

Groupe de travail Réseau

J. Rosenberg, Cisco

**Request for Comments : 5411**

Catégorie : Information

Traduction Claude Brière de L'Isle

janvier 2009

## Guide touristique du protocole d'initialisation de session (SIP)

### Statut du présent mémoire

Le présent document donne des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de Copyright

Copyright (C) The Internet Society (2009).

### Résumé

Le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) fait l'objet de nombreuses spécifications produites par l'IETF. Il peut être difficile de localiser le bon document, ou même de déterminer l'ensemble des demandes de commentaires (RFC, *Request for Comments*) sur SIP. La présente spécification sert de guide à la série de RFC sur SIP. Elle fait la liste des spécifications actuelles sous la rubrique SIP, résume brièvement chacune, et les groupe en catégories.

### Table des matières

1. Introduction.....	1
2. Domaine d'application de ce document.....	3
3. Spécifications du cœur de SIP.....	3
4. Interfonctionnement avec le réseau téléphonique public commuté (RTPC).....	5
5. Extensions d'infrastructure d'objet général.....	6
6. Traversée de NAT.....	8
7. Primitives de commande d'appel.....	8
8. Cadre d'événement.....	9
9. Paquetages d'événement.....	9
10. Qualité de service.....	10
11. Opérations et gestion.....	10
12. Compression SIP.....	11
13. URI de service SIP.....	11
14. Extensions mineures.....	11
15. Mécanismes de sécurité.....	13
16. Conférence.....	14
17. Messagerie instantanée, présence, et multimédia.....	15
18. Services d'urgence.....	15
19. Considérations sur la sécurité.....	16
20. Remerciements.....	16
21. Références pour information.....	16
Adresse de l'auteur.....	22
Déclaration complète de droits de reproduction.....	23

## 1. Introduction

Le protocole d'initialisation de session (SIP) [RFC3261] fait l'objet de nombreuses spécifications qui ont été produites par l'IETF. Il peut être difficile de localiser le bon document, ou même de déterminer l'ensemble des RFC sur SIP. "Pas de panique !" [HGTTG]. La présente spécification sert de guide à la série des RFC SIP. C'est une photographie présente des spécifications sous la rubrique SIP au moment de la publication. Il est envisagé que ce document soit lui-même l'objet de mises à jour régulières avec la maturation des spécifications de SIP. De plus, il fait référence à de nombreuses spécifications, qui, au moment de la publication de ce document, n'étaient pas encore finalisées, et peuvent être finalement terminées ou abandonnées. Donc, l'énumération des spécifications comme travail en cours est sujette à des changements.

Pour chaque spécification, un paragraphe de description est inclus pour résumer l'objet de la spécification. Chaque

spécification inclut aussi une lettre qui désigne sa catégorie sur la voie de la normalisation [RFC2026]. Ces valeurs sont :

S : Sur la voie de la normalisation (norme proposée, projet de norme, ou norme adoptée)

E : Expérimentale

B : Bonnes pratiques actuelles

I : Information

Les spécifications sont groupées par sujet. Les sujets sont :

Cœur : spécifications SIP dont on attend qu'elles soient utilisées pour chaque session ou enregistrement auquel un point d'extrémité participe.

Interopérabilité avec le réseau téléphonique public commuté (RTPC) : spécifications relatives à l'interfonctionnement avec le réseau téléphonique.

Infrastructure d'objet général : extensions d'objet général à SIP, SDP (protocole de description de session) et MIME, mais dont il n'est pas prévu qu'elles soient toujours utilisées.

Traversée de NAT : spécifications qui traitent de la traversée de NAT et de pare-feu.

Primitives de commandes d'appel : spécifications pour manipuler les dialogues et appels SIP.

Cadre d'événements : définitions des spécifications centrales pour le cadre d'événements SIP, fournissant la capacité pub/sub.

Paquetages d'événement : paquetages qui utilisent le cadre d'événements SIP.

Qualité de service : spécifications relatives à la qualité de service (QS) multimédia.

Opérations et gestion : spécifications relatives à la configuration et la gestion des déploiements de SIP.

Compression de SIP : spécifications pour faciliter l'usage de SIP avec le cadre de compression de signalisation (Sigcomp).

URI de service SIP : spécifications sur comment utiliser les URI pour traiter les services multimédia.

Extensions mineures : spécifications qui résolvent un étroit espace de problème ou fournissent une optimisation.

Mécanismes de sécurité : spécifications qui fournissent une fonction de sécurité pour SIP.

Conférence : spécifications pour conférence multimédia.

Messagerie instantanée, présence, et multimédia : extensions à SIP relatives à la messagerie instantanée (IM) la présence, et le multimédia. Cela couvre seulement les extensions SIP relatives à ces sujets. Voir la [RFC6914] sur un traitement complet de SIP pour IM et présence (SIMPLE).

Services d'urgence : extensions SIP relatives aux services d'urgence. Voir la [RFC6443] pour un traitement plus complet des fonctions supplémentaires relatives aux services d'urgence.

Normalement, les extensions à SIP tiennent naturellement dans ces sujets, et les développeurs intéressés par un sujet particulier mettent souvent en œuvre beaucoup ou toutes les spécifications de ce domaine. Il y a quelques spécifications qui rentrent dans plusieurs domaines, et dans ce cas elles sont mentionnées plus d'une fois.

Ne pas imprimer toutes les spécifications citées ici en une fois, car elles pourraient avoir le sort des règles de "Brockian Ultracriquet" quand elles sont mises ensemble : s'effondrer sous leur propre poids et former un trou noir [HGTTG].

Le présent document n'est pas lui-même une mise à jour de la RFC 3261 ni une extension à SIP. C'est un document d'information, destiné à guider les arrivants, les utilisateurs, et les déployeurs sur les nombreuses spécifications associées à SIP.

## 2. Domaine d'application de ce document

Il est très difficile d'énumérer l'ensemble des spécifications de SIP. C'est parce que beaucoup de protocoles sont intimement liés à SIP et utilisés par presque toutes les mises en œuvre de SIP, mais ne sont pas formellement des extensions de SIP. À ce titre, le présent document définit formellement une "spécification SIP" comme :

- o La RFC 3261 et toute spécification qui définit une extension pour elle, où une extension est un mécanisme qui change ou met à jour d'une certaine manière un comportement qui y est spécifié.
- o La spécification SDP de base [RFC4566] et toute spécification qui définit une extension à SDP dont le principal objet est de prendre en charge SIP.
- o Toute spécification qui définit un objet MIME dont le principal objet est de prendre en charge SIP.

Exclus de cette liste sont les exigences, architectures, définitions de registre, cadres non normatifs, et processus. Les bonnes pratiques actuelles sont incluses quand elles définissent des mécanismes normatifs pour accomplir une tâche, ou fournissent une description significative de l'usage des spécifications normatives, comme des flux d'appels.

Les processus de changement de SIP [RFC3427] définissent deux types d'extensions à SIP : les extensions normales et les en-têtes P- (où P signifie "préliminaire", "privé", ou "propriétaire", et le préfixe "P-" est inclus dans le nom du champ d'en-tête) qui sont destinés à être utilisés dans des domaines d'applicabilité limitée. Les en-têtes P- ne peuvent pas être définis dans la voie de la normalisation. Pour la plus grande partie, les en-têtes P- ne sont pas inclus dans la liste donnée ici, à l'exception de ceux qui ont eu un usage général en dépit de leur statut d'en-tête P-.

Le présent document inclut des spécifications qui ont déjà été approuvées par l'IETF et ont reçu un numéro de RFC, en plus des projets Internet, qui sont encore en cours de développement au sein de l'IETF et vont finalement recevoir un numéro de RFC. L'inclusion ici des projets Internet aide à encourager les mises en œuvre précoces et les démonstrations d'interopérabilité du protocole, et donc aide au processus d'établissement des normes. Leur inclusion identifie aussi où l'IETF vise une solution à un espace de problème particulier. Noter que l'allocation finale par l'IANA de codets (comme les étiquettes d'option et les noms de champs d'en-tête) n'a lieu que peu avant la publication comme RFC, et donc que les allocations de codets peuvent changer.

## 3. Spécifications du cœur de SIP

Les spécifications du cœur de SIP représentent l'ensemble des spécifications dont les fonctions sont largement applicables. Une extension est largement applicable si elle tient dans une des catégories applicables :

- o Pour les spécifications qui impactent la gestion de session SIP, l'extension va être utilisée pour presque toutes les sessions initiées par un agent d'utilisateur.
- o Pour les spécifications qui impactent les enregistrements SIP, l'extension va être utilisée pour presque tous les enregistrements initiés par un agent d'utilisateur.
- o Pour les spécifications qui impactent les abonnements SIP, l'extension va être utilisée pour presque tous les abonnements initiés par un agent d'utilisateur.

En d'autres termes, il n'y a pas de spécification qui soit utilisée juste pour certaines demandes et pas pour d'autres ; ce sont des spécifications qui vont s'appliquer à chacune des demandes pour lesquelles l'extension est pertinente. Dans la galaxie SIP, ces spécifications sont comme des serviettes [HGTTG].

RFC 3261, Protocole d'initialisation de session (S) : la [RFC3261] est le cœur du protocole SIP lui-même. La RFC 3261 rend obsolète la [RFC2543]. C'est le président de la galaxie [HGTTG] pour autant que la suite des spécifications SIP est concernée.

RFC 3263, Localisation des serveurs SIP (S) : la [RFC3263] donne les procédures du DNS pour prendre un URI SIP et déterminer un serveur SIP associé à cet URI SIP. La RFC 3263 est essentielle pour toute mise en œuvre qui utilise SIP avec le DNS. La RFC 3263 utilise les enregistrement SRV du DNS [RFC2782] et les enregistrements NAPTR [RFC3401].

- RFC 3264, Modèle d'offre/réponse avec le protocole de description de session (S) : la [RFC3264] définit comment le protocole de description de session (SDP) [RFC4566] est utilisé avec SIP pour négocier les paramètres d'une session de supports. Elle est d'un large usage et fait partie intégrante du comportement de la RFC 3261.
- RFC 3265, Notification d'événement spécifique de SIP (S) : la [RFC3265] définit les méthodes SUBSCRIBE et NOTIFY. Ces deux méthodes fournissent un cadre général de notification d'événement pour SIP. Pour utiliser réellement le cadre, les extensions doivent être définies pour des paquetages d'événements spécifiques. Un paquetage d'événements définit un schéma pour les données d'événement et décrit d'autres aspects du traitement d'événement spécifique de ce schéma. Une mise en œuvre de la RFC 3265 est exigée quand un paquetage d'événements est utilisé.
- RFC 3325, Extensions privées à SIP pour les identités affirmées au sein d'un réseau de confiance (I) : bien que son statut d'en-tête P- implique qu'elle a une applicabilité limitée, la [RFC3325], qui définit le champ d'en-tête P-Asserted-Identity, a été largement déployée. Elle est utilisée comme mécanisme de base pour fournir des services d'identifiant d'appelant affirmé par le réseau. Sa mise à jour prévue, la [RFC5876], précise aussi son usage pour l'identification des parties connectées.
- RFC 3327, Champ d'en-tête d'extension SIP pour l'enregistrement de contacts non adjacents (S) : la [RFC3327] définit le champ d'en-tête Path. Ce champ est inséré par les mandataires entre un client et son registraire. Il permet que les demandes entrantes chez un client traversent ces mandataires avant d'être livrées à l'agent d'utilisateur. Il est essentiel dans tout déploiement SIP qui a des mandataires de bordure, qui sont des mandataires entre le client et le mandataire de rattachement ou le registraire SIP.
- RFC 3581, Extension à SIP pour l'acheminement de réponse symétrique (S) : la [RFC3581] définit le paramètre rport de l'en-tête Via. Il permet aux réponses SIP de traverser les NAT. C'est une des diverses spécifications qui sont utilisées pour la traversée de NAT (voir la Section 6).
- RFC 3840, Indication des capacités d'agent d'utilisateur dans SIP (S) : la [RFC3840] définit un mécanisme pour porter les informations de capacités d'un agent d'utilisateur dans les demandes REGISTER et dans les demandes de formation de dialogue comme INVITE. Il a trouvé une utilisation avec la conférence (le paramètre isfocus déclare qu'un agent d'utilisateur est un serveur de conférence) et avec des applications comme de bouton poussoir.
- RFC 4320, Actions visant les problèmes identifiés dans la transaction Non-INVITE de SIP (S) : la [RFC4320] met formellement à jour la RFC 3261 et modifie certains des comportements associés aux transactions non INVITE. Cela règle certains des problèmes trouvés dans les temporisations et les cas de défaillance.
- RFC 4474, Améliorations pour la gestion d'identité authentifiée dans SIP (S) : la [RFC4474] définit un mécanisme pour fournir une identité cryptographiquement vérifiable de la partie appelante dans une demande SIP. Connue sous le nom de "Identité SIP", ce mécanisme donne une solution de remplacement à la RFC 3325. Il a eu peu de déploiements jusqu'à présent, mais son importance comme construction clé des techniques anti-pourriels et des nouveaux mécanismes de sécurité en fait une partie centrale des spécifications SIP.
- RFC5627, Obtention et utilisation des URI d'agent d'utilisateur mondialement acheminable (GRUU) dans SIP (S) : la [RFC5627] définit un mécanisme pour diriger les demandes vers une instance d'UA spécifique. GRUU est essentiel pour des caractéristiques comme le transfert et fournit une autre pièce de l'histoire de la traversée de NAT de SIP.
- RFC5626, Gestion des connexions initiées par le client dans SIP (S) : la [RFC5626], aussi appelée SIP sortant, définit des changements importants au mécanisme d'enregistrement de SIP qui permettent la livraison des messages SIP vers un UA quand il est derrière un NAT. Cette spécification est la pierre angulaire de la stratégie de traversée de NAT de SIP.
- RFC 4566, Protocole de description de session (S) : la [RFC4566] définit un format pour représenter des sessions multimédia. Les objets SDP sont portés dans le corps des messages SIP et, sur la base du modèle d'offre/réponse, sont utilisés pour négocier les caractéristiques des supports d'une session entre utilisateurs.
- RFC5939, Négociation de capacité SDP (S) : la [RFC5939] définit un ensemble d'extensions à SDP qui permettent la négociation de capacités au sein de SDP. La négociation de capacités peut être utilisée pour choisir entre différents profils de RTP (sûr ou non sûr) ou de négocier les codecs lorsque un agent doit en choisir un parmi un ensemble de codecs pris en charge.
- RFC5245, Établissement de connectivité interactive (ICE) (S) : la [RFC5245] définit une technique pour la traversée de NAT par des sessions de supports pour les protocoles qui utilisent le modèle d'offre/réponse. Cette spécification est le

mécanisme recommandé par l'IETF pour la traversée de NAT pour les flux de supports SIP, et est destinée à être utilisée même par les points d'extrémité qui ne sont eux-mêmes jamais derrière un NAT. Une étiquette d'option SIP et une étiquette de caractéristique de support [RFC5768] (aussi une spécification du cœur) ont été définies pour être utilisées avec ICE.

RFC 3605, Attribut du protocole de contrôle en temps réel (RTCP) dans le protocole de description de session (SDP) (S) : la [RFC3605] définit un moyen pour signaler explicitement, au sein d'un message SDP, l'adresse et l'accès IP pour RTCP, plutôt que d'utiliser la règle accès+1 du protocole de transport en temps réel (RTP) [RFC3550]. Il est nécessaire pour les appareils derrière des NAT, et la spécification est exigée par ICE.

RFC 4916, Identité connectée dans le protocole d'initialisation de session (SIP) (S) : la [RFC4916] met formellement à jour la RFC 3261. Elle définit une extension à SIP qui permet à un utilisateur appelant de déterminer l'identité de l'utilisateur appelé final (la partie connectée). Du fait des services de transmission et de reciblage, ce peut n'être pas le même que l'utilisateur que l'appelant essayait originellement de joindre. Le mécanisme fonctionne en tandem avec la spécification d'identité SIP [RFC4474] pour fournir des signatures sur l'identité de la partie connectée. Il peut aussi être utilisé si l'identité d'une partie change à mi-appel due à des actions de contrôle d'appel de tiers ou du comportement du RTPC.

RFC 3311, Méthode SIP UPDATE (S) : la [RFC3311] définit la méthode UPDATE pour SIP. Cette méthode est destinée à être un moyen de mettre à jour les informations de session avant l'achèvement de la transaction INVITE initiale. Elle peut aussi être utilisée pour mettre à jour d'autres informations, comme l'identité du participant [RFC4916], sans impliquer la mise à jour d'un échange d'offre/réponse. Elle a été développée initialement pour prendre en charge la [RFC3312], mais a trouvé d'autres usages. En particulier, son usage avec la RFC 4916 signifie qu'elle va normalement être utilisée au titre de chaque session, pour porter une identité connectée sûre.

RFC 5630, Utilisation du schéma d'URI SIPS dans le protocole d'initialisation de session (SIP) (S) : la [RFC5630] est destinée à mettre à jour la RFC 3261. Elle révisé le traitement de l'URI SIPS, originellement défini dans la RFC 3261, pour corriger de nombreuses erreurs et problèmes rencontrés avec ce mécanisme.

RFC 3665, Exemple de flux d'appel de base du protocole d'initialisation de session (SIP) (B) : la [RFC3665] contient les bonnes pratiques actuelles de flux d'appel pour les interactions SIP de base -- établissement d'appel, terminaison, et enregistrement.

Corrections essentielles à SIP : une collection de corrections à SIP qui traite les erreurs et vulnérabilités importantes. Cela inclut une correction exigeant la détection de boucle dans tout mandataire qui fourche [RFC5393], des éclaircissements sur comment fonctionne l'enregistrement de chemin [RFC5658], et une correction au BNF IPv6 [RFC5954].

#### 4. Interfonctionnement avec le réseau téléphonique public commuté (RTPC)

De nombreuses extensions et usages de SIP se rapportent à l'interopérabilité et aux communications avec ou à travers le RTPC (réseau téléphonique public commuté).

RFC 2848, protocole de service PINT (S) : la [RFC2848] est une des premières extensions à SIP. Elle définit les procédures pour utiliser SIP à invoquer les services qui s'exécutent en fait sur le RTPC. Sa principale application est pour le contrôle d'appel de tiers, permettant à un hôte IP d'établir un appel entre deux points d'extrémité du RTPC. L'interfonctionnement RTPC/Internet (PINT, *PSTN/Internet Interworking*) a un objectif relativement étroit et n'a pas connu un très large déploiement.

RFC 3910, Protocole SPIRITS (S) : en continuant la tendance à désigner les extensions relatives au RTPC avec des références alcooliques, SPIRITS (Services du RTPC qui demandent de services Internet) [RFC3910] définit l'inverse de PINT. Il permet de passer dans le RTPC pour demander à un élément IP de traiter l'appel en attente. Il a été développé principalement pour prendre en charge le signal d'appel Internet (ICW, *Internet Call Waiting*). Peut-être la prochaine spécification sera appelée le gargarisme explosif pan galactique [HGTTG].

RFC 3372, SIP pour téléphones (SIP-T) : contexte et architectures (I) : SIP-T [RFC3372] définit un mécanisme pour utiliser SIP entre des paires de passerelles RTPC. Son idée essentielle est de tunneler la signalisation de sous-système utilisateur RNIS (ISUP, *ISDN User Part*) entre les passerelles dans le corps des messages SIP. SIP-T était motivé par le développement de INFO [RFC2976]. SIP-T a eu une large mise en œuvre pour le modèle limité de déploiement qu'il vise. Comme les points d'extrémité ISUP disparaissent du réseau, le besoin de ce mécanisme va diminuer.

RFC 3398, Transposition de ISUP en SIP (S) : la [RFC3398] définit comment faire la transposition de protocole de la signalisation SS7 de sous-système utilisateur RNIS (ISUP) en SIP. Il est largement utilisé dans les passerelles de SS7 à SIP et fait partie du cadre de SIP-T.

RFC 4497, Interfonctionnement entre le protocole d'initialisation de session (SIP) et QSIG (B) : la [RFC4497] définit comment faire la transposition de protocole de Q.SIG, utilisé pour la signalisation de commutateur privés (PBX) en SIP.

RFC 3578, Transposition de la signalisation en chevauchement ISUP dans SIP (S) : la [RFC3578] définit un mécanisme pour transposer la numérotation en chevauchement dans SIP. Cette spécification est largement considérée comme la plus vilaine spécification SIP, car l'introduction de la spécification elle-même indique qu'elle pose de nombreux problèmes. La signalisation en chevauchement (la pratique d'envoyer les chiffres dans le réseau au fur et à mesure de leur frappe au lieu d'attendre la collecte complète du numéro de l'appelé) est largement incompatible avec SIP à un certain nombre de niveaux très fondamentaux. Ceci dit, la RFC 3578 est sans danger et connaît un certain usage.

RFC 3960, Support précoce et génération de tonalités d'appel dans SIP (I) : la [RFC3960] définit des lignes directrices pour traiter les supports précoces -- la pratique d'envoi de supports de l'appelé ou d'un serveur d'application vers l'appelant avant l'acceptation de l'appel. Les supports précoces sont souvent générés depuis le RTPC. Les supports précoces sont un sujet complexe, et cette spécification ne traite pas complètement les problèmes qui y sont associés.

RFC 3959, Type de disposition de session précoce pour le protocole d'initialisation de session (SIP) (S) : la [RFC3959] définit un nouveau type de disposition de session à utiliser avec des supports précoces. Elle indique que le SDP dans le corps est pour une session spéciale de supports précoces. Elle est peu utilisée.

RFC 3204, Types de supports MIME pour objets ISUP et QSIG (S) : la [RFC3204] définit des objets MIME pour représenter les messages de signalisation SS7 et QSIG. Les messages de signalisation SS7 sont portés dans le corps des messages SIP quand SIP-T est utilisé. Les messages de signalisation QSIG peuvent être portés de façon similaire.

RFC3666, Flux d'appels du réseau téléphonique public commuté (RTPC) en protocole d'initialisation de session (SIP) (B) : la [RFC3666] donne les bonnes pratiques de flux d'appel pour interfonctionner avec le RTPC.

## 5. Extensions d'infrastructure d'objet général

Ces extensions sont des améliorations de portée générale à SIP, SDP, et MIME qui peuvent servir à des usages très divers. Cependant, elles ne sont pas utilisées pour chaque session ou enregistrement, comme le sont les spécifications du cœur.

RFC 3262, Fiabilité des réponses provisoires dans SIP (S) : SIP définit deux types de réponses à une demande : finale et provisoire. Les réponses provisoires sont numérotées de 100 à 199. Dans SIP, ces réponses ne sont pas envoyées de façon fiable. Ce choix a été fait dans la RFC 2543 car les messages étaient destinés à juste être vraiment d'information et rendus à l'utilisateur. Cependant, des travaux suivants sur l'interfonctionnement avec le RTPC ont montré le besoin de transposer les réponses provisoires en messages du RTPC qui ont besoin d'une livraison fiable. La [RFC3262] a été développée pour permettre la fiabilité des réponses provisoires. La spécification définit la méthode PRACK, utilisée pour indiquer qu'une réponse provisoire a été reçue. Bien qu'elle donne une capacité générique pour SIP, les mises en œuvre de la RFC 3262 ont été très courantes dans les appareils d'interfonctionnement avec le RTPC. Cependant, PRACK apporte de nombreuses complications pour un bénéfice relativement faible. À ce titre, il n'a vu qu'un niveau modéré de déploiement.

RFC 3323, Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP) (S) : la [RFC3323] définit le champ d'en-tête Privacy, utilisé par les clients pour demander l'anonymat pour leurs demandes. Bien qu'il définisse plusieurs services de confidentialité, le seul largement utilisé est celui qui prend en charge la confidentialité du champ d'en-tête P-Asserted-Identity [RFC3325].

RFC 5767, Mécanisme de confidentialité piloté par l'agent d'utilisateur pour SIP (S) : la [RFC5767] définit un mécanisme pour réaliser des appels anonymes dans SIP. C'est une solution de remplacement de la [RFC3323], et qui place plus d'intelligence dans le point d'extrémité pour construire des messages anonymes en accédant directement aux services du réseau.

RFC 2976, Méthode INFO (S) : la [RFC2976] a été définie comme une extension à la RFC 2543. Elle définit une méthode, INFO, utilisée pour transporter des informations de mi-dialogue qui n'ont pas d'impact sur SIP lui-même. Son

application pilote était le transport d'informations relatives au RTPC quand on utilise SIP entre une paire de passerelles. Bien que conçu à l'origine pour une utilisation plus large, il n'a trouvé un usage normalisé qu'avec SIP-T [RFC3372]. Il a été utilisé pour prendre en charge de nombreuses extensions propriétaires et non interopérables du fait de la faible définition de sa portée.

RFC 3326, Champ d'en-tête Reason pour SIP (S) : la [RFC3326] définit le champ d'en-tête Reason. Il est utilisé dans des demandes, comme BYE, pour indiquer la raison de l'envoi de la demande.

RFC 3388, Groupement de lignes de supports dans le protocole de description de session (SDP) (S) : la [RFC3388] définit un cadre pour grouper des flux de supports dans un message SDP. Un tel groupement permet d'exprimer des relations entre ces flux, comme quel flux est l'audio pour une alimentation vidéo particulière.

RFC 3420, Message/sipfrag de type de support Internet (S) : la [RFC3420] définit un objet MIME qui contient un fragment de message SIP. Seuls certains champs d'en-tête et parties du message SIP sont présents. Par exemple, il est utilisé pour rapporter les réponses reçues à une demande envoyée suite à un REFER.

RFC 3608, Champ d'en-tête d'extension du protocole d'initialisation de session (SIP) pour la découverte de chemin de service durant l'enregistrement SIP (S) : la [RFC3608] permet à un client de déterminer, à partir d'une réponse REGISTER, un chemin de mandataires à utiliser dans les demandes qu'il envoie en dehors d'un dialogue. Il peut aussi être utilisé par les mandataires pour vérifier l'en-tête Route dans les demandes initiées par le client. Sous de nombreux aspects, il est l'inverse du champ d'en-tête Path, mais a eu peu d'usage parce que les mandataires sortants par défaut ont été suffisants dans de nombreux déploiements.

RFC 3841, Préférences d'appelant pour SIP (S) : la [RFC3841] définit un ensemble d'en-têtes qu'un client peut inclure dans une demande pour contrôler la façon dont la demande est acheminée en aval. Elle permet à un client de diriger une demande sur un UA avec des capacités spécifiques, qu'un UA indique en utilisant la [RFC3840].

RFC 4028, Temporisateurs de session dans SIP (S) : la [RFC4028] définit un mécanisme de maintien en vie pour la signalisation SIP. Il est principalement destiné à fournir un moyen de nettoyer le vieil état dans les mandataires qui conservent l'état d'appel pour les appels provenant de points d'extrémité défaillants qui ne se sont jamais terminés normalement. En dépit de son nom, le temporisateur de session n'est pas un mécanisme pour détecter une défaillance du réseau à mi-appel. Les temporisateurs de session introduisent une grande complexité pour un gain relativement faible, et elle a eu un déploiement modéré.

RFC 4168, SCTP comme transport pour SIP (S) : la [RFC4168] définit comment transporter les messages SIP sur le protocole de transmission de commandes de flux (SCTP) [RFC4960]. SCTP a un usage très limité pour le transport SIP.

RFC 4244, Extension à SIP pour les informations d'historique de demande (S) : la [RFC4244] définit le champ d'en-tête History-Info, qui indique les informations sur comment et pourquoi un appel en est venu à être acheminé à une destination particulière.

RFC 4145, Transport de supports fondé sur TCP dans le protocole de description de session (SDP) (S) : la [RFC4145] définit une extension à SDP pour établir des sessions fondées sur TCP entre des agents d'utilisateur. Elle définit qui établit la connexion et comment son cycle de vie est géré. Elle a eu relativement peu d'usage dû au petit nombre de types de supports qui utilisent TCP aujourd'hui.

RFC 4091, Sémantique des types d'adresse de réseau de remplacement (ANAT) pour le cadre de groupage du protocole de description de session (SDP) (S) : la [RFC4091] définit un mécanisme pour inclure des adresses IPv4 et IPv6 comme solution de remplacement pour une session de supports. Ce mécanisme a été déconseillé en faveur de ICE [RFC5245].

RFC 6871, Négociation de capacités de support SDP (S) : la [RFC6871] définit une extension au cadre de négociation de capacité SDP [RFC5939] pour négocier les codecs, les paramètres de codec, et les flux de supports.

RFC 5621, Traitement du corps de message dans le protocole d'initialisation de session (SIP) : la [RFC5621] précise le traitement des corps dans SIP, se concentrant principalement sur le comportement multi-parties, qui était sous spécifié dans SIP.

## 6. Traversée de NAT

Ces extensions de SIP visent principalement la traversée de NAT pour SIP.

RFC 5245, Établissement de connexité interactive (ICE) (S) : la [RFC5245] définit une technique pour la traversée de NAT des sessions de supports pour les protocoles qui utilisent le modèle d'offre/réponse. Cette spécification est le mécanisme recommandé par l'IETF pour la traversée de NAT pour les flux de supports SIP, et est destinée à être utilisée même par les points d'extrémité qui ne sont eux-mêmes jamais derrière un NAT. Une étiquette d'option SIP et une étiquette de caractéristique de support [RFC5768] ont été définies pour être utilisées avec ICE.

RFC 5768, Candidats TCP avec indication de la prise en charge de l'établissement de connexité interactive (ICE) (S) : la [RFC5768] spécifie l'usage de ICE pour les flux TCP. Cela permet le choix de voix fondée sur RTP par dessus TCP seulement quand des NAT ou des pare-feu empêcheraient la voix fondée sur UDP de fonctionner.

RFC 3605, Attribut du protocole de contrôle en temps réel (RTCP) dans le protocole de description de session (SDP) (S) : la [RFC3605] définit un moyen de signaler explicitement, dans un message SDP, l'adresse et l'accès IP pour RTCP, plutôt que d'utiliser la règle d'accès+1 du protocole de transport en temps réel (RTP) [RFC3550]. Il est nécessaire pour les appareils derrière un NAT, et la spécification est exigée par ICE.

RFC 5626, Gestion des connexions initiées par le client sur SIP (S) : la [RFC5626], aussi appelée sortie SIP, définit des changements importants au mécanisme d'enregistrement SIP qui permettent la livraison de messages SIP à un UA quand il est derrière un NAT.

RFC 3581, Extension à SIP pour l'acheminement symétrique de réponse (S) : la [RFC3581] définit le paramètre rport de l'en-tête Via. Il permet aux réponses SIP de traverser le NAT.

RFC 5627, Obtention et utilisation d'identifiants d'agent d'utilisateur mondialement acheminable (GRUU) dans SIP (S) : la [RFC5627] définit un mécanisme pour diriger les demandes vers une instance d'UA spécifique. Le GRUU est essentiel pour les caractéristiques comme le transfert et fournit une autre pièce de l'histoire de la traversée de NAT de SIP.

## 7. Primitives de commande d'appel

De nombreuses extensions SIP donnent une boîte à outils de techniques de gestion de dialogue et d'appel. Ces techniques ont été combinées pour construire de nombreux services fondés sur SIP.

RFC 3515, Méthode REFER (S) : REFER [RFC3515] définit un mécanisme pour demander à un agent d'utilisateur d'envoyer une demande SIP. C'est une forme de contrôle à distance de SIP, et c'est le principal outil utilisé pour le transfert d'appel dans SIP. Il faut faire attention que toutes les utilisations potentielles de REFER (ni tous les schémas d'URI) ne sont pas bien définies. Les mises en œuvre devraient seulement utiliser celles qui sont bien définies, et ne devraient pas compter ou supposer à priori le comportement des autres pour éviter des comportements inattendus de la part des UA distants, des problèmes d'interopérabilité, et autres mauvaises surprises.

RFC 3725, Bonnes pratiques actuelles pour le contrôle d'appel de tiers (3pcc) (B) : la [RFC3725] définit un certain nombre de flux d'appels différents qui permettent à une entité SIP, appelée le contrôleur, de créer des sessions SIP parmi d'autres agents d'utilisateur SIP.

RFC 3911, Champ d'en-tête SIP Join (S) : la [RFC3911] définit le champ d'en-tête Join. Lorsque envoyé dans un INVITE, il cause la jonction du receveur au dialogue résultant dans une conférence avec un autre dialogue en cours.

RFC 3891, En-tête SIP Replaces (S) : la [RFC3891] définit un mécanisme qui permet à un nouveau dialogue de remplacer un dialogue existant. Il est utile pour certains services de transfert évolués.

RFC 3892, Mécanisme SIP Referred-By (S) : la [RFC3892] définit le champ d'en-tête Referred-By. Il est utilisé dans les demandes déclenchées par REFER, et donne l'identité de la partie référente à la partie référée.

RFC 4117, Invocation de services de transcodage dans SIP en utilisant la commande d'appel de tiers (3pcc) (I) : la [RFC4117] définit comment utiliser 3pcc pour l'invocation de services de transcodage pour un appel.

## 8. Cadre d'événement

RFC 3265, Notification d'événement spécifique de SIP (S) : la [RFC3265] définit les méthodes SUBSCRIBE et NOTIFY. Ces deux méthodes fournissent un cadre général de notification d'événement pour SIP. Pour utiliser réellement le cadre, les extensions doivent être définies pour des paquetages d'événement spécifiques. Un paquetage d'événements définit un schéma pour les données d'événement et décrit les autres aspects du traitement d'événement spécifique de ce schéma. La mise en œuvre de la RFC 3265 est exigée quand un paquetage d'événements est utilisé.

RFC 3903, Extension à SIP pour la publication d'état d'événement (S) : la [RFC3903] définit la méthode PUBLISH. Ce n'est pas un paquetage d'événements, mais elle est utilisée par tous les paquetages d'événement comme mécanisme pour pousser un événement dans le système.

RFC 4662, Extension de notification d'événement du protocole d'initialisation de session (SIP) pour les listes de ressources (S) : la [RFC4662] définit une extension à la RFC 3265 qui permet à un client de s'abonner à une liste de ressources en utilisant un seul abonnement. Le serveur, appelé un serveur de liste de ressources (RLS, *Resource List Server*) va "étendre" l'abonnement et s'abonner à chaque membre individuel de la liste. Elle a trouvé son applicabilité principalement dans le domaine de la présence, mais peut être utilisée avec tout paquetage d'événements.

RFC 5839, Extension aux événements du protocole d'initialisation de session (SIP) pour la notification d'événement conditionnel (S) : la [RFC5839] définit une extension à la RFC 3265 pour optimiser les performances des notifications. Quand un client s'abonne, il peut indiquer quelle version d'un document il a afin que le serveur puisse sauter l'envoi d'une notification si le client est à jour. Elle est applicable à tout paquetage d'événements.

## 9. Paquetages d'événement

Ce sont les paquetages d'événement définis pour utiliser le cadre d'événements de SIP. Beaucoup d'entre eux sont aussi mentionnés ailleurs dans leurs domaines respectifs.

RFC 3680, Paquetage d'événements SIP pour les enregistrements (S) : la [RFC3680] définit un paquetage d'événements pour trouver les changements de l'état d'enregistrement.

RFC 5628 (S) : la [RFC5628] est une extension du paquetage d'événements d'enregistrement [RFC3680] qui permet aux agents d'utilisateur d'apprendre leurs GRUU. C'est particulièrement utile pour aider à synchroniser un client et son registraire avec leur GRUU temporaire actuellement valide.

RFC 3842, Paquetage d'événement Résumé de message et Indication de message en attente pour SIP (S) : la [RFC3842] définit un moyen pour qu'un agent d'utilisateur découvre les messages vocaux et autres messages en attente pour lui. Son principal objet est d'activer le voyant de message vocal en attente sur la plupart des téléphones professionnels.

RFC 3856, Paquetage d'événement de présence pour SIP (S) : la [RFC3856] définit un paquetage d'événements pour indiquer la présence d'utilisateurs avec SIP.

RFC 3857, Paquetage-gabarit d'événement d'information d'observateur pour SIP (S) : la [RFC3857], aussi appelée winfo, donne un mécanisme pour qu'un agent d'utilisateur trouve quels abonnements sont en place pour un paquetage d'événements particulier. Son principal usage est avec présence, mais il peut être utilisé avec tout paquetage d'événements.

RFC 4235, Paquetage d'événement de dialogue initié par INVITE pour SIP (S) : la [RFC4235] définit un paquetage d'événements pour apprendre l'état des dialogues en cours chez un agent d'utilisateur, et est une des nombreuses RFC qui commencent par le numéro important de 42 [HGTTG].

RFC 4575, Paquetage d'événement SIP pour l'état de Conférence (S) : la [RFC4575] définit un mécanisme pour apprendre les changements de l'état de conférence, incluant des membres de la conférence.

RFC 4730, Paquetage d'événement SIP pour stimulus à pression de touche (KPML) (S) : la [RFC4730] définit un moyen pour qu'une application dans le réseau s'abonne à l'ensemble de pressions de touches faites sur le clavier d'un téléphone traditionnel. C'est, avec la [RFC4733], un des deux mécanismes définis pour traiter le DTMF. La RFC 4730 est une solution de chemin de signalisation, et la RFC 4733 est une solution de chemin de supports.

RFC 6035, Paquetage d'événements SIP pour le rapport de la qualité de la voix (S) : la [RFC6035] définit un paquetage d'événements SIP qui permet la collecte et le rapport de métriques qui mesurent la qualité pour les sessions de voix sur le protocole Internet (VoIP).

RFC 6794, Cadre pour les politiques de session du protocole d'initialisation de session (SIP) (S) : la [RFC6794] définit un cadre pour les politiques de session. Dans ce cadre, les serveurs de politique sont utilisés pour dire à l'agent d'utilisateur les caractéristiques de support requises pour une session particulière. Le cadre de politique de session n'a pas été largement mis en œuvre.

RFC 6795, Paquetage d'événements SIP pour les politiques de session spécifiques de la session (S) : la [RFC6795] définit un paquetage d'événements SIP utilisé en conjonction avec le cadre de politique de session [RFC6794].

RFC 5362, Paquetage d'événements Ajouts en instance du protocole d'initialisation de session (S) : la [RFC5362] définit un paquetage d'événements SIP qui permet à un UA d'apprendre si le consentement a été donné pour l'ajout d'une adresse à une "liste de diffusion" SIP. Il est utilisé en conjonction avec le cadre SIP pour le consentement [RFC5360].

## 10. Qualité de service

Plusieurs spécifications se consacrent aux interactions de SIP avec les mécanismes de qualité de service (QS) du réseau.

RFC 3312, Intégration de gestion de ressource et SIP (S) : la [RFC3312], mise à jour par la [RFC4032], définit un moyen de s'assurer que le téléphone de l'appelé ne sonne pas avant qu'une réservation de QS ait été installée dans le réseau. Elle fait cela en définissant un cadre général de préconditions, qui définit les conditions qui doivent être vraies afin qu'une session SIP se poursuive.

RFC 5432, Choix d'un mécanisme de qualité de service (QS) dans le protocole de description de session (SDP) (S) : la [RFC5432] définit un moyen pour que les agents d'utilisateur négocient quel type de mécanisme de QS de bout en bout utiliser pour une session. Pour l'instant, deux peuvent être utilisés : le protocole de réservation de ressource (RSVP, *Resource Reservation Protocol*) et prochaines étapes de signalisation (NSIS, *Next Steps in Signaling*). Cette négociation est faite par une extension à SDP. Du fait du déploiement limité de RSVP et du déploiement encore plus limité de NSIS, cette extension n'est pas largement utilisée.

RFC 3313, Extensions privées à SIP pour l'autorisation de support (I) : la [RFC3313] définit un en-tête P- qui donne un mécanisme pour passer un jeton d'autorisation entre SIP et un protocole de réservation de QS du réseau comme RSVP. Son objet est de s'assurer que la QS du réseau n'est accordée que si un client a fait un appel SIP à travers le réseau du même fournisseur. Cette spécification est parfois appelée la spécification du jardin clos de SIP par les vrais androïdes paranoïaques de la communauté SIP. C'est parce qu'elle exige le couplage de la signalisation et du réseau IP sous-jacent.

RFC 3524, Transposition de flux de support en flux de réservation de ressource (S) : la [RFC3524] définit un usage du cadre de groupement SDP pour indiquer qu'un ensemble de flux de supports devrait être traité par une seule réservation de ressource.

## 11. Opérations et gestion

Plusieurs spécifications ont été définies pour prendre en charge le fonctionnement et la gestion des systèmes SIP. Cela inclut des mécanismes pour les diagnostics de configuration et du réseau.

RFC 6080, Cadre pour la livraison de profil d'agent d'utilisateur SIP (S) : la [RFC6080] définit un mécanisme qui permet à un agent d'utilisateur SIP d'amorcer sa configuration à partir du réseau et de recevoir des mises à jour de sa configuration, si elle devait changer. C'est considéré comme un élément essentiel du déploiement d'un réseau SIP utilisable.

RFC 6035, Paquetage d'événement SIP pour le rapport de la qualité vocale (S) : la [RFC6035] définit un paquetage d'événements SIP qui permet la collecte et le rapport des métriques de qualité des sessions de voix sur IP (VoIP).

## 12. Compression SIP

Sigcomp [RFC3320], [RFC4896] a été défini pour permettre la compression de messages SIP sur des liaisons à faible bande passante. Sigcomp ne fait pas formellement partie de SIP. Cependant, l'usage de Sigcomp avec SIP a exigé des extensions à SIP.

RFC 3486, Compression de SIP (S) : la [RFC3486] définit un paramètre d'URI SIP qui peut être utilisé pour indiquer qu'un serveur SIP prend en charge Sigcomp.

RFC 5049, Application de la compression de signalisation (SigComp) au protocole d'initialisation de session (SIP) (S) : la [RFC5049] définit comment appliquer Sigcomp à SIP.

## 13. URI de service SIP

Plusieurs extensions définissent des services bien connus qui peuvent être invoqués par la construction de demandes avec des structures spécifiques pour l'URI de demande, résultant en comportements spécifiques au serveur d'agent d'utilisateur (UAS, *User Agent Server*).

RFC 3087, Contrôle de contexte de service en utilisant l'URI de demande SIP (I) : la [RFC3087] a introduit le contexte d'utilisation des URI de demande, codés de façon appropriée, pour invoquer les services.

RFC 4662, Extension de notification d'événement SIP pour les listes de ressources (S) : la [RFC4662] définit une ressource appelée un serveur de liste de ressources (RLS). Un client peut envoyer une demande d'abonnement à ce serveur. Le serveur va générer une série d'abonnements, compiler les informations résultantes, et les renvoyer à l'abonné. L'ensemble de ressources auxquelles le RLS va s'abonner est une propriété de l'URI de demande dans la demande SUBSCRIBE.

RFC 5363, Cadre et considérations sur la sécurité pour les services de liste d'URI du protocole d'initialisation de session (SIP) (S) : la [RFC5363] définit le cadre pour les services de liste dans SIP. Dans ce cadre, un UA peut inclure un objet liste XML dans le corps de diverses demandes et le serveur va fournir des services en mode liste en conséquence. Par exemple, un SUBSCRIBE avec une liste s'abonne à l'URI dans la liste.

RFC 5367, Abonnements aux listes de ressources contenues dans les demandes dans SIP (S) : la [RFC5367] utilise le cadre de liste d'URI de la [RFC5363] et permet à un client de s'abonner à une ressource appelée un serveur de liste de ressources. Ce serveur va générer des abonnements à l'URI dans la liste, compiler les informations résultantes, et les renvoyer à l'abonné.

RFC 5365, Demandes MESSAGE à destinataires multiples dans SIP (S) : la [RFC5365] utilise le cadre de liste d'URI de la [RFC5363] et permet à un client d'envoyer un MESSAGE à un certain nombre de receveurs.

RFC 5366, Établissement de conférence en utilisant des listes contenues dans les demandes dans SIP (S) : la [RFC5366] utilise le cadre de liste d'URI de la [RFC5363]. Elle permet à un client de demander au serveur d'agir comme point de concentration de conférence et d'envoyer une invitation à chaque receveur de la liste.

RFC 4240, Services de base de support réseau avec SIP (I) : la [RFC4240] définit un moyen pour que les serveurs d'application SIP invoquent les services d'annonce et de conférence à partir d'un serveur de supports. Cela est fait par un ensemble de paramètres d'URI définis qui disent quoi faire au serveur de supports, comme quel fichier exécuter et dans quelle langage le rendre.

RFC 4458, URI du protocole d'initialisation de session (SIP) pour des applications comme la messagerie vocale et la réponse vocale interactive (IVR) (I) : la [RFC4458] définit un moyen d'invoquer les services de messagerie vocale et d'IVR en utilisant un URI SIP construit d'une façon particulière.

## 14. Extensions mineures

Ces extensions SIP ne tiennent pas facilement dans un seul cas d'utilisation spécifique. Elles ont une applicabilité assez

générale, mais résolvent un problème relativement étroit ou fournissent une optimisation.

RFC 4488, Suppression de l'abonnement implicite REFER (S) : la [RFC4488] définit une amélioration à REFER. REFER crée normalement un abonnement implicite à la cible du REFER. Cet abonnement est utilisé pour repasser les mises à jour sur les progrès de la référence. Cette extension permet que cet abonnement implicite soit outrepassé à titre d'optimisation.

RFC 4538, Autorisation de demande par identification de dialogue dans SIP (S) : la [RFC4538] donne un mécanisme qui permet à un UAS d'autoriser une demande parce que le demandeur prouve qu'il connaît le dialogue en cours avec l'UAS. La spécification est utile en conjonction avec le cadre SIP d'interaction d'application [RFC5629].

RFC 4508, Étiquettes de portage des caractéristiques avec la méthode REFER de SIP (S) : la [RFC4508] définit un mécanisme pour porter les étiquettes de caractéristiques de la RFC 3840 dans REFER. Elle est utile pour informer la cible du REFER des caractéristiques de la cible prévue de la demande référencée.

RFC 5373, Demande des modes de réponse pour SIP (S) : la [RFC5373] définit une extension pour indiquer à l'appelé si le téléphone devrait ou non sonner et/ou avoir une réponse immédiate. Ceci est utile pour les applications de bouton poussoir et de diagnostic.

RFC 5079, Rejet des demandes anonymes dans SIP (S) : la [RFC5079] définit un mécanisme pour qu'un appelé indique à l'appelant qu'un appel a été rejeté parce que l'appelant est anonyme. Ceci est nécessaire pour la mise en œuvre de la caractéristique de rejet d'appel anonyme (ACR, *Anonymous Call Rejection*) dans SIP.

RFC 5368, Référence à des ressources multiples dans SIP (S) : la [RFC5368] permet à un UA d'envoyer un REFER pour demander au receveur du REFER de générer plusieurs demandes SIP, pas juste une. Ceci est utile pour les conférences, où un client pourrait vouloir demander à un serveur de conférence d'éjecter plusieurs utilisateurs.

RFC 4483, Mécanismes pour le contenu indirect dans les messages du protocole d'initialisation de session (SIP) (S) : la [RFC4483] définit un mécanisme pour diriger le contenu. Au lieu de porter un objet dans un corps SIP, l'URL de référence est porté à sa place, et le receveur déréférence l'URL pour obtenir l'objet. La spécification a une applicabilité potentielle pour l'envoi de grands messages instantanés, mais n'a pas encore trouvé beaucoup d'utilisations réelles.

RFC 3890, Modificateur de bande passante indépendant du transport pour le protocole de description de session (SDP) (S) : la [RFC3890] spécifie une extension à SDP qui permet la description de la bande passante pour une session de support qui est indépendante du mécanisme de transport sous-jacent.

RFC 4583, Format du protocole de description de session (SDP) pour les flux du protocole de contrôle à codage binaire de la prise de parole (BFCP) (S) : la [RFC4583] définit un mécanisme de SDP pour signaler les flux de contrôle de la prise de parole qui utilisent BFCP. Elle est utilisée pour les commandes de bouton poussoir et de prise de parole dans les conférences.

RFC 5898, Préconditions de connexité pour les flux de support du protocole de description de session (SDP) (S) : la [RFC5898] définit un usage du cadre de précondition [RFC3312]. La précondition de connexité assure que la session n'est pas établie tant que la connexité de paquet réelle n'est pas vérifiée.

RFC 4796, Attribut de contenu du protocole SDP (S) : la [RFC4796] définit un attribut SDP pour décrire l'objet d'un flux de supports. Les exemples incluent une vue de transparents, l'orateur, un signe de langage, et ainsi de suite.

RFC 6157, Transition IPv6 dans le protocole d'initialisation de session (SIP) (S) : la [RFC6157] définit les pratiques pour l'interfonctionnement entre IPv6 et les agents d'utilisateur IPv6. Ceci est fait à travers des mandataires multi-rattachements qui interagissent avec IPv4 et IPv6, ainsi qu'avec ICE [RFC5245] pour la traversée des supports. La spécification inclut des extensions mineures et des précisions à SDP afin de couvrir quelques cas supplémentaires.

RFC 5923, Réutilisation de connexion dans le protocole d'initialisation de session (SIP) (S) : la [RFC5923] définit une extension à SIP qui permet qu'une connexion de la sécurité de la couche transport (TLS, *Transport Layer Security*) entre des serveurs soit réutilisée pour des demandes dans les deux directions. Normalement, deux connexions sont établies entre une paire de serveurs, une pour les demandes dans chaque direction.

## 15. Mécanismes de sécurité

Plusieurs extensions fournissent des caractéristiques de sécurité supplémentaires pour SIP.

RFC 4474, Améliorations de la gestion d'identité authentifiée dans SIP (S) : la [RFC4474] définit un mécanisme pour fournir une identité cryptographiquement vérifiable de l'appelant dans une demande SIP. Appelé "Identité SIP", ce mécanisme fournit une solution de remplacement à la RFC 3325. Elle a eu peu de déploiements jusqu'à présent, mais son importance comme construction clé pour les techniques anti pourriels et de nouveaux mécanismes de sécurité en fait une partie centrale des spécifications SIP.

RFC 4916, Identité connectée dans le protocole d'initialisation de session (SIP) (S) : la [RFC4916] met formellement à jour la RFC 3261. Elle définit une extension à SIP qui permet à un utilisateur appelant de déterminer l'identité de l'appelé final (partie connectée). Du fait des services de transmission et de reciblage, ce peut n'être pas le même que l'utilisateur que l'appelant essayait à l'origine de joindre. Le mécanisme fonctionne en tandem avec la spécification d'identité SIP [RFC4474] pour fournir des signatures sur l'identité de la partie connectée. Elle peut aussi être utilisée si l'identité d'une partie change à mi-appel du fait d'actions de contrôle d'appel de tiers ou du comportement du RTPC.

RFC 5630, Utilisation du schéma d'URI SIPS dans le protocole d'initialisation de session (SIP) (S) : la [RFC5630] est destinée à mettre à jour la RFC 3261. Elle révisé le traitement de l'URI SIPS, originellement défini dans la RFC 3261, pour corriger de nombreuses erreurs et problèmes qui ont été rencontrés avec ce mécanisme.

RFC 5923, Certificats de domaine dans le protocole d'initialisation de session (SIP) (B) : la [RFC5923] précise l'usage de SIP sur TLS à l'égard du traitement de certificat, et définit des procédures supplémentaires nécessaires pour l'interopérabilité.

RFC 3323, Mécanisme de confidentialité pour le protocole d'initialisation de session (SIP) (S) : la [RFC3323] définit le champ d'en-tête "Privacy", utilisé par les clients pour demander l'anonymat pour leurs demandes. Bien qu'il définisse plusieurs services de confidentialité, le seul largement utilisé est celui qui prend en charge la confidentialité du champ d'en-tête P-Asserted-Identity [RFC3325].

RFC 4567, Extensions de gestion de clé pour le protocole de description de session (SDP) et le protocole de flux en temps réel (RTSP) (S) : la [RFC4567] définit des extensions à SDP qui permettent de tunneler un protocole de gestion de clé, à savoir MIKEY [RFC3830], à travers des échanges d'offre/réponse. Ce mécanisme est une des trois techniques de chiffrement du protocole sûr de transport en temps réel (SRTP) spécifiées pour SIP, la sécurité de la couche de transport de datagrammes (DTLS, *Datagram Transport Layer Security*) [RFC5763] ayant été choisie comme solution finale.

RFC 4568, Descriptions de sécurité du protocole de description de session (SDP) pour les flux de supports (S) : la [RFC4568] définit des extensions à SDP qui permettent la négociation du matériel de chiffrement directement à travers l'offre/réponse, sans un protocole de gestion de clés séparé. Ce mécanisme, parfois appelé "sdescriptions", a l'inconvénient que les clés de supports sont disponibles à toute entité qui a la visibilité du SDP. C'est une des trois techniques de chiffrement de SRTP spécifiées pour SIP, DTLS-SRTP [RFC5763] ayant été choisi comme solution finale.

RFC 5763, Cadre pour établir un contexte de sécurité SRTP utilisant DTLS (S) : la [RFC5763] définit le cadre global et le traitement SDP et SIP exigé pour effectuer la gestion de clés pour RTP utilisant la TLS de datagrammes (DTLS) [RFC4347] directement entre les points d'extrémité, sur le chemin des supports. C'est une des trois techniques de chiffrement de SRTP spécifiées pour SIP, DTLS-SRTP [RFC5763] ayant été choisi comme solution finale.

RFC 3853, Exigences S/MIME de la norme de chiffrement évolué (AES) pour le protocole d'initialisation de session (SIP) (S) : la [RFC3853] met formellement à jour la RFC 3261. C'est une brève spécification qui met à jour les mécanismes cryptographiques utilisés dans SIP S/MIME. Cependant, SIP S/MIME a eu très peu de déploiements.

RFC 6072, Service de gestion de certificats pour le protocole d'initialisation de session (SIP) (S) : la [RFC6072] définit un service de certificat pour SIP dont l'objet est de faciliter le déploiement de S/MIME. Le service de certificat permet aux clients de mémoriser et restituer leurs propres certificats, en plus d'obtenir les certificats pour d'autres utilisateurs.

RFC 3893, Format de corps d'identité authentifiée du protocole d'initialisation de session (SIP) (S) : la [RFC3893] définit un fragment de message SIP qui peut être signé afin de fournir une identité authentifiée sur une demande. C'est un prédécesseur précoce de la [RFC4474], et par conséquent, le corps d'identité authentifiée n'a pas eu de déploiement.

SAML, Profil et lien SAML de SIP (S) : [SAML] définit l'usage du langage de balisage d'assertion de sécurité (SAML, *Security Assertion Markup Language*) au sein de SIP, et décrit comment l'utiliser en conjonction avec l'identité SIP [RFC4474] pour fournir des assertions authentifiées sur le rôle ou les attributs d'un utilisateur.

RFC 5360, Cadre pour les communications fondées sur le consentement dans le protocole d'initialisation de session (SIP) (S) : la [RFC5360] définit plusieurs extensions à SIP, incluant les champs d'en-tête "Trigger-Consent" et "Permission-Missing". Ces champs d'en-tête, en plus des autres procédures définies dans le document, définissent un moyen de gérer les membres d'une "liste de diffusion SIP" utilisée pour la messagerie instantanée ou les conférences. En particulier, elle aide à éviter le problème de l'utilisation de tels services d'amplification pour les besoins d'une attaque sur le réseau en s'assurant qu'un utilisateur autorise l'ajout de son adresse sur un tel service.

RFC 5361, Format de document pour demander le consentement (S) : la [RFC5361] définit un objet XML utilisé par le cadre de consentement. Les documents de consentement sont envoyés d'un "serveur de liste de diffusion" SIP aux utilisateurs pour leur permettre de gérer leur participation à des listes.

RFC 5362, Paquetage d'événements Ajouts en instance du protocole d'initialisation de session (S) : la [RFC5362] définit un paquetage d'événements SIP qui permet à un UA d'apprendre si le consentement a été donné à l'ajout d'une adresse à une "liste de diffusion" SIP. Elle est utilisée en conjonction avec le cadre SIP pour le consentement [RFC5360].

RFC 3329, Accord de mécanisme de sécurité pour SIP (S) : la [RFC3329] définit un mécanisme pour empêcher les attaques en dégradation en conjonction avec l'authentification SIP. Le mécanisme a eu un déploiement très limité. Il était défini au titre de la suite de spécifications 3GPP de sous système multimédia IP (IMS) [3GPP.24.229], et n'est nécessaire que quand il y a plusieurs mécanismes de sécurité déployés à un serveur particulier. En pratique, cela n'a pas été le cas.

RFC 4572, Transport sur support en mode connexion sur le protocole de sécurité de la couche Transport (TLS) dans le protocole de description de session (SDP) (S) : la [RFC4572] spécifie un mécanisme pour signaler les flux de supports fondés sur TLS entre les points d'extrémité. Elle étend les paramètres de signalisation de supports fondés sur TCP définis dans la [RFC4145] pour inclure des informations d'empreinte digitale pour les flux TLS afin que TLS puisse opérer entre des hôtes d'extrémité en utilisant des certificats auto signés.

RFC 5027, Préconditions de sécurité pour les flux de supports du protocole de description de session (S) : la [RFC5027] définit une précondition à utiliser avec le cadre de préconditions [RFC3312]. La précondition de sécurité empêche une session d'être établie tant qu'un flux de supports de sécurité n'est pas établi.

RFC 3310, Authentification par résumé dans le protocole de transfert Hypertexte (HTTP) utilisant l'authentification et l'accord de clés (AKA) (S) : la [RFC3310] définit une extension à l'authentification par résumé pour lui permettre de fonctionner avec les accreditifs mémorisés dans les téléphones cellulaires. Bien que techniquement ce soit une extension au résumé HTTP, son application principale est SIP. Cette extension est principalement utile pour les mises en œuvre de IMS.

RFC 4169, Authentification par résumé du protocole de transfert Hypertexte (HTTP) en utilisant l'accord de clé et d'authentification (AKA) version-2 (S) : la [RFC4169] est une amélioration de la [RFC3310] qui améliore encore la sécurité de l'authentification.

## 16. Conférence

De nombreuses extensions SIP et SDP visent les conférences comme principale application.

RFC 4574, Attribut Label du protocole de description de session (SDP) (S) : la [RFC4574] définit un attribut SDP pour fournir une étiquette opaque pour les flux de supports. Ces étiquettes peuvent être référencées par des documents externes, et en particulier, par des documents de politique de conférence. Cela permet à un UA de lier ensemble des documents qu'il peut obtenir par des mécanismes de conférence aux flux de supports auxquels ils se réfèrent.

RFC 3911, Champ d'en-tête SIP Join (S) : la [RFC3911] définit le champ d'en-tête Join. Quant il est envoyé dans un INVITE, il cause la jonction du receveur au dialogue résultant dans une conférence avec un autre dialogue en cours.

RFC 4575, Paquetage d'événement du protocole d'initialisation de session (SIP) pour l'état Conférence (S) : la [RFC4575] définit un mécanisme pour apprendre les changements de l'état de conférence, y compris des membres de la conférence.

RFC 5368, Référence à des ressources multiples dans le protocole d'initialisation de session (SIP) (S) : la [RFC5368] permet à un UA d'envoyer un REFER pour demander au receveur du REFER de générer plusieurs demandes SIP, pas juste une. C'est utile pour les conférences, où un client voudrait demander au serveur de conférence d'éjecter plusieurs utilisateurs.

RFC 5366, Établissement de conférence en utilisant des listes contenues dans des demandes dans le protocole d'initialisation de session (SIP) (S) : la [RFC5366] est similaire à la [RFC5367]. Cependant, au lieu de s'abonner à la ressource, une demande INVITE est envoyée à la ressource, et va agir comme un point de concentration de conférence et générer une invitation à chaque receveur de la liste.

RFC4579, Contrôle d'appel du protocole d'initialisation de session (SIP) - Conférence pour les agents d'utilisateur (B) : la [RFC4579] définit les bonnes pratiques de procédure et de flux d'appel pour les conférences. Cela inclut des créations de conférence, d'adhésion, et la numérotation, entre autres capacités.

RFC 4583, Format du protocole de description de session (SDP) pour les flux du protocole de contrôle à codage binaire de la prise de parole (BFCP) (S) : la [RFC4583] définit un mécanisme de SDP pour signaler les flux de contrôle de la prise de parole qui utilisent BFCP. Elle est utilisée pour les commandes de bouton poussoir et de prise de parole dans les conférences.

## 17. Messagerie instantanée, présence, et multimédia

SIP fournit des extensions pour la messagerie instantanée, la présence, et le multimédia.

RFC 3428, Extension SIP pour la messagerie instantanée (S) : la [RFC3428] définit la méthode MESSAGE, utilisée pour l'envoi d'un message instantané sans établir de session (parfois appelée "mode page").

RFC 3856, Paquetage d'événement de présence pour SIP (S) : la [RFC3856] définit un paquetage d'événements pour indiquer la présence d'un utilisateur par SIP.

RFC 3857, Paquetage-gabarit d'événement d'information d'observateur pour SIP (S) : la [RFC3857], aussi appelée "winfo", fournit un mécanisme pour qu'un agent d'utilisateur trouve quels abonnements sont en place pour un paquetage d'événements particulier. Son utilisation principale est avec présence, mais il peut être utilisé avec tout paquetage d'événements.

RFC 5547, Mécanisme d'offre/réponse du protocole de description de session (SDP) pour activer le transfert de fichier (S) : la [RFC5547] définit un mécanisme pour signaler une session de transfert de fichiers avec SIP.

## 18. Services d'urgence

Les services d'urgence incluent des caractéristiques de préemption, qui permettent à des individus autorisés d'obtenir l'accès aux ressources du réseau en cas d'urgence, avec les appels d'urgence traditionnels.

RFC 4411, Extension de l'en-tête Reason pour les événements de préemption du protocole d'initialisation de session (SIP) (S) : la [RFC4411] définit une extension de l'en-tête Reason, qui permet à un UA de savoir que son dialogue a été supprimé parce qu'une session de priorité supérieure est apparue.

RFC 4412, Priorité de ressource de communications pour SIP (S) : la [RFC4412] définit un nouveau champ d'en-tête, Resource-Priority, qui permet à une session d'obtenir un traitement prioritaire de la part du réseau.

RFC 6442, Véhicule de localisation pour le protocole d'initialisation de session (S) : la [RFC6442] définit un mécanisme pour porter des objets de localisation dans les messages SIP. C'est utilisé pour porter la localisation d'un UA à un serveur d'appel d'urgence.

## 19. Considérations sur la sécurité

La présente spécification fait un survol des spécifications existantes et n'introduit aucun problème de sécurité par elle-même. Bien sûr, le monde serait beaucoup plus sûr si chacun suivait cette règle simple : "Pas de panique !" [HGTTG].

## 20. Remerciements

L'auteur tient à remercier Spencer Dawkins, Brian Stucker, Keith Drage, John Elwell, et Avshalom Houry de leurs commentaires sur ce document.

## 21. Références pour information

- [3GPP.24.229] 3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 5.22.0, septembre 2008.
- [HGTTG] Adams, D., "The Hitchhiker's Guide to the Galaxy", septembre 1979.
- [RFC2026] S. Bradner, "Le processus de [normalisation de l'Internet](#) -- Révision 3", ([BCP0009](#)) octobre 1996. (*Remplace RFC1602, RFC1871*) (MàJ par [RFC3667](#), [3668](#), [3932](#), [3979](#), [3978](#), [5378](#), [6410](#), [8179](#), [8789](#), [9282](#))
- [RFC2543] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP : protocole d'initialisation de session", mars 1999. (*Obsolète, voir [RFC3261](#), [RFC3262](#), [RFC3263](#), [RFC3264](#), [RFC3265](#)*) (P.S.)
- [RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "Enregistrement de ressource DNS pour la spécification de la [localisation des services](#) (DNS SRV)", février 2000, DOI 10.17487/RFC2782.
- [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.)
- [RFC2976] S. Donovan, "Méthode INFO pour SIP", octobre 2000. (P.S., *Remplacée par la RFC6086*)
- [RFC3087] B. Campbell, R. Sparks, "Contrôle de contexte de service en utilisant l'URI de demande SIP", avril 2001. (*Information*)
- [RFC3204] E. Zimmerer et autres, "[Types de support MIME](#) pour objets ISUP et QSIG", décembre 2001. (MàJ par [RFC3459](#)) (P.S.)
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002, DOI 10.17487/RFC3261. (*Mise à jour par [3265](#), [3853](#), [4320](#), [4916](#), [5393](#), [6665](#), [8217](#), [8760](#)*)
- [RFC3262] J. Rosenberg et H. Schulzrinne, "[Fiabilité des réponses provisoires](#) dans le protocole d'initialisation de session (SIP)", juin 2002. (P.S.)
- [RFC3263] J. Rosenberg, H. Schulzrinne, "Protocole d'initialisation de session (SIP) : [Localisation des serveurs SIP](#)", juin 2002. (*Remplace [RFC2543](#)*) (P.S. ; MàJ par [RFC7984](#), [RFC8898](#))
- [RFC3264] J. Rosenberg et H. Schulzrinne, "[Modèle d'offre/réponse](#) avec le protocole de description de session (SDP)", juin 2002. (P.S. ; MàJ par [RFC8843](#), [9143](#))
- [RFC3265] A.B. Roach, "[Notification d'événement spécifique](#) du protocole d'initialisation de session (SIP)", juin 2002. (MàJ par [RFC6446](#)) (*Remplacée par la RFC6665*)
- [RFC3310] A. Niemi, J. Arkko, V. Torvinen, "Authentification par résumé dans le protocole de transfert Hypertexte (HTTP) utilisant l'authentification et l'accord de clés (AKA)", septembre 2002. (*Information*)
- [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.)
- [RFC3313] W. Marshall, éd., "Extensions privée du protocole d'initialisation de session (SIP) pour l'autorisation du support", janvier 2003. (*Information*)
- [RFC3320] R. Price, et autres, "[Compression de signalisation](#) (SigComp)", janvier 2003. (MàJ par [RFC4896](#)) (P.S.)
- [RFC3323] J. Peterson, "Mécanisme de [confidentialité pour le protocole d'initialisation](#) de session (SIP)", novembre 2002.
- [RFC3325] C. Jennings, J. Peterson et M. Watson, "[Extensions privées au protocole d'initialisation de session](#) (SIP) pour l'assertion d'identité au sein de réseaux de confiance", novembre 2002. (*Information* ; MàJ par [RFC8217](#))
- [RFC3326] H. Schulzrinne, D. Oran, G. Camarillo, "[Champ d'en-tête Reason](#) pour le protocole d'initialisation de session (SIP)", décembre 2002. (P.S. : MàJ par [RFC9366](#))
- [RFC3327] D. Willis, B. Hoeneisen, "[Champ d'en-tête d'extension](#) du protocole d'initialisation de session (SIP) pour enregistrer des contacts non adjacents", décembre 2002. (P.S.)
- [RFC3329] J. Arkko et autres, "[Accord de mécanisme de sécurité](#) pour le protocole d'initialisation de session (SIP)", janvier 2003. (P.S.)
- [RFC3372] A. Vemuri, J. Peterson, "[Protocole d'initialisation de session pour le téléphone](#) (SIP-T) : Contexte et architectures", septembre 2002. ([BCP0063](#))
- [RFC3388] G. Camarillo, G. Eriksson, J. Holler et H. Schulzrinne, "Groupage des lignes de support dans le protocole de description de session (SDP)", décembre 2002. (*Remplacée par* [RFC5888](#))
- [RFC3398] G. Camarillo et autres, "[Transposition du SSU RNIS en SIP](#)", décembre 2002. (P.S.)
- [RFC3401] M. Mealling, "[Système de découverte dynamique de délégation](#) (DDDS) Partie I : DDDS complet", octobre 2002. (*Info.*)
- [RFC3420] R. Sparks, "[message/sipfrag de type de support Internet](#)", novembre 2002.
- [RFC3427] A. Mankin et autres, "Processus des changements au protocole d'initialisation de session (SIP)", BCP 67, décembre 2002. (*Remplacée par* [RFC5727](#))
- [RFC3428] B. Campbell et autres, "[Extension de messagerie instantanée](#) pour le protocole d'initialisation de session (SIP)", décembre 2002.
- [RFC3482] M. Foster, T. McGarry, J. Yu, "[Portabilité des numéros dans le réseau téléphonique](#) commuté mondial (GSTN) : généralités", février 2003. (*Information*)
- [RFC3486] G. Camarillo, "[Compression du protocole d'initialisation de session](#) (SIP)", février 2003. (MàJ par [RFC5049](#)) (P.S.)
- [RFC3515] R. Sparks, "[Méthode Refer](#) du protocole d'initialisation de session (SIP)", avril 2003. (MàJ par [RFC8217](#))
- [RFC3524] G. Camarillo, A. Monrad, "[Transposition de flux de support en flux de réservation de ressource](#)", avril 2003. (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](#), [RFC8083](#), [RFC8108](#), [RFC8860](#))
- [RFC3578] G. Camarillo et autres, "[Transposition de la signalisation en chevauchement](#) du sous-système utilisateur (SSU) du réseau numérique à intégration de services (RNIS) dans le protocole d'initialisation de session (SIP)", août 2003. (P.S.)
- [RFC3581] J. Rosenberg, H. Schulzrinne, "[Extension au protocole d'initialisation de session \(SIP\)](#) pour l'acheminement à

réponse symétrique", août 2003. *(P.S.)*

- [RFC3605] C. Huitema, "[Attribut du protocole de contrôle](#) en temps réel (RTCP) dans le protocole de description de session (SDP)", octobre 2003. *(P.S.)*
- [RFC3608] D. Willis, B. Hoeneisen, "[Champ d'en-tête d'extension du protocole d'initialisation de session](#) (SIP) pour la découverte de chemin de service durant l'enregistrement", octobre 2003. *(P.S.)*
- [RFC3665] A. Johnston, S. Donovan, R. Sparks, C. Cunningham et K. Summers, "Exemples de flux d'appel de base du protocole d'initialisation de session (SIP)", BCP 75, décembre 2003.
- [RFC3666] A. Johnston et autres, "Flux d'appels du réseau téléphonique public commuté (RTPC) en protocole d'initialisation de session (SIP)", décembre 2003. ([BCP0076](#))
- [RFC3680] J. Rosenberg, "[Paquetage d'événements du protocole](#) d'initialisation de session (SIP) pour les enregistrements", mars 2004. *(P.S.)*
- [RFC3725] J. Rosenberg et autres, "Bonnes pratiques actuelles [pour la commande d'appel de tiers \(3pcc\)](#) dans le protocole d'initialisation de session (SIP)", avril 2004. ([BCP0085](#))
- [RFC3830] J. Arkko et autres, "MIKEY : [Gestion de clé multimédia pour l'Internet](#)", août 2004. (*MàJ par* [RFC4738](#)) *(P.S.)*
- [RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "[Indication des capacités d'agent d'utilisateur](#) dans le protocole d'initialisation de session (SIP)", août 2004
- [RFC3841] J. Rosenberg, H. Schulzrinne, P. Kyzivat, "[Préférences de l'appelant](#) pour le protocole d'initialisation de session (SIP)", août 2004. *(P.S.)*
- [RFC3842] R. Mahy, "[Paquetage d'événement Résumé de message](#) et Indication de message en attente pour le protocole d'initialisation de session (SIP)", août 2004.
- [RFC3853] J. Peterson, "[Exigences S/MIME de la norme de chiffrement évolué](#) (AES) pour le protocole d'initialisation de session (SIP)", juillet 2004. *(P.S.)*
- [RFC3856] J. Rosenberg, "[Paquetage d'événement Presence](#) pour le protocole d'initialisation de session (SIP)", août 2004.
- [RFC3857] J. Rosenberg, "[Paquetage-gabarit d'événement d'information](#) d'observateur pour le protocole d'initialisation de session (SIP)", août 2004. *(P.S.)*
- [RFC3890] M. Westerlund, "[Modificateur de bande passante indépendant du transport](#) pour le protocole de description de session (SDP)", septembre 2004. *(P.S.)*
- [RFC3891] R. Mahy, B. Biggs, R. Dean, "[En-tête "Replaces"](#) du protocole d'initialisation de session (SIP)", septembre 2004. *(P.S.)*
- [RFC3892] R. Sparks, "[Mécanisme Referred-by](#) du protocole d'initialisation de session (SIP)", septembre 2004. (*MàJ par* [RFC8217](#))
- [RFC3893] J. Peterson, "[Format de corps d'identité authentifiée](#) (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.
- [RFC3903] A. Niemi, "[Extension au protocole d'initialisation de session](#) (SIP) pour la publication d'état d'événement", octobre 2004.
- [RFC3910] V. Gurbani et autres, "[Protocole SPIRITS](#) (Services du RTPC demandant des services Internet)", octobre 2004. *(P.S.)*
- [RFC3911] R. Mahy, D. Petrie, "[En-tête "Join" du protocole](#) d'initialisation de session (SIP)", octobre 2004. *(P.S.)*
- [RFC3959] G. Camarillo, "[Type de disposition Session précoce](#) pour le protocole d'initialisation de session (SIP)",

décembre 2004. (P.S.)

- [RFC3960] G. Camarillo, H. Schulzrinne, "[Support précoce et génération des tonalités d'appel](#) dans le protocole d'initialisation de session (SIP)", décembre 2004. (Information)
- [RFC4028] S. Donovan, J. Rosenberg, "[Temporisateurs de session](#) dans le protocole d'initialisation de session (SIP)", avril 2005. (P.S.)
- [RFC4032] G. Camarillo, P. Kyzivat, "[Mise à jour du cadre de préconditions](#) du protocole d'initialisation de session (SIP)", mars 2005. (MàJ [RFC3312](#)) (P.S.)
- [RFC4091] G. Camarillo, J. Rosenberg, "[Sémantique des types d'adresse de réseau de remplacement](#) (ANAT) pour le cadre de groupage du protocole de description de session (SDP)", juin 2005. (P.S.)
- [RFC4117] G. Camarillo et autres, "Invocation de services de transcodage dans le protocole d'initialisation de session (SIP) en utilisant la commande d'appel de tiers (3pcc)", juin 2005. (Information)
- [RFC4145] D. Yon, G. Camarillo, "[Transport de support fondé sur TCP](#) dans le protocole de description de session (SDP)", septembre 2005. (MàJ par [RFC4572](#)) (P.S.)
- [RFC4168] J. Rosenberg et autres, "[Le protocole de transmission de contrôle de flux](#) (SCTP) comme transport pour le protocole d'initialisation de session (SIP)", octobre 2005. (P.S.)
- [RFC4169] V. Torvinen et autres, "Authentification par résumé du protocole de transfert Hypertext (HTTP) en utilisant l'accord de clé et d'authentification (AKA) version-2", novembre 2005. (Information)
- [RFC4235] J. Rosenberg et autres, "[Paquetage d'événement de dialogue](#) initié par INVITE pour le protocole d'initialisation de session (SIP)", novembre 2005. (P.S.)
- [RFC4240] E. Burger et autres, "Services de base de support réseau avec SIP", décembre 2005. (Information)
- [RFC4244] M. Barnes, éd., "Extension au protocole d'initialisation de session (SIP) pour les informations d'historique de demande", novembre 2005. (P.S.) (Remplacée par [RFC7044](#))
- [RFC4320] R. Sparks, "Actions visant les [problèmes identifiés dans la transaction Non-INVITE](#) du protocole d'initialisation de session (SIP)", janvier 2006. (MàJ [RFC3261](#)) (P.S.)
- [RFC4347] E. Rescorla, N. Modadugu, "[Sécurité de la couche de transport de datagrammes](#)", avril 2006. (P.S.)
- [RFC4411] J. Polk, "[Extension de l'en-tête Reason](#) pour les événements de préemption du protocole d'initialisation de session (SIP)", février 2006. (P.S.)
- [RFC4412] H. Schulzrinne et J. Polk, "[Priorité de ressource de communications](#) pour le protocole d'initialisation de session (SIP)", février 2006. (P.S.)
- [RFC4458] C. Jennings et autres, "URI du protocole d'initialisation de session (SIP) pour des applications comme la messagerie vocale et la réponse vocale interactive (IVR)", avril 2006. (Information ; MàJ par [RFC8119](#))
- [RFC4474] J. Peterson et C. Jennings, "Améliorations de la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", août 2006. (P.S. ; Remplacée par [RFC8224](#))
- [RFC4483] E. Burger, éd., "[Mécanismes pour le contenu](#) indirect dans les messages du protocole d'initialisation de session (SIP)", mai 2006. (P.S.)
- [RFC4488] O. Levin, "[Suppression de l'abonnement implicite](#) de la méthode REFER du protocole d'initialisation de session (SIP)", mai 2006. (P.S.)
- [RFC4497] J. Elwell et autres, "Interfonctionnement entre SIP et QSIG", mai 2006. ([BCP0117](#))
- [RFC4508] O. Levin, A. Johnston, "[Étiquettes de portage](#) des caractéristiques avec la méthode REFER du protocole d'initialisation de session (SIP)", mai 2006. (P.S. ; MàJ par [RFC8217](#))

- [RFC4538] J. Rosenberg, "[Autorisation de demande par identification](#) de dialogue dans le protocole d'initialisation de session (SIP)", juin 2006. (P.S.)
- [RFC4566] M. Handley, V. Jacobson et C. Perkins, "SDP : [Protocole de description de session](#)", juillet 2006. (P.S. ; remplacée par RFC8866)
- [RFC4567] J. Arkko et autres, "[Extensions de gestion de clés](#) pour le protocole de description de session (SDP) et le protocole d'écoulement en temps réel (RTSP)", juillet 2006. (P.S.)
- [RFC4568] F. Andreassen et autres, "[Définition d'attributs de sécurité](#) dans le protocole de description de session (SDP) pour les flux de support", juillet 2006. (P.S.)
- [RFC4572] J. Lennox, "Transport sur support en mode connexion sur le protocole de sécurité de la couche Transport (TLS) dans le protocole de description de session (SDP)", juillet 2006. (MàJ RFC4145) (P.S. ; remplacée par RFC8122)
- [RFC4574] O. Levin, G. Camarillo, "[Attribut Label](#) du protocole de description de session (SDP)", août 2006. (P.S.)
- [RFC4575] J. Rosenberg et autres, "[Paquetage d'événement](#) du protocole d'initialisation de session (SIP) pour l'état Conference", août 2006. (P.S.)
- [RFC4579] A. Johnston, O. Levin, "Commande d'appel du protocole d'initialisation de session (SIP) – Conférence pour agents d'utilisateur", août 2006. (BCP0119)
- [RFC4583] G. Camarillo, "Format de protocole de description de session (SDP) pour les flux du protocole de contrôle à codage binaire de la prise de parole (BFCP)", novembre 2006. (P.S. ; remplacée par RFC8856)
- [RFC4662] A. B. Roach et autres, "[Extension de notification d'événement](#) du protocole d'initialisation de session (SIP) pour les listes de ressources", août 2006. (P.S.)
- [RFC4730] E. Burger, M. Dolly, "[Paquetage d'événement du protocole d'initialisation de session](#) (SIP) pour stimulus par langage de balisage à pression de touche (KPML)", novembre 2006. (P.S.)
- [RFC4733] H. Schulzrinne, T. Taylor, "[Charge utile RTP pour chiffres DTME](#), tonalités téléphoniques, et signaux de téléphonie", décembre 2006. (Remplace RFC2833) (MàJ par RFC4734, RFC5244) (P.S.)
- [RFC4796] J. Hautakorpi, G. Camarillo, "[Attribut Contenu](#) du protocole de description de session (SDP)", février 2007. (P.S.)
- [RFC4896] A. Surtees et autres, "[Corrections et précisions](#) à la compression de signalisation (SigComp)", juin 2007. (MàJ RFC3320, RFC3321, RFC3485) (P.S.)
- [RFC4916] J. Elwell, "[Identité connectée](#) dans le protocole d'initialisation de session (SIP)", juin 2007. (MàJ RFC3261) (P.S.)
- [RFC4960] R. Stewart, éd., "Protocole de transmission de commandes de flux (SCTP)", septembre 2007. (Remplace RFC2960, RFC3309 ; P.S. ; Remplacée par RFC9260)
- [RFC5027] F. Andreassen, D. Wing, "[Préconditions de sécurité](#) pour les flux de support du protocole de description de session (SDP)", octobre 2007. (MàJ RFC3312) (P.S.)
- [RFC5059] N. Bhaskar et autres, "[Mécanisme de routeur d'amorçage](#) (BSR) pour la diffusion groupée indépendante du protocole (PIM)", janvier 2008. (Remplace RFC2362) (MàJ RFC4601) (P.S.)
- [RFC5079] J. Rosenberg, "[Rejet des demandes anonymes](#) dans le protocole d'initialisation de session (SIP)", décembre 2007. (P.S.)
- [RFC5245] J. Rosenberg, "Établissement de connectivité interactive (ICE) : Protocole pour la traversée de traducteur d'adresse réseau (NAT) pour les protocoles d'offre/réponse", avril 2010. (P. S. ; remplace RFC4091, 4092 ; remplacée par 8445)

- [RFC5360] J. Rosenberg et autres, "[Cadre des communications fondées sur le consentement](#) dans le protocole d'initialisation de session (SIP)", octobre 2008. (P.S. ; MàJ par [RFC8217](#))
- [RFC5361] G. Camarillo, "[Format de document](#) pour une demande de consentement", octobre 2008. (P.S.)
- [RFC5362] G. Camarillo, "[Paquetage d'événements Ajouts en instance](#) du protocole d'initialisation de session (SIP)", octobre 2008. (P.S.)
- [RFC5363] G. Camarillo, A.B. Roach, "[Cadre et considérations sur la sécurité](#) pour les services URI-List du protocole d'initialisation de session (SIP)", octobre 2008. (P.S.)
- [RFC5365] M. Garcia-Martin, G. Camarillo, "[Demandes MESSAGE](#) à destinataires multiples dans le protocole d'initialisation de session (SIP)", octobre 2008. (P.S.)
- [RFC5366] G. Camarillo, A. Johnston, "[Établissement de conférence](#) en utilisant des listes contenues dans des demandes dans le protocole d'initialisation de session (SIP)", octobre 2008. (P.S.)
- [RFC5367] G. Camarillo et autres, "[Abonnements aux listes de ressources](#) contenues dans les demandes dans le protocole d'initialisation de session (SIP)", octobre 2008. (MàJ [RFC3265](#)) (P.S.)
- [RFC5368] G. Camarillo et autres, "[Référence à des ressources multiples](#) dans le protocole d'initialisation de session (SIP)", octobre 2008. (P.S. ; MàJ par [RFC8262](#))
- [RFC5373] D. Willis, éd., A. Allen, "[Demande de modes de réponse](#) pour le protocole d'initialisation de session (SIP)", novembre 2008. (P.S.)
- [RFC5393] R. Sparks et autres, "[Correction d'une faiblesse de la sécurité](#) des mandataires de fourchement dans le protocole d'initialisation de session (SIP)", décembre 2008. (MàJ [RFC3261](#)) (P.S.)
- [RFC5432] J. Polk et autres, "Sélection du mécanisme de qualité de service dans le protocole de description de session (SDP)", mars 2009. (P. S.)
- [RFC5547] M. Garcia-Martin, M. Isomaki, G. Camarillo, S. Loreto, P. Kyzivat, "Mécanisme d'offre/réponse du protocole de description de session (SDP) pour activer le transfert de fichier", mai 2009. (P. S.)
- [RFC5621] G. Camarillo, "Traitement du corps de message dans le protocole d'initialisation de session (SIP)", septembre 2009. (MàJ [RFC3204](#), [RFC3261](#), [RFC3459](#)) (P. S. ; MàJ par [RFC8262](#))
- [RFC5626] C. Jennings, R. Mahy, F. Audet, éd., "[Gestion des connexions initiées par le client](#) dans le protocole d'initialisation de session (SIP)", octobre 2009, DOI 10.17487/RFC5626. (MàJ [RFC3261](#), [RFC3327](#)) (P. S.)
- [RFC5627] J. Rosenberg, "[Obtention et utilisation des URI](#) d'agent d'utilisateur mondialement acheminable (GRUU) dans le protocole d'initialisation de session (SIP)", octobre 2009. (P. S.)
- [RFC5628] P. Kyzivat, "[Extension de paquetage d'événement d'engistrement](#) pour les URI d'agent d'utilisateur mondialement acheminables (GRUU) du protocole d'initialisation de session (SIP)", octobre 2009. (P. S.)
- [RFC5629] J. Rosenberg, "[Cadre de l'interaction d'application](#) dans le protocole d'initialisation de session (SIP)", octobre 2009. (P.S.)
- [RFC5630] F. Audet, "[Utilisation du schéma d'URI SIPS](#) dans le protocole d'initialisation de session (SIP)", octobre 2009. (MàJ [RFC3261](#), [RFC3608](#)) (P. S.)
- [RFC5658] T. Froment, C. Lebel, B. Bonnaerens, "Questions d'adressage de Record-Route dans le protocole d'initialisation de session (SIP)", octobre 2009. (P. S.)
- [RFC5763] J. Fischl, H. Tschofenig, E. Rescorla, "Cadre pour l'établissement d'un contexte de sécurité pour le protocole sécurisé de transport en temps réel (SRTP) utilisant la sécurité de la couche de transport de datagrammes (DTLS)", DOI 10.17487/RFC5763, mai 2010. (P. S. ; MàJ par [RFC7983](#))

- [RFC5767] M. Munakata, S. Schubert, T. Ohba, "Mécanisme de confidentialité piloté par l'agent d'utilisateur pour SIP", avril 2010. (*Information*)
- [RFC5768] J. Rosenberg, "Indication de la prise en charge de l'établissement de connexité interactive (ICE) dans le protocole d'établissement de session (SIP)", avril 2010. (*P. S.*)
- [RFC5839] A. Niemi, D. Willis, "Extension aux événements du protocole d'initialisation de session (SIP) pour la notification d'événement conditionnel", mai 2010. (*P. S.*)
- [RFC5876] J. Elwell, "Mise à jour de l'identité affirmée dans le protocole d'initialisation de session (SIP)", avril 2010. (*MàJ RFC3325*) (*Information*)
- [RFC5898] F. Andreasen, G. Camarillo, D. Oran, D. Wing, "Préconditions de connexité pour les flux de support du protocole de description de session (SDP)", juillet 2010. (*P. S.*)
- [RFC5923] V. Gurbani, R. Mahy, etc., "Réutilisation de connexion dans SIP", juin 2010. (*PS*)
- [RFC5939] F. Andreasen, "Négociation de capacités dans le protocole de description de session (SDP)", septembre 2010. (*P.S.*)
- [RFC5954] V. Gurbani, B. Carpenter, B. Tate, "Correction essentielle pour la comparaison d'ABNF et d'URI IPv6 dans la RFC3261", août 2010. (*MàJ RFC3261*) (*P.S.*)
- [RFC6035] A. Pendleton, A. Clark, A. Johnston, H. Sinnreich, "Paquetage d'événements du protocole d'initialisation de session pour le rapport de la qualité de la voix", novembre 2010. (*P.S.*)
- [RFC6072] C. Jennings, J. Fischl, éditeurs, "Service de gestion de certificats pour le protocole d'initialisation de session (SIP)", février 2011. (*P. S.*)
- [RFC6080] D. Petrie, S. Channabasappa, éd.. "Cadre pour la livraison de profil d'agent d'utilisateur du protocole d'initialisation de session", mars 2011. (*P. S.*)
- [RFC6157] G. Camarillo, K. El Malki, V. Gurbani, "Transition à IPv6 dans le protocole d'initialisation de session (SIP)", avril 2011. (*MàJ la RFC3264*) (*P.S.*)
- [RFC6442] J. Polk, B. Rosen, J. Peterson, "Véhicule de localisation pour le protocole d'initialisation de session", décembre 2011. (*P.S.* ; *MàJ par RFC7852, RFC8262, RFC8787*)
- [RFC6443] B. Rosen, H. Schulzrinne, J. Polk, A. Newton, "Cadre pour les appels d'urgence qui utilisent l'Internet multi supports", décembre 2011. (*Information*)
- [RFC6794] V. Hilt, G. Camarillo et J. Rosenberg, "Cadre pour les politiques de session du protocole d'initialisation de session (SIP)", décembre 2012.
- [RFC6795] V. Hilt et G. Camarillo, "Paquetage d'événement du protocole d'initialisation de session (SIP) pour les politiques spécifiques de session", décembre 2012.
- [RFC6871] R. Gilman, R. Even, F. Andreasen, "Négociation des capacités du support pour le protocole de description de session (SDP)", février 2013. (*MàJ RFC5939*) (*P.S.*)
- [RFC6914] J. Rosenberg, "SIMPLE rendu simple : vue d'ensemble des spécifications de l'IETF pour la messagerie instantanée et la présence avec le protocole d'initialisation de session (SIP)", avril 2013. (*Information*)
- [SAML] Tschofenig, H., Hodges, J., Peterson, J., Polk, J., et D. Sicker, "SIP SAML Profile and Binding", Travail en cours, novembre 2008.

## Adresse de l'auteur

Jonathan Rosenberg

Cisco  
Iselin, NJ  
US  
mél : [jdrosen@cisco.com](mailto:jdrosen@cisco.com)  
URI : <http://www.jdrosen.net>

## **Déclaration complète de droits de reproduction**

Copyright (C) The IETF Trust (2009).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs 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 viole 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](mailto:ietf-ipr@ietf.org).