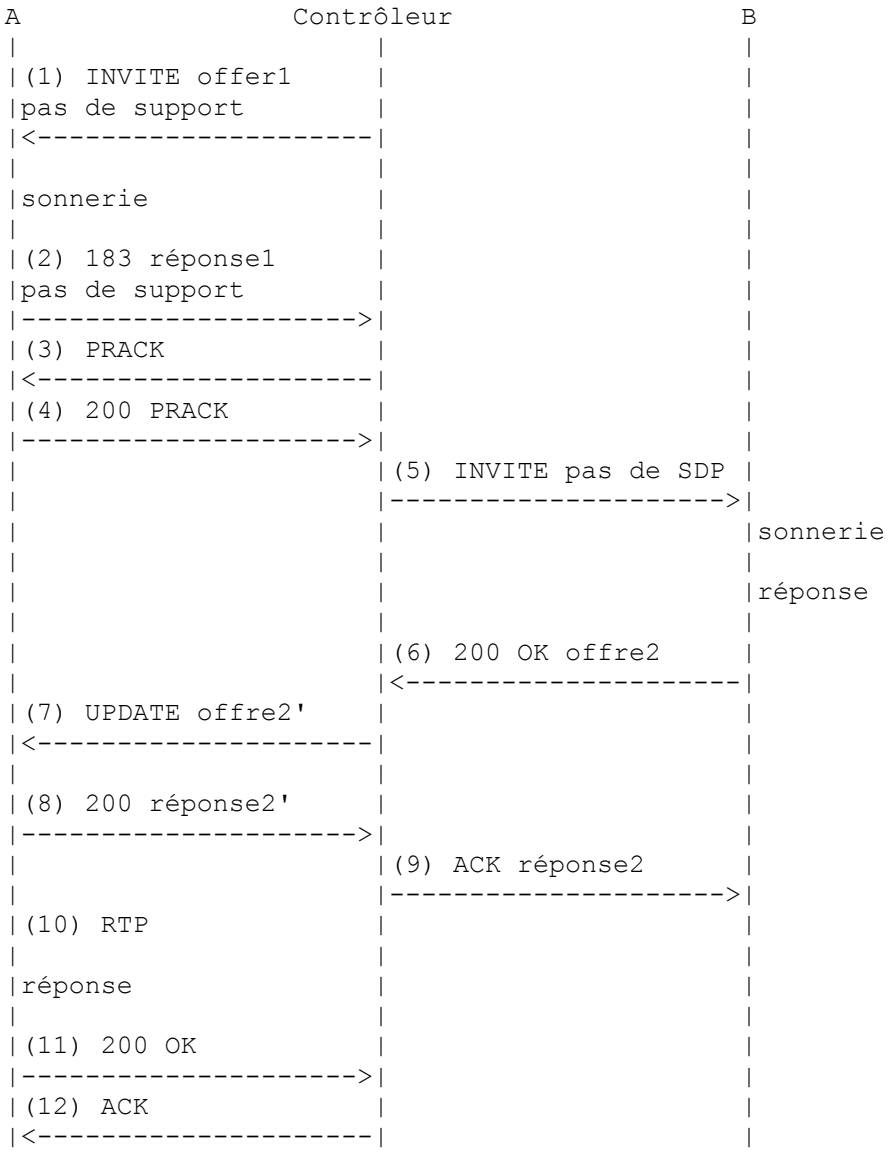


Figure 9

Le cas où l'usager A génère des supports précoces est rendu plus compliqué, et est montré à la Figure 9. Le flux est fondé sur le Flux IV. Le contrôleur envoie un INVITE à l'usager A (1), avec une offre ne contenant aucun flux de support. L'usager A génère une réponse provisoire fiable (2) contenant une réponse sans flux de support. Le contrôleur envoie des PRACK à cette réponse provisoire (3). Maintenant, le contrôleur envoie un INVITE sans SDP à l'usager B (5). Le téléphone de l'usager B sonne, et il répond, d'où résulte un 200 OK (6) avec une offre, offre2. Le contrôleur a maintenant besoin de mettre à jour les paramètres de session avec l'usager A. Cependant, comme l'appel n'a pas encore eu de réponse, il ne peut pas utiliser un re-INVITE. Il utilise plutôt une demande SIP UPDATE (7) [RFC3311], passant l'offre (après l'avoir modifiée pour que le champ Origine soit correct). L'usager A génère sa réponse dans le 200 OK au message UPDATE (8). Cette réponse est passée à l'usager B dans le ACK (9). Lorsque l'usager A répond finalement (11), il n'y a pas de changement dans l'état de session, de sorte que le contrôleur fait simplement un ACK au 200 OK (12).

Noter qu'il est probable qu'il y aura un émondage des supports dans ce flux d'appel. L'usager A est vraisemblablement une passerelle RTPC, et a généré une réponse provisoire à cause des supports précoces du côté RTPC. Le RTPC va livrer ces supports même si la passerelle n'a nulle part où les envoyer, car l'offre initiale provenant du contrôleur n'a pas de flux de support. Lorsque l'usager B répond, les supports peuvent commencer à s'écouler. Cependant, tout support envoyé à la passerelle depuis le RTPC jusqu'à ce point sera perdu.

9. Contrôle d'appel de tiers et préconditions SDP

Une extension SIP a été spécifiée pour permettre le couplage de la signalisation et de la réservation de ressources [RFC3312]. La présente spécification s'appuie sur les échanges de descriptions de session avant l'achèvement de l'établissement d'appel. Ces flux sont initiés lorsque certains paramètres SDP sont passés dans le INVITE initial. Par suite, l'interaction de ce mécanisme avec le contrôle d'appel de tiers n'est pas évident et vaut la peine qu'on le détaille.

9.1 Initiation du contrôleur

Dans un scénario d'utilisation, le contrôleur souhaite utiliser des préconditions afin d'éviter les scénarios d'échec d'appel mentionnés au paragraphe 4.4. Précisément, le contrôleur peut utiliser des préconditions afin de garantir que ni l'une ni l'autre partie n'est alertée si il n'y a pas un ensemble commun de supports et de codecs. Il peut aussi fournir aux deux parties des informations sur la composition des supports de l'appel avant qu'ils décident de l'accepter.

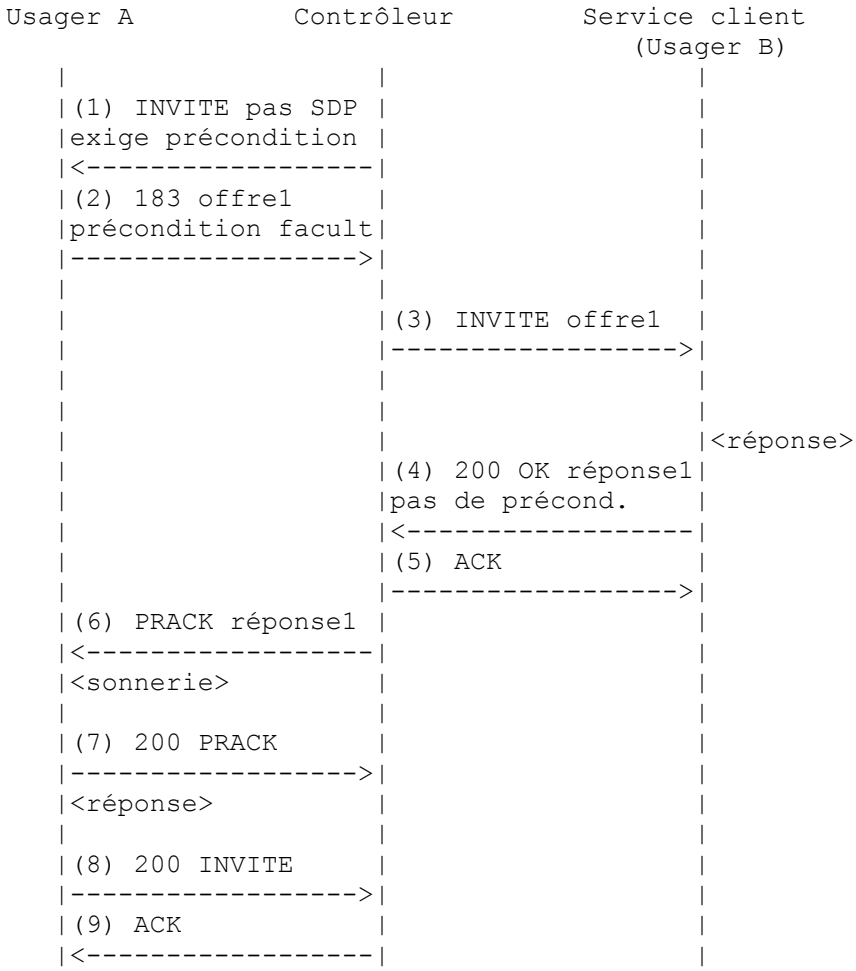


Figure 10

Le flux de ce scénario est montré à la Figure 10. Dans cet exemple, on suppose que l'usager B est un automate ou un agent de quelque sorte qui va répondre immédiatement à l'appel. Donc, le flux se fonde sur Flux I. Le contrôleur envoie un INVITE à l'usager A ne contenant pas de SDP, mais avec un en-tête Require qui indique que des préconditions sont requises. Ce scénario spécifique (un INVITE sans offre, mais avec un en-tête Require qui indique des préconditions) n'est pas décrit dans la [RFC3312]. Il est RECOMMANDÉ que l'UAS réponde avec une offre dans une 1xx incluant les flux de support qu'il souhaite utiliser pour l'appel, et pour chacun, la liste de toutes les préconditions qu'il prend en charge comme facultatives. Bien sûr, l'usager n'est pas alerté à ce moment. Le contrôleur prend cette offre et la passe à l'usager B (3). L'usager B ne prend pas les préconditions en charge, ou n'est pas intéressé par elles. Donc, lorsque il répond à l'appel, le 200 OK contient une réponse sans aucune liste de préconditions (4). Cette réponse est passée à l'usager A dans le PRACK (6). À ce point, l'usager A sait qu'il n'y a aucune préconditions réellement utilisée dans l'appel, et donc, il peut alerter l'usager. Lorsque l'appel a une réponse, l'usager A envoie un 200 OK au contrôleur (8) et l'appel est réalisé.

Dans le cas où l'offre générée par l'usager A n'est pas acceptable pour l'usager B (à cause, par exemple, du non recouvrement des codecs ou des supports) l'usager B va immédiatement rejeter le INVITE (message 3). Le contrôleur va alors ANNULER la demande à l'usager A. Dans cette situation, ni l'usager A ni l'usager B n'auront été alertés, ce qui produit l'effet désiré. Il est intéressant de noter que cette propriété est réalisée en utilisant des préconditions même si les types spécifiques de préconditions qui sont pris en charge par l'usager A importent peu.

Il est aussi entièrement possible que l'usager B désire réellement des préconditions. Dans ce cas, il peut générer de lui-même un 1xx avec une réponse contenant les préconditions. Cette réponse sera quand même passée à l'usager A, et les deux parties vont procéder à toute mesure nécessaire pour satisfaire aux préconditions. Aucun des utilisateur ne sera alerté tant que les préconditions ne seront pas satisfaites.

9.2 Initiative de la partie A

Au paragraphe 9.1, le contrôleur demandait l'utilisation de préconditions pour atteindre un certain but. Il est aussi possible que le contrôleur ne se soucie pas (peut être il ne les connaît même pas) des préconditions, mais ce n'est pas le cas d'un des participants à l'appel. Un flux d'appel pour ce cas est montré dans la Figure 11.

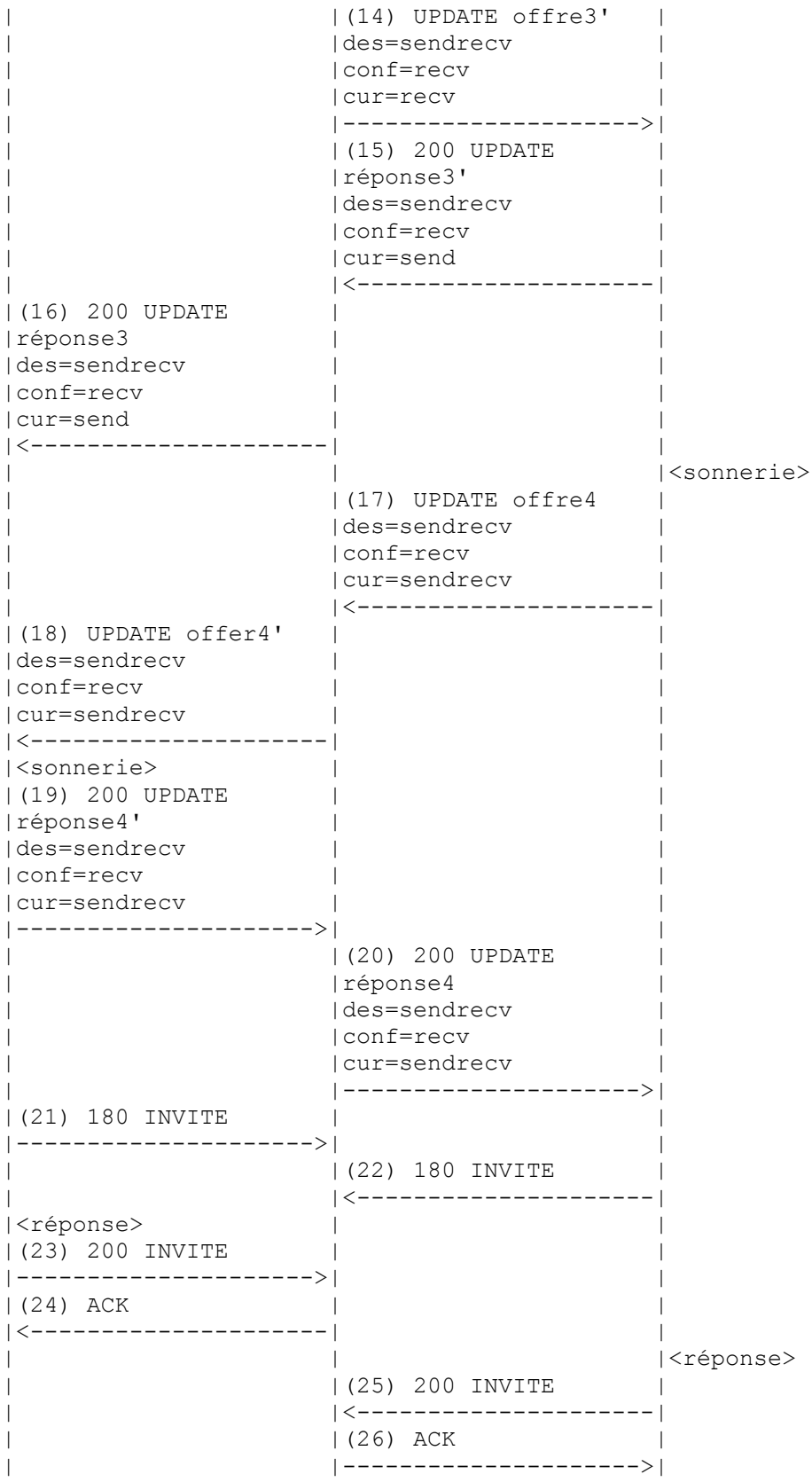


Figure 11

Le contrôleur suit le Flux IV ; il n'a pas d'exigence spécifique pour la prise en charge de la spécification de préconditions [RFC3312]. Donc, il envoie un INVITE (1) avec SDP qui ne contient pas de lignes de support. L'usager A est intéressé par la prise en charge de préconditions, et ne veut pas faire sonner son téléphone tant que les ressources ne sont pas réservées. Comme il n'y a pas de flux de supports dans le INVITE, il ne peut pas réserver les ressources pour les flux de supports, et il ne peut donc pas faire sonner le téléphone jusqu'à ce qu'elles aient été convoyées dans une offre ultérieure et réservées ensuite. Donc, il génère un 183 avec la réponse, et n'alerte pas l'usager (2). Le contrôleur fait un PRACK pour cela (3) et A répond au

PRACK (4).

À ce point, le contrôleur tente d'amener B dans l'appel. Il envoie à B un INVITE sans SDP (5). B est intéressé à avoir des préconditions pour cet appel. Donc, il génère son offre dans un 183 qui contient les attributs SDP appropriés (6). Le contrôleur passe cette offre à A dans une demande UPDATE (7). Le contrôleur utilise UPDATE parce que l'appel n'a pas encore eu de réponse, et donc, il ne peut pas utiliser un re-INVITE. L'usager A voit que son homologue est capable de prendre en charge les préconditions. Comme il désire des préconditions pour l'appel, il génère une réponse dans le 200 OK (8) au message UPDATE. Cette réponse est à son tour passée à B dans le PRACK pour la réponse provisoire (9). Maintenant, les deux côtés effectuent la réservation de ressource. L'usager A réussit d'abord, et passe une description de session mise à jour dans une demande UPDATE (13). Le contrôleur la passe simplement à A (après la manipulation du champ Origine, comme requis dans le Flux IV) dans un UPDATE (14), et la réponse (15) est repassée à A (16). Le même flux se produit de B vers A, lorsque la réservation de B réussit (17-20). Comme les préconditions sont satisfaites, les deux côtés sonnent (21 et 22), puis tous deux répondent (23 et 25), complétant l'appel.

Ce qui est important à propos de ce flux est que le contrôleur ne sait rien des préconditions. Il passe simplement le SDP comme nécessaire. Le truc est l'utilisation de UPDATE et PRACK pour passer le SDP lorsque nécessaire. Cette détermination est entièrement fondée sur les règles d'offre/réponse décrites dans les [RFC3262] et [RFC3311], et est indépendante des préconditions.

10. Exemple de flux d'appel

10.1 Cliquer pour numéroter

La première application de cette capacité qu'on discute ici est le cliquer pour numéroter. Dans ce service, un usager navigue sur les pages de la Toile d'un site de commerce électronique, et voudrait parler à un représentant su service client. L'usager clique sur un lien, et un appel est passé au représentant du service client. Lorsque le représentant décroche, le téléphone du bureau de l'usager sonne. Lorsque l'usager décroche, le représentant du service client est là, prêt à parler à l'usager.

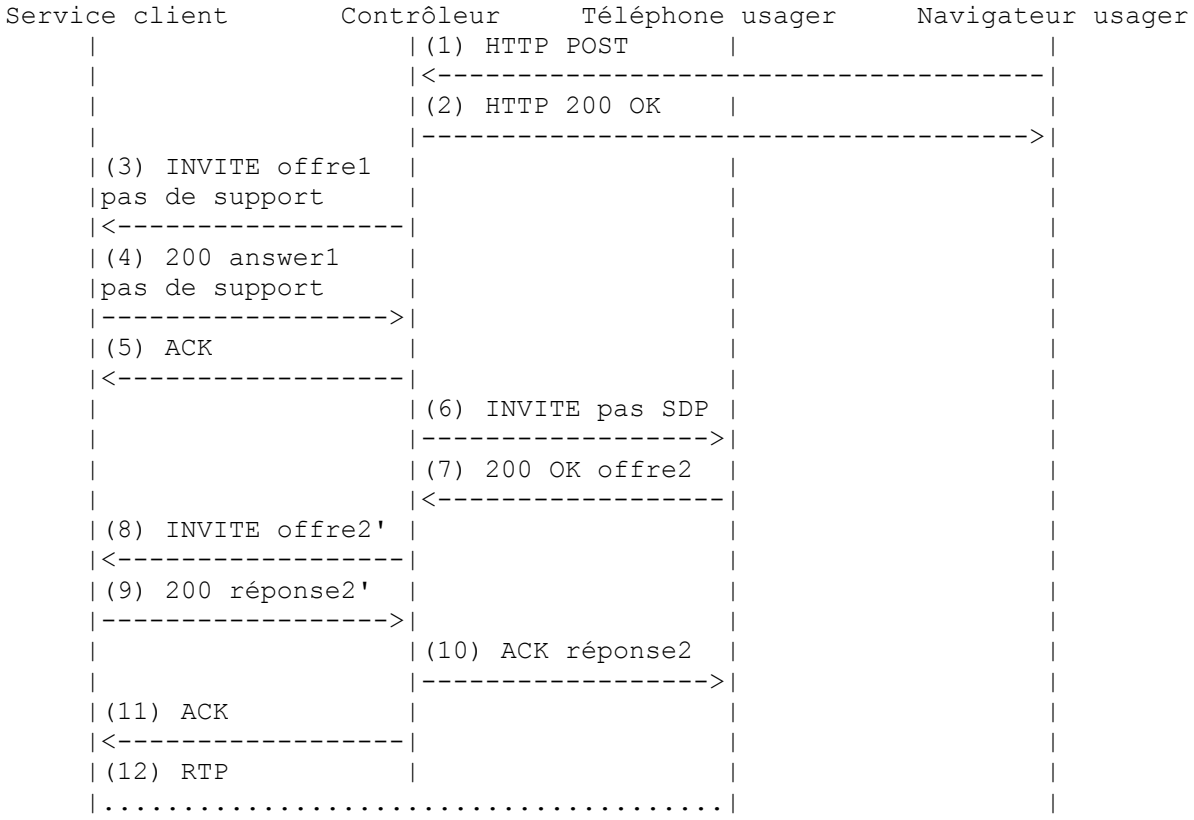


Figure 12

Le flux d'appel pour ce service est donné à la Figure 12. Il est identique à celui de la Figure 4, sauf que le service est déclenché par une demande HTTP POST lorsque l'usager clique sur la liaison. Normalement, cette demande POST ne va contenir le numéro ni de l'usager ni du représentant du service client. Le numéro de l'usager va normalement être obtenu par l'application

de la Toile à partir de bases de données en arrière plan, dans la mesure où l'usager se sera vraisemblablement connecté au site, donnant au serveur le contexte nécessaire. Le numéro du service client va normalement être obtenu par approvisionnement. Donc, le HTTP POST ne fournit en fait rien de plus que l'indication qu'un appel est désiré.

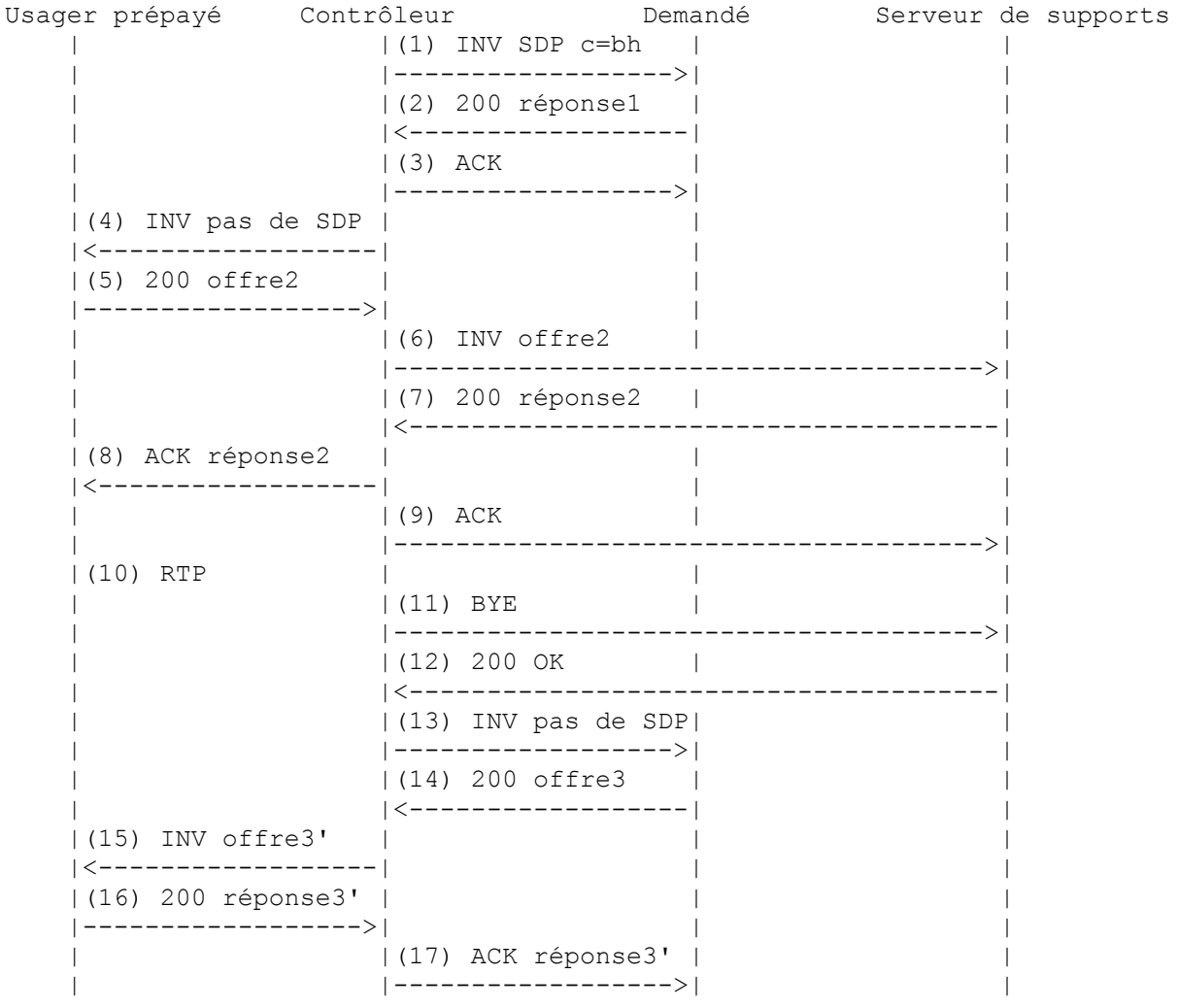
On note que ce service peut être fourni par d'autres mécanismes, à savoir PINT [RFC2848]. Cependant, il y a de nombreuses différences entre la façon dont le service est fourni par PINT, et celle dont il est fourni ici :

- La solution PINT ne permet des appels qu'entre deux points d'extrémité RTPC. La solution décrite ici permet des appels entre des téléphones RTPC (par des passerelles à capacité SIP) et des téléphones IP natifs.
- Lorsque utilisée pour des appels entre deux téléphones RTPC, la solution peut résulter en ce qu'une portion de l'appel soit acheminée sur l'Internet. Dans PINT, l'appel est toujours acheminé seulement sur le RTPC. Cela peut donner des appels de meilleure qualité avec la solution PINT, selon le codec utilisé et les capacités de QS du réseau qui achemine la portion Internet de l'appel.
- La solution PINT exige des extensions à SIP (PINT est une extension à SIP) tandis que la solution décrite ici est faite avec le SIP de base.
- La solution PINT permet au contrôleur (agissant comme client PINT) de se "retirer" une fois l'appel établi. La solution décrite ici exige que le contrôleur maintienne l'état d'appel pour toute la durée de l'appel.

10.2 Capacité d'annonce à mi appel

Le mécanisme de contrôle d'appel de tiers décrit ici peut aussi être utilisé pour permettre des annonces en cours d'appel. Considérons un service de cartes d'appel prépayées. Une fois la carte prépayée établie, le système doit établir un temporisateur pour terminer quand les minutes sont épuisées. Lorsque ce temporisateur arrive à expiration, on aimerait que l'usager entende une annonce qui lui dise de rentrer une carte de crédit pour continuer. Une fois entrées les informations de la carte de crédit, de l'argent est ajouté à la carte prépayée, et l'usager est reconnecté au destinataire de l'appel.

On considère ici l'usage du contrôle d'appel de tiers juste pour exécuter le dialogue de mi appel pour collecter les informations de la carte de crédit.



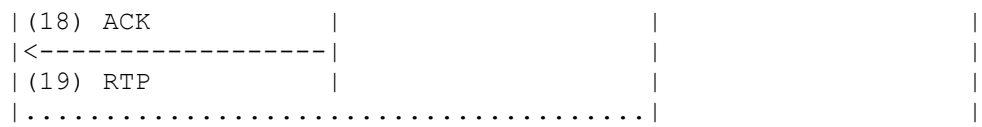


Figure 13

On suppose que l'appel est établi de sorte que le contrôleur est dans l'appel comme B2BUA. Lorsque le temporisateur arrive à expiration, on souhaite connecter l'appelant à un serveur de supports. Le flux en est montré à la Figure 13. Lorsque le temporisateur arrive à expiration, le contrôleur place le demandé sur une adresse de connexion de 0.0.0.0 (1). Cela "déconnecte" effectivement le demandé. Le contrôleur envoie alors un INVITE sans SDP à l'appelant prépayé (4). L'offre retournée de l'appelant (5) est utilisée dans un INVITE au serveur de supports qui va collecter les chiffres (6). C'est une instanciation de Flux I. Ce flux est le seul qui puisse être utilisé ici parce que le serveur de supports est un automate, et va répondre immédiatement à l'INVITE. Si le contrôleur connectait l'usager prépayé à un autre utilisateur final, le Flux III devrait être utilisé. Le serveur de supports retourne un 200 OK (7) immédiat avec une réponse, qui est passée à l'appelant dans un ACK (8). Le résultat est que le serveur de supports et l'appelant prépayé ont leurs flux de supports connectés.

Le serveur de supports fait une annonce, et invite l'usager à entrer un numéro de carte de crédit. Après avoir collecté les chiffres, le numéro de carte est validé. Le serveur de supports passe alors le numéro de carte au contrôleur (en utilisant des moyens qui sortent du domaine d'application de la présente spécification) puis raccroche l'appel (11).

Après avoir raccroché avec le serveur de supports, le contrôleur reconnecte l'usager au demandé original. Pour ce faire, le contrôleur envoie un INVITE sans SDP au demandé (13). Le 200 OK (14) contient une offre, offre3. Le contrôleur modifie le SDP (comme on l'a fait dans le Flux III) et passe l'offre dans un INVITE à l'utilisateur prépayé (15). Celui-ci génère une réponse dans un 200 OK (16) que le contrôleur passe à l'usager B dans le ACK (17). À ce point, l'appelant et le demandé sont reconnectés.

11. Recommandations de mise en œuvre

La plus grande partie du travail impliqué dans la prise en charge du contrôle d'appel de tiers est au sein du contrôleur. Un UA SIP standard devrait être contrôlable en utilisant les mécanismes décrits ici. Cependant, le contrôle d'appel de tiers s'appuie sur quelques caractéristiques qui pourraient n'être pas mises en œuvre. À ce titre, on RECOMMANDE que les mises en œuvre de serveurs d'agent d'utilisateur prennent en charge ce qui suit :

- o des offres et des réponses qui contiennent une ligne de connexion avec une adresse de 0.0.0.0.
- o des demande re-INVITE qui changent l'accès auquel les supports devraient être envoyés
- o des re-INVITE qui changent l'adresse de connexion
- o des re-INVITE qui ajoutent un flux de supports
- o des re-INVITE qui retirent un flux de supports (en réglant son accès à zéro)
- o des re-INVITE qui ajoutent un codec dans l'ensemble dans un flux de supports
- o un adresse de connexion SDP de zéro
- o des demandes INVITE initiales avec une adresse de connexion de zéro
- o des demandes INVITE initiales sans SDP
- o des demandes INVITE initiales avec SDP mais sans ligne de supports
- o des re-INVITE sans SDP
- o la méthode UPDATE [RFC3311]
- o la fiabilité des réponses provisoires [RFC3262]
- o l'intégration de gestion de ressource et SIP [RFC3312].

12. Considérations sur la sécurité

12.1 Autorisation et authentification

Dans la plupart des utilisations de SIP INVITE, l'acceptation ou non d'un appel se fonde sur une décision prise par une personne quand sont présentées les informations sur l'appel, comme l'identité de l'appelant. Dans d'autres cas, un automate répond aux appels, et la décision de le faire peut dépendre de l'application à laquelle SIP est appliqué. Par exemple, si un appelant fait un appel SIP à un service de portail vocal, l'appel peut être rejeté si l'appelant n'a pas adhéré préalablement (peut-être via un site de la Toile). Dans d'autres cas, les politiques de traitement d'appel sont faites sur la base de scripts automatisés, comme ceux décrits par le Langage de traitement d'appels [RFC3880]. Fréquemment, ces décisions sont aussi fondées sur l'identité de l'appelant.

Ces mécanismes d'autorisation seront appliqués aux appels normaux entre parties et de tiers, car les deux ne peuvent être distingués. Par suite, il est important que ces politiques d'autorisation continuent de fonctionner correctement pour les appels de tiers. Bien sûr, les appels de tiers introduisent une nouvelle partie – celle qui initie l'appel de tiers. Faire que les politiques d'autorisation s'appliquent sur la base de l'identité du tiers, ou qu'elles s'appliquent sur la base des participants à l'appel ? Idéalement, les participants devraient pouvoir connaître les identités des deux autres parties, et avoir des politiques d'autorisation fondées sur celles-ci, comme approprié. Cependant, ce n'est pas possible en utilisant les mécanismes existants. Par suite, la bonne pratique suivante est que les demandes INVITE contiennent l'identité du tiers. Finalement, c'est l'utilisateur qui demande la communication, et il y a du sens à ce que les politiques d'autorisation d'appel se fondent sur cette identité.

Cela exige, à son tour, que le contrôleur s'authentifie comme étant ce tiers. Cela peut être un défi, et le mécanisme approprié dépend du scénario spécifique de l'application.

Dans un scénario courant, le contrôleur agit au nom d'un des participants à l'appel. Un exemple typique est le "cliquer pour numéroter", où le contrôleur et le représentant du service client sont gérés par le même domaine administratif. Bien sûr, pour des besoins d'identification, le contrôleur peut légitimement prétendre être le représentant du service client. Dans ce scénario, il serait approprié que le INVITE à l'utilisateur final contienne un champ From qui identifie le représentant du service client, et authentifie la demande en utilisant S/MIME (voir la Section 23 de la [RFC3261]) signée par la clé du représentant du service client (qui est détenue par le contrôleur). Cela exige que le contrôleur ait en fait des accréditifs avec lesquels s'authentifier auprès du représentant du service client. Dans de nombreux autres cas, le contrôleur représente un des participants, mais ne possède pas leurs accréditifs. Malheureusement, il n'y a actuellement aucun mécanisme normalisé qui permette à un utilisateur de déléguer des accréditifs au contrôleur d'une façon qui limite leur usage à des opérations spécifiques de contrôle d'appel de tiers. En l'absence de tels mécanismes, le mieux qu'on puisse faire est d'utiliser le nom affiché dans le champ From pour indiquer l'identité de l'usager au nom duquel l'appel est fait. Il est RECOMMANDÉ que le nom affiché soit réglé à "[contrôleur] au nom de [usager]", où l'usager et le contrôleur sont, respectivement, les identités textuelles de l'usager et du contrôleur. Dans ce cas, l'URI dans le champ From va identifier le contrôleur.

Dans d'autres situations, il n'y a pas de relation réelle entre le contrôleur et les participants à l'appel. Dans ces situations, le contrôleur aurait idéalement un moyen d'affirmer que l'appel vient d'une identité particulière (qui pourrait être un des participants, ou même un tiers, selon l'application) et de valider l'assertion avec une signature utilisant la clé du contrôleur.

12.2 Chiffrement et intégrité de bout en bout

Avec le contrôle d'appel de tiers, le contrôleur est en fait un des participants pour autant que le dialogue SIP est concerné. Donc, le chiffrement et l'intégrité des messages SIP, tels que fournis par S/MIME, vont survenir entre les participants et le contrôleur, plutôt que directement entre les participants. Cependant, l'intégrité, l'authenticité et la confidentialité des sessions de support peuvent être protégées par un contrôleur. La sécurité de bout en bout des supports est fondée sur l'échange du matériel de chiffrement au sein de SDP [RFC4568].

Le fonctionnement approprié de ces mécanismes avec le contrôle d'appel de tiers dépend du comportement approprié du contrôleur. Tant qu'il n'essaye pas de désactiver explicitement des mécanismes, les protocoles vont fonctionner correctement entre les participants, résultant en une session de supports sûre que même le contrôleur ne peut espionner ou modifier. Comme le contrôle d'appel de tiers se fonde sur un modèle de confiance entre les usagers et le contrôleur, il est raisonnable de supposer qu'il fonctionne correctement. Cependant, il n'y a pas de moyen cryptographique qui puisse empêcher le contrôleur d'interférer avec les échanges initiaux de matériels de chiffrement. Par suite, il y a une possibilité triviale pour le contrôleur de s'insérer en intermédiaire dans les supports d'échange, si il le désirait.

13. Remerciements

Les auteurs tiennent à remercier Paul Kyzivat, Rohan Mahy, Eric Rescorla, Allison Mankin et Sriram Parameswar de leurs commentaires.

14. Références

12.1 Références normatives

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

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665)

[RFC3262] J. Rosenberg et H. Schulzrinne, "Fiabilité des réponses provisoires dans le protocole d'initialisation de session (SIP)", juin 2002. *(P.S.)*

[RFC3264] J. Rosenberg et H. Schulzrinne, "Modèle d'offre/réponse avec le protocole de description de session (SDP)", juin 2002.

[RFC3311] J. Rosenberg, "Méthode UPDATE du protocole d'initialisation de session (SIP) ", octobre 2002.

[RFC3312] G. Camarillo, éd., "Intégration de la gestion de ressource et du protocole d'initialisation de session (SIP)", octobre 2002. (*MàJ par* RFC4032, RFC5027) *(P.S.)*

[RFC3326] H. Schulzrinne, D. Oran, G. Camarillo, "Champ d'en-tête Reason pour le protocole d'initialisation de session (SIP)", décembre 2002. *(P.S.)*

14.2 Références pour information

[RFC2848] S. Petrack, L. Conroy, "Protocole de service PINT : extensions à SIP et SDP pour l'accès IP aux services de téléphone", juin 2000. *(P.S.)*

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160)

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

[RFC4568] F. Andreasen et autres, "Définition d'attributs de sécurité dans le protocole de description de session (SDP) pour les flux de support", juillet 2006. *(P.S.)*

15. Adresse des auteurs

Jonathan Rosenberg
dynamicsoft
600 Lanidex Plaza
Parsippany, NJ 07054
USA
mél : jdrosen@dynamicsoft.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland
mél : Gonzalo.Camarillo@ericsson.com

Henning Schulzrinne
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027
USA
mél : schulzrinne@cs.columbia.edu

Jon Peterson
Neustar
1800 Sutter Street
Suite 570
Concord, CA 94520
USA
mél : jon.peterson@neustar.biz

16. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de

reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d’autres langues que l’anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

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

Propriété intellectuelle

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

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

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

Remerciement

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