Groupe de travail Réseau
Request for Comments : 5630
RFC mises à jour : 3261, 3608
Catégorie : Sur la voie de la normalisation

F. Audet, Skype Labs
octobre 2009

Traduction Claude Brière de l'Isle

Utilisation du schéma d'URI SIPS dans le protocole d'initialisation de session (SIP)

Résumé
Le présent document apporte des précisions et des lignes directrices concernant l'utilisation du schéma d'URI SIPS dans le protocole l'initialisation de session (SIP). Il fait aussi des changements normatifs à SIP.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5630

Table des matières

1. Introduction

La signification et l'usage du schéma d'URI SIPS et de la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC5246] sont sous spécifiés dans SIP [RFC3261] et ont été une source de confusion pour les mises en œuvre.

Le présent document fournit des éclaircissements et des lignes directrices concernant l'utilisation du schéma d'URI SIPS dans le protocole d'initialisation de session (SIP, *Session Initiation Protocol*). Il fait aussi des changements normatifs à SIP (incluant la [RFC3261] et la [RFC3608].

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 le BCP 14, [RFC2119].

3. Fondements

3.1 Modèles pour l'utilisation de TLS dans SIP

Cette section décrit brièvement l'usage de TLS dans SIP.

3.1.1 Certificat fourni par le serveur

Dans ce modèle, seul le serveur TLS fournit un certificat durant la prise de contact TLS. Ceci est applicable seulement entre un agent d'utilisateur (UA, *user agent*) et un mandataire, où l'UA est le client TLS et le mandataire est le serveur TLS, et donc l'UA utilise TLS pour authentifier le mandataire mais le mandataire n'utilise pas TLS pour authentifier l'UA. Si le mandataire a besoin d'authentifier l'UA, cela peut être réalisé par l'authentification par résumé HTTP de SIP. Cette directionnalité implique que la connexion TLS doit toujours être établie par l'UA (par exemple, durant la phase d'enregistrement). Comme SIP permet les demandes dans les deux directions (par exemple, un appel entrant) l'UA est supposé garder cette connexion TLS en vie, et cette connexion est supposée être réutilisée pour les demandes entrantes et sortantes.

Cette solution d'avoir l'UA qui toujours initie et garde en vie la connexion résout aussi le problème de la traduction d'adresse réseau (NAT, *Network Address Translation*) et du pare-feu car elle assure que les résponses et les demandes ultérieures vont toujours être livrables sur la connexion existante.

La [RFC5626] fournit le mécanisme pour initier et maintenir les connexions sortantes d'une façon interopérable standard.

3.1.2 Authentification mutuelle

Dans ce modèle, le client TLS et le serveur TLS fournissent tous deux un certificat dans la phase de prise de contact TLS. Quand c'est utilisé entre un UA et un mandataire (ou entre deux UA) cela implique qu'un UA est en possession d'un certificat. Quand il envoie une demande SIP et qu'il n'y a pas déjà en place de connexion TLS convenable, un client d'agent d'utilisateur (UAC, *user agent client*) prend le rôle de client TLS dans l'établissement d'une nouvelle connexion TLS. Quand il établit une connexion TLS pour la réception d'une demande SIP, un serveur d'agent d'utilisateur (UAS, *user agent server*) prend le rôle de serveur TLS. Parce que dans SIP un UA ou un mandataire agit comme UAC et comme UAS selon qu'il envoie ou reçoit les demandes, la nature symétrique du TLS mutuel est très pratique. Cela permet que les connexions TLS soient établies ou supprimées à volonté et ne reposent pas sur le maintien en vie de la connexion TLS pour d'autres demandes.

Cependant, il y a quelques limitations significatives.

La première limitation évidente n'est pas avec l'authentification mutuelle en soi mais avec le modèle où la connexion TLS sous-jacente peut être établie par l'un où l'autre côté, de façon interchangeable, ce qui n'est pas possible dans de nombreux environnements. Par exemples, les NAT et les pare-feu vont souvent permettre que les connexions TCP soient établies dans une seule direction. Cela inclut la plupart des déploiements résidentiels de SIP, par exemple. L'authentification mutuelle peut être utilisée dans ces environnements, mais seulement si la connexion est toujours démarrée par le même côté, par exemple, en utilisant la [RFC5626] comme décrit au paragraphe 3.1.1. Devoir s'appuyer sur la [RFC5626] dans ce cas nie beaucoup des avantages de l'authentification mutuelle.

La seconde limitation significative est que l'authentification mutuelle exige que les deux côtés échangent un certificat. Cela s'est révélé impraticable dans de nombreux environnements, en particulier pour les UA SIP, à cause des difficultés de l'établissement d'une infrastructure de certificats pour une large population d'utilisateurs.

Pour ces raisons, l'authentification mutuelle est surtout utilisée dans les communications de serveur à serveur (par exemple, entre mandataires SIP, ou entre mandataires et passerelles ou serveurs de supports) et dans des environnements où l'utilisation de certificats des deux côtés est possible (par exemple, des appareils de haute sécurité utilisés au sein d'une entreprise).

3.1.3 Utilisation de TLS avec SIP au lieu de SIPS

Parce qu'un URI SIPS implique que les demandes envoyées à la ressource identifiée par lui vont être envoyées sur chaque bond SIP sur TLS, les URI SIPS ne conviennent pas pour "TLS au mieux" : elles conviennent seulement pour les demandes "TLS-seul". Ceci est reconnu au paragraphe 26.2.2 de la [RFC3261].

Les utilisateurs qui distribuent un URI SIPS comme adresse d'enregistrement peuvent choisir d'opérer sur des appareils qui refusent les demandes sur des transports non sûrs.

Si on veut utiliser "TLS au mieux" pour SIP, on a juste besoin d'utiliser un URI SIP, et d'envoyer la demande sur TLS.

Utiliser SIP sur TLS est très simple. Un UA ouvre une connexion TLS et utilise des URI SIP au lieu d'URI SIPS pour tous les champs d'en-tête dans le message SIP (From, To, Request-URI, Contact, Route, etc.). Quand TLS est utilisé, le champ d'en-tête Via indique TLS.

Le paragraphe 26.3.2.1 de la [RFC3261] déclare : "Quand un UA vient en ligne et s'enregistre dans son domaine administratif local, il DEVRAIT établir une connexion TLS avec son registraire (...). Une fois que l'enregistrement a été accepté par le registraire, l'UA DEVRAIT laisser cette connexion TLS ouverte pourvu que le registraire agisse aussi comme serveur mandataire auquel les demandes sont envoyées pour les utilisateurs dans ce domaine administratif. La connexion TLS existante va être réutilisée pour livrer les demandes entrantes à l'UA qui vient de terminer l'enregistrement."

La [RFC5626] décrit comment établir et maintenir une connexion TLS dans des environnements où elle peut seulement être initiée par l'UA.

De même, les mandataires peuvent transmettre les demandes en utilisant TLS si ils peuvent ouvrir une connexion TLS, même si l'ensemble de chemins utilise des URI SIP au lieu d'URI SIPS. Les mandataires peuvent insérer des champs d'en-tête Record-Route utilisant des URI SIP même si ils utilisent le transport TLS. Le paragraphe 26.3.2.2 de la [RFC3261] explique comment les demandes inter domaines peuvent utiliser TLS.

Certains agents d'utilisateur, serveurs de redirection, et mandataires pourraient avoir des politiques locales qui appliquent TLS sur toutes les connexions, indépendamment de si SIPS est utilisé ou non.

3.1.4 Usage du paramètre d'URI transport=tls et du paramètre TLS Via

Le paragraphe 26.2.2de la [RFC3261] déconseillait le paramètre de transport d'URI "transport=tls" dans les URI SIPS ou SIP :

"Noter que dans le schéma d'URI SIPS, le transport est indépendant de TLS, et donc "sips:alice@atlanta.com;transport=TCP" et "sips:alice@atlanta.com;transport=sctp" sont tous deux valides (bien qu'on note que UDP n'est pas un transport valide pour SIPS). L'utilisation de "transport=tls" a par conséquent été déconseillée, en partie parce que il était spécifique d'un seul bond de la demande. Ceci est un changement par rapport à la RFC 2543."

Le paramètre "tls" n'a pas été éliminé de l'ABNF dans la [RFC3261], Section 25, car le paramètre doit rester dans l'ABNF pour la rétro compatibilité afin que les analyseurs soient capables de traiter correctement le paramètre. Le paramètre

transport=tls n'a jamais été défini dans une RFC, mais seulement dans certains projets Internet entre les [RFC2543] et [RFC3261].

La présente spécification n'utilise pas le paramètre transport=tls.

La réinstallation du paramètre transport=tls, ou d'un mécanisme de remplacement pour indiquer l'utilisation de TLS sur un seul bond dans un URI, sort du domiane d'application de la présente spécification.

Pour les champs d'en-tête Via, les protocoles de transport suivants sont définis dans la [RFC3261] : "UDP", "TCP", "TLS", "SCTP", et dans la [RFC4168] : "TLS-SCTP".

3.2 Détection de la sécurité bond par bond

La présence d'un URI de demande SIPS n'indique pas nécessairement que la demande a été envoyée de façon sûre sur chaque bond. Donc comment un UAS sait-il si SIPS a été utilisé pour le chemin entier de la demande pour sécuriser la demande de bout en bout ? Effectivement, l'UAS ne peut pas en être sûr. Cependant, le paragraphe 26.4.4 de la [RFC3261] recommande comment un UAS peut faire des vérifications pour valider la sécurité. De plus, le champ d'en-tête History-Info [RFC4244] pourrait être inspecté pour détecter un reciblage de SIP et SIPS. Le reciblage de SIP à SIPS par un mandataire est un problème parce que il peut donner au receveur de la demande l'impression que la demande a été livrée de façon sûre sur chaque bond, alors qu'en fait, elle ne l'a pas été.

Pour développer, toutes les vérifications peuvent être circonvenues par tout mandataire ou agent d'utilisateur de boucle locale (B2BUA, *back-to-back user agent*) sur le chemin qui ne suit pas les règles et recommandations de la présente spécification et de la [RFC3261].

Les mandataires peuvent avoir leur propre politique concernant l'acheminement des demandes aux URI SIP ou SIPS. Par exemple, certains mandataires dans certains environnements peuvent être configurés à acheminer seulement des URI SIPS. Certains mandataires peuvent être configurés à détecter des non conformités et rejeter les demandes non sûres. Par exemple, les mandataires pourraient inspecter les URI de demande, les champs d'en-tête Path, Record-Route, To, From, Contact, et Via pour appliquer SIPS.

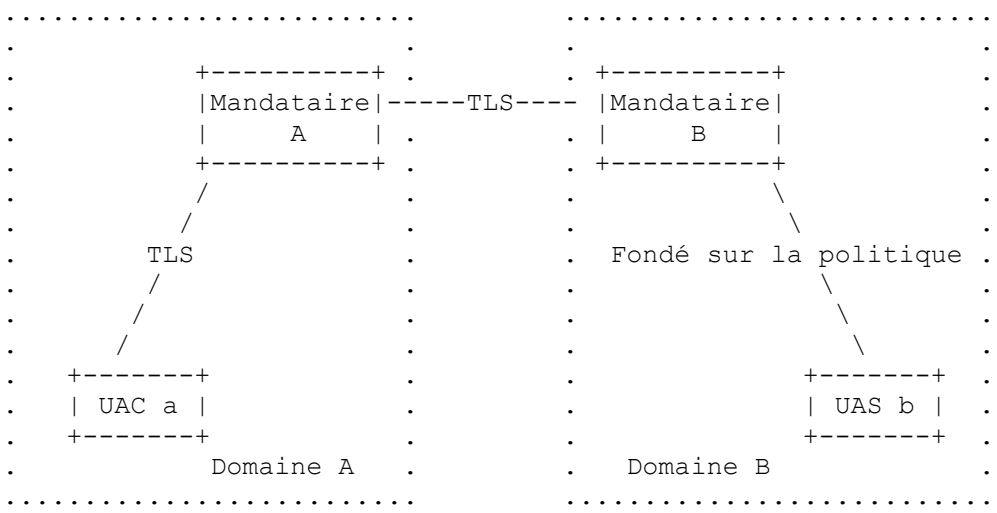
Le paragraphe 26.4.4 de la [RFC3261] explique que S/MIME peut aussi être utilisé par l'UAC d'origine pour s'assurer que la forme originale du champ d'en-tête To est portée de bout en bout. Bien que non spécifiquement mentionnée au paragraphe 26.4.4 de la [RFC3261], ceci est destiné à impliquer que la [RFC3893] va être utilisée pour "tunneler" les champs d'en-tête importants (comme To et From) dans un corps S/MIME chiffré et signé, dupliquant les informations du message SIP, et permettant à l'UAS de valider le contenu de ces champs d'en-tête importants. Bien que cette approche soit certainement légale, une approche préférable est d'utiliser le mécanisme Identity de SIP défini dans la [RFC4474]. Le mécanisme Identity de SIP crée un résumé d'identité signé, qui inclut, entre autres choses, l'adresse d'enregistrement (AOR, *Address of Record*) de l'envoyeur (d'après le champ d'en-tête From) et l'AOR de la cible originale (d'après le champ d'en-tête To).

3.3 Problèmes de la signification de SIPS dans la RFC 3261

Le paragraphe 19.1 de la [RFC3261] décrit un URI SIPS comme suit : "Un URI SIPS spécifie que la ressource va être contactée en toute sécurité. Cela signifie que, en particulier, TLS est à utiliser entre l'UAC et le domaine qui possède l'URI. À partir de là, des communications sûres sont utilisées pour atteindre l'utilisateur, mais le mécanisme spécifique de sécurité dépend de la politique du domaine."

Le paragraphe 26.2.2 le répète, à l'égard des URI de demande : "Quand il est utilisé comme Request-URI d'une demande, le schéma SIPS signifie que chaque bond sur lequel la demande est transmise, jusqu'à ce que la demande atteigne l'entité SIP responsable de la portion de domaine de l'URI de demande, doit être sécurisé avec TLS ; une fois qu'il atteint le domaine en question, il est traité en accord avec la politique locale de sécurité et d'acheminement, éventuellement en utilisant TLS pour un dernier bond jusqu'à un UAS. Quand il est utilisé par le générateur d'une demande (comme ce serait le cas si il avait employé un URI SIPS comme adresse d'enregistrement de la cible) SIPS impose que le chemin entier de la demande jusqu'au domaine cible soit sécurisé."

Prenons le trapézoïde SIP classique pour explique la signification d'un URI sips:b@B. Au lieu d'utiliser des noms de domaine réels comme exemple.com et exemple.net, des noms logiques comme "A" et "B" sont utilisés, pour être clair.



Trapézoïde SIP avec exception du dernier bond

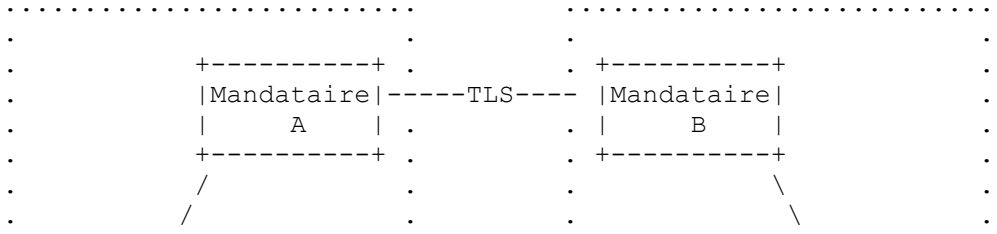
Selon la [RFC3261], si a@A envoie une demande à sips:b@B, ce qui suit s'applique :
- o TLS est exigé entre l'UA a@A et le mandataire A
- o TLS est exigé entre le mandataire A et le mandataire B
- o TLS est exigé entre le mandataire B et l'UA b@B, selon la politique locale.

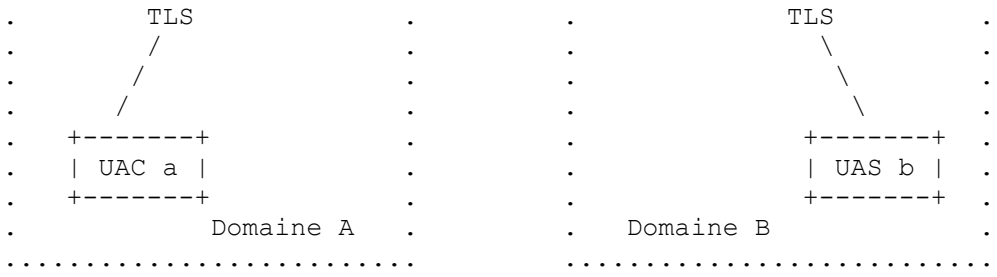
On peut alors se demander pourquoi TLS est obligatoire entre l'UA a@A et le mandataire A mais pas entre le mandataire B et l'UA b@B. La principale raison est que la [RFC3261] a été écrite avant la [RFC5626]. À l'époque, il a été reconnu que dans de nombreux déploiements pratiques, le mandataire B pourrait n'être pas capable d'établir une connexion TLS avec l'UA b parce que seul le mandataire B aurait un certificat à fournir et l'UA b n'en aurait pas. Comme l'UA b va être le serveur TLS, il ne va alors pas être capable d'accepter la connexion TLS entrante. La conséquence est qu'un UAS b conforme à la [RFC3261], bien qu'il pourrait n'avoir pas besoin de prendre en charge TLS pour les demandes entrantes, va néanmoins devoir prendre en charge TLS pour les demandes sortantes parce qu'il prend alors le rôle d'UAC. Au contraire de ce que beaucoup croient à tort, l'exception du dernier bond n'a pas été créée pour permettre d'utiliser un URI SIPS pour s'adresser à un UAS qui ne prend pas en charge TLS : l'exception du dernier bond était une tentative pour permettre aux demandes entrantes de n'être pas transportées sur TLS quand un URI SIPS est utilisé, et elle ne s'applique pas aux demandes sortantes. La raison de cela a été un peu perdue de vue, et depuis lors, la [RFC5626] a fourni une solution plus satisfaisante à ce problème. La [RFC5626] résout aussi le problème que si l'UA b est derrière un NAT ou un pare-feu, le mandataire B ne va même pas être capable d'établir une session TCP en premier lieu.

De plus, si on considère le problème de l'utilisation de SIPS dans un dialogue, si a@A envoie une demande à b@B en utilisant un URI de demande SIPS, alors, selon le paragraphe 8.1.1.8 de la [RFC3261] "le champ d'en-tête Contact DOIT contenir aussi un URI SIPS". Cela signifie que b@B, lors de l'envoi d'une nouvelle demande au sein du dialogue (par exemple, un BYE ou re-INVITE) va devoir utiliser un URI SIPS. Si il n'y a pas d'entrée Record-Route, ou si la dernière entrée de Record-Route consiste en un URI SIPS, cela implique que b@B est supposé comprendre SIPS en premier lieu, et qu'il est exigé qu'il prenne aussi en charge TLS. Si la dernière entrée de Record-Route est cependant un URI SIP, alors b va être capable d'envoyer des demandes sans utiliser TLS (mais b va quand même devoir être capable de traiter les schémas SIPS quand il analyse le message). Dans l'un et l'autre cas, l'URI de demande dans la demande de b@B à B va être un URI SIPS.

4. Vue d'ensemble du fonctionnement

À cause de tous les problèmes décrits au paragraphe 3.3, la présente spécification déconseille l'exception du dernier bond lors de la transmission d'une demande au dernier bond (voir le paragraphe 5.3). Cela va assurer que TLS est utilisé sur tous les bonds sur tout le chemin jusqu'à la cible distante.





Trapézoïde SIP sans exception de dernier bond

Le schéma SIPS implique une confiance transitive. Évidemment, il n'y a rien qui empêche les mandataires de mentir (voir le paragraphe 26.4.4 de la [RFC3261]). Bien que SIPS soit utile pour demander qu'une ressource soit contactée de façon sécurisée, il n'est pas utile comme indication qu'une ressource a en fait été contactée de façon sûre. Donc, il n'est pas approprié de déduire que parce que une demande entrante a un URi de demande (ou même un champ d'en-tête To) contenant un URI SIPS, cela garantit nécessairement que la demande a été bien transmise de façon sûre sur chaque bond. Certains ont été tentés de croire que le schéma SIPS était équivalent à un schéma HTTPS en ce sens qu'on pourrait fournir une indication visuelle à un utilisateur (par exemple, une image de cadenas) que la session est sécurisée. Ce n'est évidemment pas le cas, et donc la signification d'un URI SIPS ne doit pas être surévaluée. Il n'y a actuellement pas de mécanisme pour fournir une indication de la sécurité de bout en bout pour SIP. D'autres mécanismes peuvent fournir une indication plus concrète d'un certain niveau de sécurité. Par exemple, SIP Identity [RFC4474] fournit un mécanisme d'identité authentifiée et un mécanisme de protection de l'intégrité de domaine à domaine.

Certains se sont demandé pourquoi SIPS est utile dans un environnement mondial ouvert comme l'Internet, si (quand il est utilisé dans un URI de demande) il n'est pas une garantie absolue que la demande va en fait être livrée sur TLS sur chaque bond ? Pourquoi SIPS est il différent de juste utiliser le transport TLS avec SIP ? La différence est que utiliser un URI SIPS dans un URI de demande signifie que si on donne pour instruction au réseau d'utiliser TLS sur chaque bond et si il n'est pas possible de rejeter la demande, la demande va plutôt échouer que d'être livrée sans TLS. Juste utiliser TLS avec un URI de demande SIP au lieu d'un URI de demande SIPS implique un service "au mieux" : la demande peut mais ne va pas nécessairement être livrée sur TLS à chaque bond.

Une autre question courante est pourquoi n'avoir pas une étiquette d'option Proxy-Require et Require qui force l'utilisation de TLS ? La réponse est que cela serait seulement fonctionnellement équivalent à utiliser SIPS dans un URI de demande. Les URI SIPS peuvent cependant être utilisés dans de nombreux autres champs d'en-tête : dans Contact pour l'enregistrement, Contact dans les demandes de création de dialogue, Route, Record-Route, Path, From, To, Refer-To, Referred-By, etc. Les URI SIPS peuvent aussi être utilisés dans un format utilisable par l'homme (par exemple, des cartes professionnelles, une interface d'utilisateur). Les URI SIPS peuvent même être utilisés dans d'autres protocoles ou formats de document qui permettent d'inclure des URI SIPS (par exemple, HTML).

Le présent document spécifie que SIPS signifie que la ressource SIP désignée par URI SIPS cible est à contacter de façon sûre, en utilisant TLS à chaque bond entre l'UAC et l'UAS distant (par opposition à seulement jusqu'au mandataire responsable du domaine cible de l'URI de demande). Il sort du domaine d'application du présent document de spécifier ce qui arrive quand un URI SIPS identifie une ressource d'UAS qui "se transpose" en dehors du réseau SIP, par exemple, sur d'autres réseaux tels que le réseau téléphonique public commuté (RTPC).

4.1 Acheminement

Les URI SIP et SIPS qui sont identiques à part le schéma lui-même (par exemple, sip:alice@exemple.com et sips:alice@exemple.com) se réfèrent à la même ressource. Cette exigence est implicite dans la [RFC3261], paragraphe 19.1, qui déclare que "toute ressource décrite par un URI SIP peut être "promue' en URI SIPS juste en changeant le schéma, si c'est désiré pour communiquer de façon sûre avec cette ressource". Cela ne signifie pas que l'URI SIPS va nécessairement être accessible, en particulier, si le mandataire ne peut pas établir une connexion sûre avec un client ou un autre mandataire. Cela ne suggère pas que les mandataires vont arbitrairement "promouvoir" les URI SIP en URI SIPS quand ils transmettent une demande (voir le paragraphe 5.3). Cela signifie plutôt que quand une ressource est adressable avec SIP, elle va aussi être adressable avec SIPS.

Par exemple, considérons le cas d'un UA qui s'est enregistré avec un champ d'en-tête Contact SIPS. Si un UAC adresse plus tard une demande en utilisant un URI de demande SIP, le mandataire va transmette la demande adressée à un URI de demande SIP à l'UAS, comme illustré par le message F13 aux paragraphes 6.3 et 6.4. Le mandataire transmet la demande à l'UA en utilisant un URI de demande SIP et non l'URI de demande SIPS utilisé dans l'enregistrement. Le mandataire fait cela en remplaçant le schéma SIPS qui était utilisé dans le lien de champ d'en-tête Contact enregistré par un schéma SIP tout en laissant le reste de l'URI comme il est, et ensuite en utilisant ce nouvel URI comme URI de demande. Si le mandataire n'avait pas fait cela, et utilisé à la place un URI de demande SIPS, alors la réponse (par exemple, un 200 à un

INVITE) aurait inclus un champ d'en-tête Contact SIPS. Ce champ d'en-tête Contact SIPS aurait alors forcé les autres UA à utiliser un champ d'en-tête Contact SIPS dans toute demande de mi-dialogue, incluant le ACK (ce qui ne serait pas possible si l'UA ne prend pas en charge SIPS).

La présente spécification rend obligatoire que quand un mandataire transmet une demande, une ressource décrite par un URI de demande SIPS ne peut pas être "dégradée" en URI SIP en changeant le schéma, ou en envoyant la demande associée sur une liaison non sûre. Si une demande doit être rejetée parce que autrement elle serait "dégradée", la demande devrait être rejetée avec une réponse 480 (Temporairement indisponible) (éventuellement avec un en-tête Warning avec le code d'avertissement 380 "SIPS non permis"). De même, la présente spécification rend obligatoire que quand un mandataire transmet une demande, une ressource décrite par un URI de demande SIP ne peut pas être "promue" en un URI SIPS en changeant le schéma (autrement ce serait une "promotion" seulement à partir de ce bond plutôt que sur tous les bonds, et tromperait donc l'UAS). Si une demande doit être rejetée parce que autrement elle serait une "promotion" trompeuse, la demande devrait être rejetée avec une réponse 480 (Temporairement indisponible) (éventuellement avec un en-tête Warning avec le code d'avertissement 381 "SIPS exigé"). Voir les détails au paragraphe 5.3.

Par exemple, les AOR sip:bob@exemple.com et sips:bob@exemple.com se réfèrent au même utilisateur "Bob" dans le domaine "exemple.com" : le premier URI est la version SIP, et le second est la version SIPS. Du point de vue de l'acheminement, les demandes à sip:bob@exemple.com ou sips:bob@exemple.com sont traitées de la même manière. Quand Bob s'enregistre, il ne se soucie donc pas vraiment d'utiliser une AOR SIP ou SIPS, car les deux se réfèrent au même utilisateur. À première vue, le paragraphe 19.1.4 de la [RFC3261] semble contredire cette idée en déclarant qu'un URI SIP et un URI SIPS ne sont jamais équivalents. Précisément, cela dit qu'ils ne sont jamais équivalents pour les besoins de la comparaison des liens dans les URI de champ d'en-tête Contact dans les demandes REGISTER. Le point clé est que cette déclaration s'applique aux liens de champ d'en-tête Contact dans un enregistrement : c'est l'association du champ d'en-tête Contact avec l'AOR qui va déterminer si l'utilisateur est ou non accessible avec un URI SIPS.

Examinons cet exemple : si Bob (AOR bob@exemple.com) s'enregistre avec un champ d'en-tête Contact SIPS (par exemple, sips:bob@bobphone.exemple.com) le registraire et le service de localisation savent alors que Bob est accessible à sips:bob@bobphone.exemple.com et à sip:bob@bobphone.exemple.com.

Si une demande est envoyée à l'AOR sips:bob@exemple.com, le mandataire de Bob va l'acheminer à Bob à l'URI de demande sips:bob@bobphone.exemple.com. Si une demande est envoyée à l'AOR sip:bob@exemple.com, le mandataire de Bob va l'acheminer à Bob à l'URI de demande sip:bob@bobphone.exemple.com.

Si Bob veut s'assurer que chaque demande qui lui est livrée va toujours être transportée sur TLS, Bob peut utiliser la [RFC5626] quand il s'enregistre.

Cependant, si Bob s'était enregistré avec un champ d'en-tête Contact SIP au lieu d'un champ d'en-tête Contact SIPS (par exemple, sip:bob@bobphone.exemple.com) alors une demande à l'AOR sips:bob@exemple.com n'aurait pas été acheminée à Bob, parce qu'il n'y a pas de champ d'en-tête Contact SIPS pour Bob, et la "dégradation" de SIPS à SIP n'est pas permise.

Voir à la Section 6 les illustrations de flux d'appels.

5. Exigences normatives

Cette section décrit toutes les exigences normatives définie par cette spécification.

5.1 Comportement général d'agent d'utilisateur

5.1.1 Comportement de l'UAC

Quand on lui présente un URI SIPS, un UAC NE DOIT PAS le changer en un URI SIP. Par exemple, si une entrée de répertoire inclut une AOR SIPS, l'UAC n'est pas supposé envoyer des demandes à cette AOR en utilisant un URI de demande SIP. De même, si un utilisateur lit une carte professionnelle avec un URI SIPS, il n'est pas possible d'en déduire un URI SIP. Si une réponse 3XX inclut un champ d'en-tête Contact SIPS, l'UAC ne le remplace pas par un URI de demande SIP (par exemple, en remplaçant le schéma SIPS par un schéma SIP) quand il envoie une demande par suite de la redirection.

Comme imposé par le paragraphe 8.1.1.8 de la [RFC3261], dans une demande, "si l'URI de demande ou la valeur supérieure du champ d'en-tête Route contient un URI SIPS, le champ d'en-tête Contact DOIT contenir aussi un URI SIPS".

À réception d'une réponse 416 ou 480 (Temporairement indisponible) avec un en-tête Warning portant un code d'avertissement de 380 "SIPS Non permis", un UAC NE DOIT PAS retenter la demande en remplaçant automatiquement le

schéma SIPS par un schéma SIP comme décrit au paragraphe 8.1.3.5 de la [RFC3261], car cela serait une vulnérabilité de la sécurité. Si l'UAC retente l'appel avec un URI SIP, l'UAC DEVRAIT obtenir une confirmation de l'utilisateur pour autoriser la réinitialisation de la session avec un URI de demande SIP au lieu d'un URI de demande SIPS.

Quand l'ensemble de chemins n'est pas vide (par exemple, quand un chemin de service [RFC3608] est retourné par le registraire) il est de la responsabilité de l'UAC d'utiliser un champ d'en-tête Route consistant en tous les URI SIPS quand il utilise un URI de demande SIPS. Précisément, si l'ensemble de chemins comporte un URI SIP, l'UAC DOIT changer les URI SIP en URI SIPS simplement en changeant le schéma de "sip" en "sips" avant d'envoyer la demande. Cela permet de configurer ou découvrir un chemin de service avec tous les URI SIP et permet d'envoyer des demandes à la fois aux URI SIP et SIPS.

Quand l'UAC utilise un URI de demande SIP, si l'ensemble de chemins n'est pas vide et si l'entrée de sommet du champ d'en-tête Route est un URI SIPS avec le paramètre lr, l'UAC DOIT envoyer la demande sur TLS (en utilisant un URI de demande SIP). Si l'ensemble de chemins n'est pas vide et si l'entrée du champ d'en-tête Route est un URI SIPS sans le paramètre lr, l'UAC DOIT envoyer la demande sur TLS en utilisant un URI de demande SIPS correspondant à l'entrée supérieure de l'ensemble de chemins.

Pour souligner ce qui est déjà défini dans la [RFC3261], les UA NE DOIVENT PAS utiliser le paramètre "transport=tls".

5.1.1.1 Enregistrement

L'UAC enregistre les champs d'en-tête Contacts à une AOR SIPS ou SIP.

Si un UA souhaite être accessible avec un URI SIPS, l'UA DOIT s'enregistrer avec un champ d'en-tête Contact SIPS. Les demandes adressées à cette AOR d'UA en utilisant un URI de demande SIP ou SIPS vont être acheminées à cet UA. Cela inclut les UA qui prennent en charge à la fois SIP et SIPS. La présente spécification ne fournit aucun mécanisme fondé sur SIP pour qu'un UA provisionne son mandataire à seulement transmettre des demandes en utilisant un URI de demande SIPS. Un mécanisme non SIP comme une interface de la Toile pourrait être utilisé pour provisionner une telle préférence. Un mécanisme SIP pour provisionner une telle préférence sort du domaine d'application de cette spécification.

Si un UA ne souhaite pas être joint avec un URI SIPS, il DOIT s'enregistrer avec un champ d'en-tête Contact SIP.

Comme s'enregistrer avec un champ d'en-tête Contact SIPS implique un lien à la fois au Contact SIPS et au Contact SIP correspondant à l'AOR, un UA NE DOIT PAS inclure les deux versions de SIPS et de SIP du même champ d'en-tête Contact dans une demande REGISTER ; l'UA DOIT seulement utiliser la version SIPS dans ce cas. De même, un UA NE DEVRAIT PAS enregistrer à la fois un champ d'en-tête Contact SIP et un champ d'en-tête Contact SIPS dans des enregistrements séparés car le champ d'en-tête Contact SIP serait superflu. Si il le fait, le second enregistrement remplace le premier (par exemple, un UA pourrait s'enregistrer d'abord avec un champ d'en-tête Contact SIP, ce qui signifie qu'il ne prend pas SIPS en charge, et plus tard s'enregistrer avec un champ d'en-tête Contact SIPS, signifiant qu'il prend maintenant en charge SIPS). De même, si un UA s'enregistre d'abord avec un champ d'en-tête Contact SIPS et plus tard s'enregistre avec un champ d'en-tête Contact SIP, ce champ d'en-tête Contact SIP remplace le champ d'en-tête Contact SIPS.

La [RFC5626] peut être utilisée par un UA si il veut s'assurer qu'aucune demande ne lui est livrée sans utiliser la connexion TLS qu'il a utilisé quand s'est enregistré.

Si tous les champs d'en-tête Contact dans une demande REGISTER sont SIPS, l'UAC DOIT utiliser les AOR SIPS dans les champs d'en-tête From et To dans la demande REGISTER. Si au moins un des champs d'en-tête Contact n'est pas SIPS (par exemple, sip, mailto, tel, http, https) l'UAC DOIT utiliser des AOR SIP dans les champs d'en-tête From et To dans la demande REGISTER.

Pour souligner ce qui est déjà défini dans la [RFC3261], les UAC NE DOIVENT PAS utiliser le paramètre "transport=tls".

5.1.1.2 SIPS dans un dialogue

Si l'URI de demande dans une demande qui initie un dialogue est un URI SIP, l'UAC doit alors faire attention à ce qu'il utilise dans le champ d'en-tête Contact (au cas où Record-Route n'est pas utilisé pour ce bond). Si le champ d'en-tête Contact était un URI SIPS, cela voudrait dire que l'UAS va seulement accepter des demandes de mi-dialogue envoyées sur un transport sûr à chaque bond. Comme l'URI de demande dans ce cas est un URI SIP, il est possible que l'UA qui envoie une demande à cet URI ne soit pas capable d'envoyer des demandes à des URI SIPS. Si le champ d'en-tête Route supérieur ne contient pas d'URI SIPS, l'UAC DOIT utiliser un URI SIP dans le champ d'en-tête Contact, même si la demande est envoyée sur un transport sûr (par exemple, le premier bond pourrait réutiliser une connexion TLS avec le mandataire comme ce serait le cas avec la [RFC5626]).

Quand un rafraîchissement de cible se produit au sein d'un dialogue (par exemple, une demande re-INVITE, ou UPDATE) l'UAC DOIT inclure un champ d'en-tête Contact avec un URI SIPS si la demande d'origine utilisait un URI de demande SIPS.

5.1.1.3 Dialogues et transactions dérivés

Les sessions, dialogues, et transactions peuvent être "dérivés" d'existants. Un bon exemple d'un dialogue dérivé est celui qui a été établi par suite de l'utilisation de la méthode REFER [RFC3515].

Le principe général est que les dialogues et transactions dérivés ne peuvent pas résulter en une dégradation effective de SIPS en SIP, sans l'autorisation explicite des entités impliquées.

Par exemple, quand une demande REFER est utilisée pour effectuer un transfert d'appel, il en résulte la fin du dialogue existant et la création d'un autre sur la base de l'URI Refer-To. Si ce dialogue initial avait été établi en utilisant SIPS, alors l'UAC NE DOIT PAS en établir un nouveau en utilisant SIP, sauf si il y a une autorisation explicite donnée par le receveur de la demande REFER. Cela pourrait être un avertissement fourni à l'utilisateur. Avoir un tel avertissement pourrait être utile, par exemple, pour une application sûre de service de répertoire, pour avertir un utilisateur qu'une demande peut être acheminée à un UA qui ne prend pas en charge SIPS.

Une demande REFER peut aussi être utilisée pour se référer à des ressources qui ne résultent pas en création de dialogue. En fait, une demande REFER peut être utilisée pour pointer sur des ressources qui sont d'un type différent de celui d'origine (c'est-à-dire, non SIP ou SIPS). Voir au paragraphe 5.2 de la [RFC3515] les considérations sur la sécurité qui s'y rapportent.

D'autres exemples de dialogues et transactions dérivés incluent l'utilisation du contrôle d'appel de tiers [RFC3725], du champ d'en-tête Replaces [RFC3891], et du champ d'en-tête Join [RFC3911]. Là encore, le principe général est que ces mécanismes NE DEVRAIENT PAS résulter en une dégradation effective de SIPS en SIP, sans l'autorisation appropriée.

5.1.1.4 GRUU

Quand un URI d'agent d'utilisateur mondialement acheminable (GRUU, *Globally Routable User Agent URI*) [RFC5627] est alloué à une instance de paire d'ID/AOR, des GRUU SIP et SIPS vont être alloués. Quand un GRUU est obtenu par enregistrement, si le champ d'en-tête Contact dans la demande REGISTER contient un URI SIP, la version SIP du GRUU est retournée. Si le champ d'en-tête Contact dans la demande REGISTER contient un URI SIPS, la version SIPS du GRUU est retournée.

Si le mauvais schéma est reçu dans le GRUU (ce qui serait une erreur du registraire) l'UAC DEVRAIT le traiter comme si le schéma approprié était utilisé (c'est-à-dire, il DEVRAIT remplacer le schéma par le schéma approprié avant d'utiliser le GRUU).

5.1.2 Comportement d'UAS

Quand on lui présente un URI SIPS, un UAS NE DOIT PAS le changer en URI SIP.

Comme exigé par le paragraphe 12.1.1 de la [RFC3261] : "Si la demande qui a initié le dialogue contenait un URI SIPS dans l'URI de demande ou dans la valeur supérieure du champ d'en-tête Record-Route, si il y en avait un, ou dans le champ d'en-tête Contact si il n'y avait pas de champ d'en-tête Record-Route, le champ d'en-tête Contact dans la réponse DOIT être un URI SIPS."

Si un UAS ne souhaite pas être joint avec un URI SIPS mais seulement avec un URI SIP, l'UAS DOIT répondre avec une réponse 480 (Temporairement indisponible). L'UAS DEVRAIT inclure un en-tête Warning avec le code d'avertissement 380 "SIPS Non admis". Le paragraphe 8.2.2.1 de la [RFC3261] déclare que les UAS qui ne prennent pas du tout en charge le schéma d'URI SIPS "DEVRAIENT rejeter la demande avec une réponse 416 (Schéma d'URI non pris en charge)".

Si un UAS souhaite ne pas être contacté avec un URI SIP mais plutôt avec un URI SIPS, il DOIT rejeter une demande d'URI de demande SIP avec une réponse 480 (Temporairement indisponible). L'UAS DEVRAIT inclure un en-tête Warning avec le code d'avertissement 381 "SIPS exigé".

C'est une affaire de politique locale pour un UAS d'accepter les demandes entrantes adressées à un schéma d'URI qui ne correspond pas à ce qui a été utilisé pour l'enregistrement. Par exemple, un UA avec une politique de "toujours SIPS" va s'adresser au registraire en utilisant un URI de demande SIPS sur TLS, va s'enregistrer avec un champ d'en-tête Contact SIPS, et l'UAS va rejeter les demandes qui utilisent le schéma SIP avec une réponse 480 (Temporairement indisponible) avec un en-tête Warning et un code d'avertissement de 381 "SIPS exigé". Un UA avec une politique de "SIPS au mieux" va s'adresser au registraire en utilisant un URI de demande SIPS sur TLS, va s'enregistrer avec un champ d'en-tête Contact

SIPS, et l'UAS va accepter les demandes adressés à un URI de demande SIP ou SIPS. Un UA avec une politique de "Pas de SIPS" va s'adresser au registraire en utilisant un URI de demande SIP, pourrait utiliser TLS ou non, s'enregistrerait avec une AOR SIP et un champ d'en-tête Contact SIP, et l'UAS accepterait les demandes adressées à un URI de demande SIP.

Si un UAS a besoin de rejeter une demande parce que les URI sont utilisés de façon incohérente (par exemple, l'URI de demande est un URI SIPS, mais le champ d'en-tête Contact est un URI SIP) l'UAS DOIT rejeter la demande avec une réponse 400 (Mauvaise demande).

Quand un rafraîchissement de cible se produit au sein d'un dialogue (par exemple, une demande re-INVITE, une demande UPDATE) l'UAS DOIT inclure un champ d'en-tête Contact avec un URI SIPS si la demande d'origine a utilisé un URI de demande SIPS.

Pour souligner ce qui est déjà défini dans la [RFC3261], les UAS NE DOIVENT PAS utiliser le paramètre "transport=tls".

5.2 Comportement du registraire

L'UAC enregistre les champs d'en-tête Contacts à une AOR SIPS ou SIP. Du point de vue de l'acheminement, celle qui est utilisée importe peu pour l'enregistrement car elles identifient la même ressource. Le registraire DOIT considérer que les AOR sont identiques sauf pour celle qui a le schéma SIP et les autres qui ont le schéma SIPS comme étant équivalentes.

Un registraire DOIT accepter un lien à un champ d'en-tête Contact SIPS seulement si tous les URI appropriés sont de schéma SIPS ; autrement, il pourrait y avoir un lien imprévu d'une ressource sûre (SIPS) à une non sûre (SIP). Cela inclut l'URI de demande et les Contacts et tous les champs d'en-tête Path, mais n'inclut pas de champs d'en-tête From et To. Si les URI ne sont pas du schéma SIPS approprié, le registraire DOIT rejeter le REGISTER avec un 400 (Mauvaise demande).

Un registraire peut retourner chemin de service [RFC3608] et imposer des contraintes sur si TLS va être ou non obligatoire sur des bonds spécifiques. Par exemple, si l'entrée supérieure dans le champ d'en-tête Path retourné par le registraire est un URI SIPS, le registraire dit à l'UAC que TLS est à utiliser pour le premier bond, même si l'URI de demande est SIP.

Si un UA s'est enregistré avec un champ d'en-tête Contact SIPS, le registraire qui retourne un chemin de service [RFC3608] DOIT retourner un chemin de service consistant en URI SIP si l'intention du registraire est de permettre d'utiliser à la fois SIP et SIPS dans les demandes envoyées par ce client. Si un UA s'enregistre avec un champ d'en-tête Contact SIPS, le registraire qui retourne un chemin de service DOIT retourner un chemin de service consistant en URI SIPS si l'intention du registraire est de permettre seulement d'utiliser des URI SIPS dans les demandes envoyées par cet UA.

5.2.1 GRUU

Quand un GRUU [RFC5627] est alloué à une instance de paire d'ID/AOR par un enregistrement, le registraire DOIT allouer un GRUU SIP et un GRUU SIPS. Si le champ d'en-tête Contact dans la demande REGISTER contient un URI SIP, le registraire DOIT retourner la version SIP du GRUU. Si le champ d'en-tête Contact dans la demande REGISTER contient un URI SIPS, le registraire DOIT retourner la version SIPS du GRUU.

5.3 Comportement de mandataire

Les mandataires NE DOIVENT PAS utiliser l'exception de dernier bond de la [RFC3261] quand il transmettent ou reciblent une demande au dernier bond. Précisément, quand un mandataire reçoit une demande avec un URI de demande SIPS, le mandataire DOIT seulement transmettre ou recibler la demande à un URI de demande SIPS. Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIP au lieu d'un champ d'en-tête Contact SIPS, le mandataire NE DOIT PAS transmettre la demande à l'URI indiqué dans le champ d'en-tête Contact. Si le mandataire doit rejeter la demande pour cette raison, le mandataire DOIT la rejeter avec une réponse 480 (Temporairement indisponible). Dans ce cas, le mandataire DEVRAIT inclure un en-tête Warning avec un code d'avertissement de 380 "SIPS non admis".

Les mandataires DEVRAIENT transporter les demandes en utilisant un URI SIP sur TLS quand il est possible d'établir une connexion TLS, ou en réutiliser une existante. La [RFC5626], par exemple, permet de réutiliser une connexion TLS existante. Certains mandataires pourraient avoir des politiques qui interdisent l'envoi de toute demande sur autre chose que TLS.

Quand un mandataire reçoit une demande avec un URI de demande SIP, le mandataire NE DOIT PAS transmettre la demande à un URI de demande SIPS. Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIPS, et si le mandataire décide de transmettre la demande, le mandataire DOIT remplacer ce schéma SIPS par un schéma SIP tout en laissant le reste de l'URI comme il est, et utiliser l'URI résultant comme URI de demande de la demande transmise. Le mandataire DOIT utiliser TLS pour transmettre la demande à l'UAS. Certains mandataires pourraient avoir une politique de ne pas transmettre du tout les demandes utilisant un URI de demande non SIPS si l'UAS s'est enregistré en

utilisant un champ d'en-tête Contact SIPS. Si le mandataire choisit de rejeter la demande parce qu'il a une telle politique ou parce qu'il n'est pas capable d'établir une connexion TLS, le mandataire PEUT la rejeter avec une réponse 480 (Temporairement indisponible) avec un en-tête Warning et un code d'avertissement 381 "SIPS exigé".

Si un mandataire doit rejeter une demande parce que les URI sont utilisés de façon incohérente (par exemple, l'URI de demande est un URI SIPS, mais le champ d'en-tête Contact est un URI SIP) le mandataire DEVRAIT utiliser le code de réponse 400 (Mauvaise demande).

Il est RECOMMANDÉ que le mandataire utilise les procédures de mandataire sortant définies dans la [RFC5626] pour prendre en charge les UAC qui ne peuvent pas fournir de certificat pour établir une connexion TLS (c'est-à-dire, quand l'authentification côté serveur est utilisée).

Quand un mandataire envoie une demande en utilisant un URI de demande SIPS et reçoit une réponse 3XX avec un champ d'en-tête Contact SIP, ou une réponse 416, ou une réponse 480 (Temporairement indisponible) avec un en-tête Warning et un code d'avertissement de 380 "SIPS non admis", le mandataire NE DOIT PAS rebondir sur la réponse. Dans ce cas, le mandataire DEVRAIT transmettre la meilleure réponse au lieu de rebondir, afin de permettre à l'UAC d'effectuer l'action appropriée.

Quand un mandataire envoie une demande en utilisant un URI de demande SIP et reçoit une réponse 3XX avec un champ d'en-tête Contact SIPS, ou une réponse 480 (Temporairement indisponible) avec un en-tête Warning et un code d'avertissement de 381 "SIPS exigé", le mandataire NE DOIT PAS rebondir sur la réponse. Dans ce cas, le mandataire DEVRAIT transmettre la meilleure réponse au lieu de rebondir, afin de permettre à l'UAC d'effectuer l'action appropriée.

Pour souligner ce qui est déjà défini dans la [RFC3261], les mandataires NE DOIVENT PAS utiliser le paramètre "transport=tls".

5.4 Comportement de serveur de redirection

Utiliser un serveur de redirection avec TLS au lieu d'utiliser un mandataire se heurte à des limitations qui doivent être prises en compte. Comme il n'y a pas de connexion pré-établie entre le mandataire et l'UAS (comme avec la [RFC5626]) c'est seulement approprié pour les scénarios où les connexions entrantes sont permises. Par exemple, ce pourrait être utilisé dans un environnement de serveur à serveur (serveur de redirection ou serveur mandataire) où l'authentification mutuelle TLS est utilisée, et où il n'y a pas de problème de traversée de NAT. Un serveur de redirection ne serait pas capable de rediriger sur une entité qui n'a pas de certificat. Un serveur de redirection pourrait n'être pas utilisable si il y a un NAT entre le serveur et l'UAS.

Quand un serveur de redirection reçoit une demande avec un URI de demande SIP, le serveur de redirection PEUT redirige avec une réponse 3XX à un champ d'en-tête Contact SIP ou SIPS. Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIPS, le serveur de redirection DEVRAIT retourner un champ d'en-tête Contact SIPS si il est dans un environnement où TLS est utilisable (comme décrit au paragraphe précédent). Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIP, le serveur de redirection DOIT retourner un champ d'en-tête Contact SIP dans une réponse 3XX si il redirige la demande.

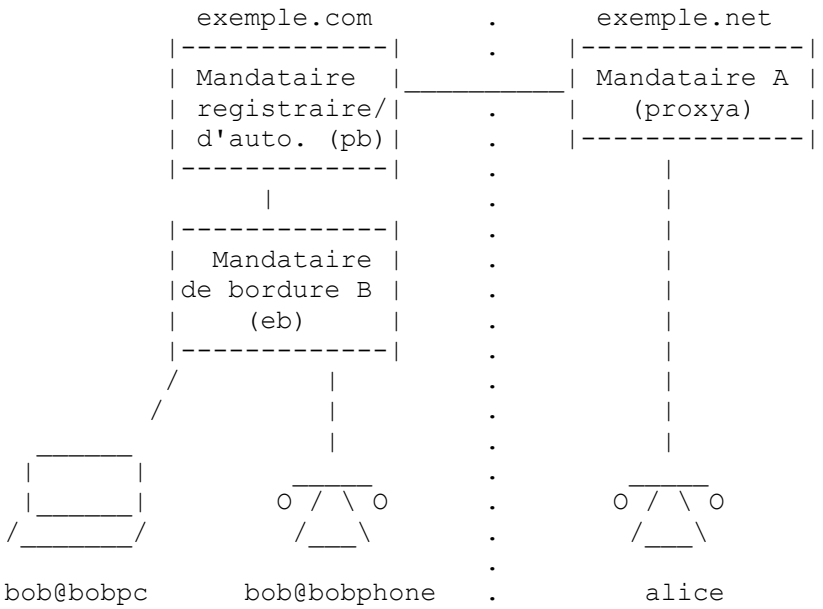
Quand un serveur de redirection reçoit une demande avec un URI de demande SIPS, le serveur de redirection PEUT rediriger avec une réponse 3XX à un champ d'en-tête Contact SIP ou SIPS. Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIPS, le serveur de redirection DEVRAIT retourner un champ d'en-tête Contact SIPS si il est dans un environnement où TLS est utilisable. Si l'UAS cible s'est enregistré précédemment en utilisant un champ d'en-tête Contact SIP, le serveur de redirection DOIT retourner un champ d'en-tête Contact SIP dans une réponse 3XX si il choisit de rediriger ; autrement, l'UAS PEUT rejeter la demande avec une réponse 480 (Temporairement indisponible) avec un en-tête Warning et un code d'avertissement 380 "SIPS Non admis". Si un serveur de redirection redirige sur un UAS dont il n'a pas connaissance (par exemple, une AOR dans un domaine différent) le champ d'en-tête Contact pourrait être de n'importe quel schéma.

Si un serveur de redirection a besoin de rejeter une demande parce que les URI sont utilisés de façon incohérente (par exemple, l'URI de demande est un URI SIPS, mais le champ d'en-tête Contact est un URI SIP) le serveur de redirection DEVRAIT utiliser le code de réponse 400 (Mauvaise demande).

Pour souligner ce qui est déjà défini dans la [RFC3261], les serveurs de redirection NE DOIVENT PAS utiliser le paramètre "transport=tls".

6. Flux d'appels

Le diagramme suivant illustre la topologie utilisée pour les exemples de cette section :



Topologie

Dans les exemples qui suivent, Bob a deux clients : l'un est un client de PC SIP qui fonctionne sur son ordinateur, et l'autre est un téléphone SIP. Le client de PC ne prend pas en charge SIPS, et par conséquent s'enregistre seulement avec un champ d'en-tête Contact SIP. Le téléphone SIP prend cependant en charge SIPS et TLS, et par conséquent s'enregistre avec un champ d'en-tête Contact SIPS. Les deux appareils de Bob passent par un mandataire de bordure B, et par conséquent, ils incluent un champ d'en-tête Route qui indique eb.exemple.com. Le mandataire de bordure B supprime le champ d'en-tête Route correspondant à lui-même, et s'ajoute dans un champ d'en-tête Path. Le flux d'appel du processus d'enregistrement est illustré au paragraphe 6.1.

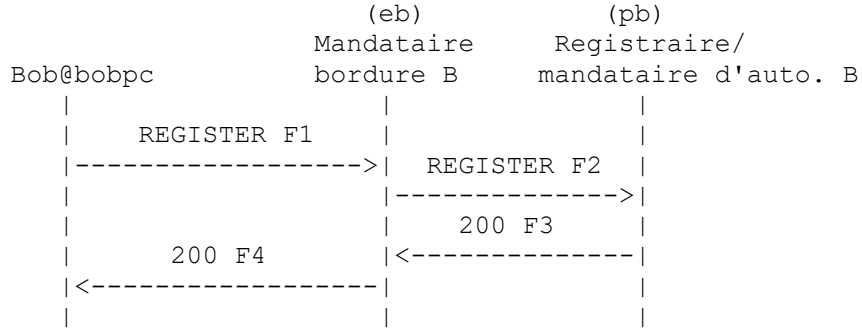
Après l'enregistrement, il y a deux liens Contact associés à l'AOR de Bob de bob@exemple.com : sips:bob@bobphone.exemple.com et sip:bob@bobpc.exemple.com.

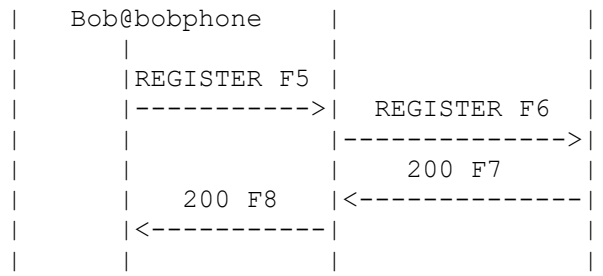
Alice appelle ensuite Bob par son propre mandataire A. Le mandataire A localise le domaine de Bob exemple.com. Dans cet exemple, ce domaine est possédé par le mandataire registraire/d'autorité de Bob Mandataire B. Le mandataire A supprime le champ d'en-tête Route correspondant à lui-même, et s'insère dans le Record-Route et transmet la demande au mandataire registraire/d'autorité B.

Les paragraphes qui suivent illustrent l'enregistrement et trois exemples. Dans le premier exemple (paragraphe 6.2) Alice appelle l'AOR SIPS de Bob. Dans le second exemple (paragraphe 6.3) Alice appelle l'AOR SIP de Bob en utilisant le transport TCP. Dans le troisième exemple (paragraphe 6.4), Alice appelle l'AOR SIP de Bob en utilisant le transport TLS.

6.1 Bob enregistre ses contacts

Ce flux illustre le processus d'enregistrement par lequel l'appareil de Bob s'enregistre. Son client de PC (Bob@bobpc) s'enregistre avec un schéma SIP, et son téléphone SIP (Bob@phone) s'enregistre avec un schéma SIPS.





Bob enregistre ses contacts

Détails du message

F1 REGISTER du client de PC de Bob -> Mandataire de bordure B

```
REGISTER sip:pb.exemple.com SIP/2.0
Via: SIP/2.0/TCP bobpc.exemple.com:5060;branch=z9hG4bKnashds
Max-Forwards: 70
To: Bob <sip:bob@exemple.com>
From: Bob <sip:bob@exemple.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Supported: path, outbound
Route: <sip:eb.exemple.com;lr>
Contact: <sip:bob@bobpc.exemple.com>
  ;+sip.instance="<urn:uuid:0C67446E-F1A1-11D9-94D3-000A95A0E128>"
  ;reg-id=1
Content-Length: 0
```

F2 REGISTER Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
REGISTER sip:pb.exemple.com SIP/2.0
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bK87asdks7
Via: SIP/2.0/TCP bobpc.exemple.com:5060;branch=z9hG4bKnashds
Max-Forwards: 69
To: Bob <sip:bob@exemple.com>
From: Bob <sip:bob@exemple.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Supported: path, outbound
Path: <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>
Contact: <sip:bob@bobpc.exemple.com>
  ;+sip.instance="<urn:uuid:0C67446E-F1A1-11D9-94D3-000A95A0E128>"
  ;reg-id=1
Content-Length: 0
```

F3 200 (REGISTER) Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bK87asdks7
Via: SIP/2.0/TCP bobpc.exemple.com:5060;branch=z9hG4bKnashds
To: Bob <sip:bob@exemple.com>;tag=2493K59K9
From: Bob <sip:bob@exemple.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
CSeq: 1826 REGISTER
Require: outbound
Supported: path, outbound
Path: <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>
Contact: <sip:bob@bobphone.exemple.com>
  ;+sip.instance="<urn:uuid:0C67446E-F1A1-11D9-94D3-000A95A0E128>"
  ;reg-id=1
  ;expires=3600
Date: Mon, 12 Jun 2006 16:43:12 GMT
```

```
  Content-Length: 0
```

F4 200 (REGISTER) Mandataire de bordure B -> Client de PC de Bob

```
  SIP/2.0 200 OK
  Via: SIP/2.0/TCP bobpc.exemple.com:5060;branch=z9hG4bKnashds
  To: Bob <sip:bob@exemple.com>;tag=2493K59K9
  From: Bob <sip:bob@exemple.com>;tag=456248
  Call-ID: 843817637684230@998sdasdh09
  CSeq: 1826 REGISTER
  Require: outbound
  Supported: path, outbound
  Path: <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>
  Contact: <sip:bob@bobphone.exemple.com>
    ;+sip.instance="<urn:uuid:0C67446E-F1A1-11D9-94D3-000A95A0E128>"
    ;reg-id=1
    ;expires=3600
  Date: Thu, 09 Aug 2007 16:43:12 GMT
  Content-Length: 0
```

F5 REGISTER Téléphone de Bob -> Mandataire de bordure B

```
  REGISTER sips:pb.exemple.com SIP/2.0
  Via: SIP/2.0/TLS bobphone.exemple.com:5061;branch=z9hG4bK9555
  Max-Forwards: 70
  To: Bob <sips:bob@exemple.com>
  From: Bob <sips:bob@exemple.com>;tag=90210
  Call-ID: faif9a@qwefnwdclk
  CSeq: 12 REGISTER
  Supported: path, outbound
  Route: <sips:eb.exemple.com;lr>
  Contact: <sips:bob@bobphone.exemple.com>
    ;+sip.instance="<urn:uuid:6F85D4E3-E8AA-46AA-B768-BF39D5912143>"
    ;reg-id=1
  Content-Length: 0
```

F6 REGISTER Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
  REGISTER sips:pb.exemple.com SIP/2.0
  Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bK876354
  Via: SIP/2.0/TLS bobphone.exemple.com:5061;branch=z9hG4bK9555
  Max-Forwards: 69
  To: Bob <sips:bob@exemple.com>
  From: Bob <sips:bob@exemple.com>;tag=90210
  Call-ID: faif9a@qwefnwdclk
  CSeq: 12 REGISTER
  Supported: path, outbound
  Path: <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
  Contact: <sips:bob@bobphone.exemple.com>
    ;+sip.instance="<urn:uuid:6F85D4E3-E8AA-46AA-B768-BF39D5912143>"
    ;reg-id=1
  Content-Length: 0
```

F7 200 (REGISTER) Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
  SIP/2.0 200 OK
  Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bK876354
  Via: SIP/2.0/TLS bobphone.exemple.com:5061;branch=z9hG4bK9555
  To: Bob <sips:bob@exemple.com>;tag=5150
  From: Bob <sips:bob@exemple.com>;tag=90210
  Call-ID: faif9a@qwefnwdclk
  CSeq: 12 REGISTER
  Require: outbound
  Supported: path, outbound
```

```
Path: <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
Contact: <sips:bob@bobphone.exemple.com>
  ;+sip.instance="<urn:uuid:6F85D4E3-E8AA-46AA-B768-BF39D5912143>"
  ;reg-id=1
  ;expires=3600
Date: Thu, 09 Aug 2007 16:43:50 GMT
Content-Length: 0
```

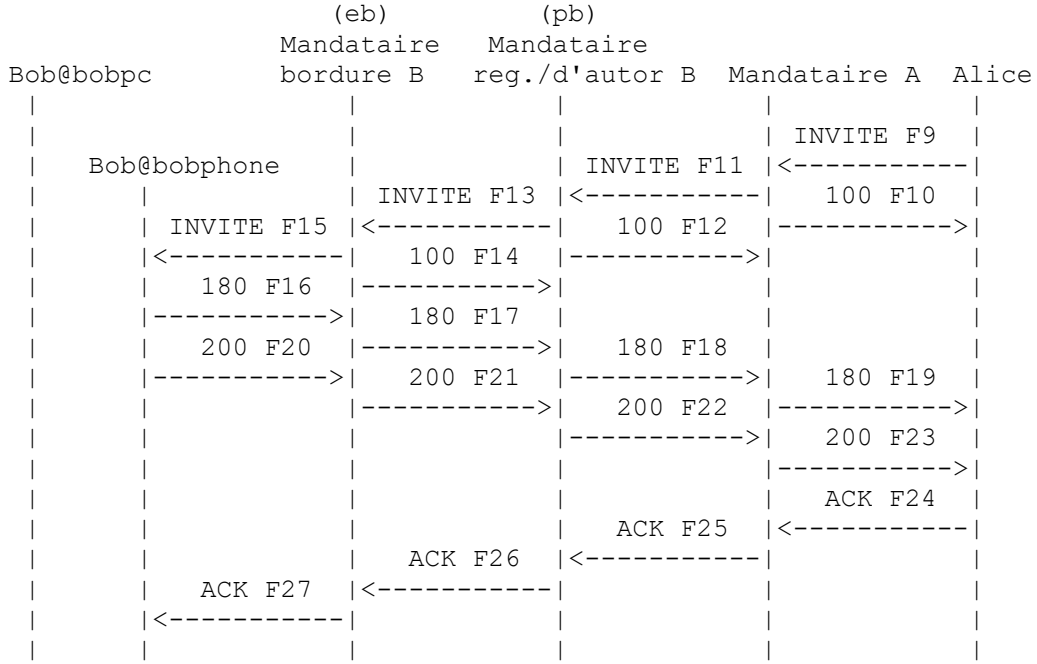
F8 200 (REGISTER) Mandataire de bordure B -> Téléphone de Bob

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS bobphone.exemple.com:5061;branch=z9hG4bK9555
To: Bob <sips:bob@exemple.com>;tag=5150
From: Bob <sips:bob@exemple.com>;tag=90210
Call-ID: faif9a@qwefnwdclk
CSeq: 12 REGISTER
Require: outbound
Supported: path, outbound
Path: <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
Contact: <sips:bob@bobphone.exemple.com>
  ;+sip.instance="<urn:uuid:6F85D4E3-E8AA-46AA-B768-BF39D5912143>"
  ;reg-id=1
  ;expires=3600
Date: Thu, 09 Aug 2007 16:43:50 GMT
Content-Length: 0
```

6.2 Alice appelle l'AOR SIPS de Bob

L'enregistrement de Bob s'est déjà produit comme au paragraphe 6.1.

Dans ce premier exemple, Alice appelle l'AOR SIPS de Bob (sips:bob@exemple.com). Le mandataire registraire/d'autorité B consulte le lien dans la base de données d'enregistrements, et trouve les deux liens de champ d'en-tête Contact. Alice s'est adressée à Bob avec un URI de demande SIPS (sips:bob@exemple.com) de sorte que le mandataire registraire/d'autorité B détermine que l'appel doit être acheminé seulement au téléphone de Bob (qui s'est enregistré en utilisant un champ d'en-tête Contact SIPS) et donc la demande est seulement envoyée à sips:bob@bobphone.exemple.com, à travers le mandataire de bordure B. Le mandataire registraire/d'autorité B et le mandataire de bordure B s'insèrent dans le Record-Route. Bob répond à sips:bob@bobphone.exemple.com.



Alice appelle l'AOR SIPS de Bob

Détails du message

F9 INVITE Alice -> Mandataire A

```
INVITE sips:bob@exemple.com SIP/2.0
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
Max-Forwards: 70
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Route: <sips:proxya.exemple.net;lr>
Contact: <sips:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {as per SDP}
{SDP non montré}
```

F10 100 (INVITE) Mandataire A -> Alice

```
SIP/2.0 100 Trying
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F11 INVITE Mandataire A -> Mandataire de registraire/d'autorité B

```
INVITE sips:bob@exemple.com SIP/2.0
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
Max-Forwards: 69
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route: <sips:proxya.exemple.net;lr>
Contact: <sips:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {as per SDP}
{SDP non montré}
```

F12 100 (INVITE) Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 100 Trying
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F13 INVITE Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
INVITE sips:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
Max-Forwards: 68
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
```

```
Route: <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@edge.exemple.com;lr;ob>
Record-Route: <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F14 100 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 100 Trying
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F15 INVITE Mandataire de bordure B -> Téléphone de Bob

```
INVITE sips:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKbiba
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
Max-Forwards: 67
To: Bob <sips:bob@exemple.com>
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F16 180 (INVITE) Téléphone de Bob -> Mandataire de bordure B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKbiba
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:bob@bobphone.exemple.com>
Content-Length: 0
```

F17 180 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
```

```
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:bob@bobphone.exemple.com>
Content-Length: 0
```

F18 180 Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:bob@bobphone.exemple.com>
Content-Length: 0
```

F19 180 (INVITE) Mandataire A -> Alice

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:bob@bobphone.exemple.com>
Content-Length: 0
```

F20 200 (INVITE) Téléphone de Bob -> Mandataire de bordure B

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKbiba
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
Contact: <sips:bob@bobphone.exemple.com>
Content-Length: 0
```

F21 200 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bKbalouba
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
```

```
  Record-Route:
   <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
   <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
  Contact: <sips:bob@bobphone.exemple.com>
  Content-Length: 0
```

F22 200 Mandataire de registraire/d'autorité B -> Mandataire A

```
  SIP/2.0 200 OK
  Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKpouet
  Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
  To: Bob <sips:bob@exemple.com>;tag=5551212
  From: Alice <sips:alice@exemple.net>;tag=8675309
  Call-ID: lzksjf8723k@sodk6587
  CSeq: 1 INVITE
  Record-Route:
   <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
   <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
  Contact: <sips:bob@bobphone.exemple.com>
  Content-Length: 0
```

F23 200 (INVITE) Mandataire A -> Alice

```
  SIP/2.0 200 OK
  Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKprout
  To: Bob <sips:bob@exemple.com>;tag=5551212
  From: Alice <sips:alice@exemple.net>;tag=8675309
  Call-ID: lzksjf8723k@sodk6587
  CSeq: 1 INVITE
  Record-Route:
   <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
   <sips:pb.exemple.com;lr>, <sips:proxya.exemple.net;lr>
  Contact: <sips:bob@bobphone.exemple.com>
  Content-Length: 0
```

F24 ACK Alice -> Mandataire A

```
  ACK sips:bob@bobphone.exemple.com SIP/2.0
  Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKksdjf
  Max-Forwards: 70
  To: Bob <sips:bob@exemple.com>;tag=5551212
  From: Alice <sips:alice@exemple.net>;tag=8675309
  Call-ID: lzksjf8723k@sodk6587
  CSeq: 1 ACK
  Route: <sips:proxya.exemple.net;lr>, <sips:pb.exemple.com;lr>,
   <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@pb.exemple.com;lr;ob>
  Content-Length: 0
```

F25 ACK Mandataire A -> Mandataire de registraire/d'autorité B

```
  ACK sips:bob@bobphone.exemple.com SIP/2.0
  Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKplo7hy
  Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKksdjf
  Max-Forwards: 69
  To: Bob <sips:bob@exemple.com>;tag=5551212
  From: Alice <sips:alice@exemple.net>;tag=8675309
  Call-ID: lzksjf8723k@sodk6587
  CSeq: 1 ACK
  Route: <sips:pb.exemple.com;lr>,
   <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@pb.exemple.com;lr;ob>
  Content-Length: 0
```

F26 ACK Mandataire registraire/d'autorité B -> Mandataire de bordure B

```
ACK sips:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bK8msdu2
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKplo7hy
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKksdjf
Max-Forwards: 69
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Route: <sips:pb.exemple.com;lr>,
 <sips:psodkfsj+34+kklsL+uJH-Xm816k09Kk@pb.exemple.com;lr;ob>
Content-Length: 0
```

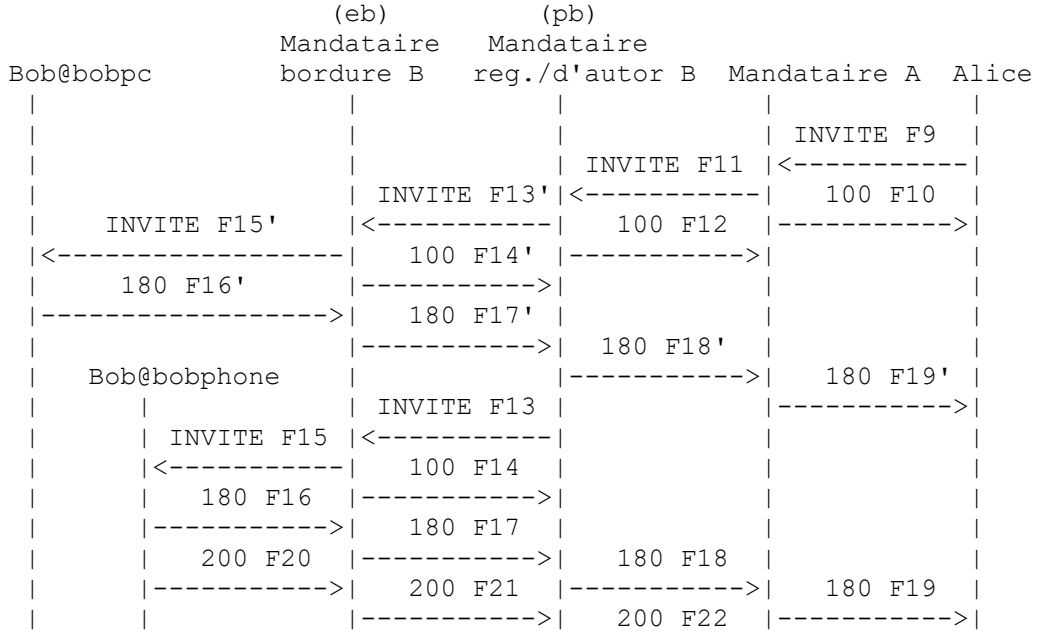
F27 ACK Mandataire B -> Téléphone de Bob

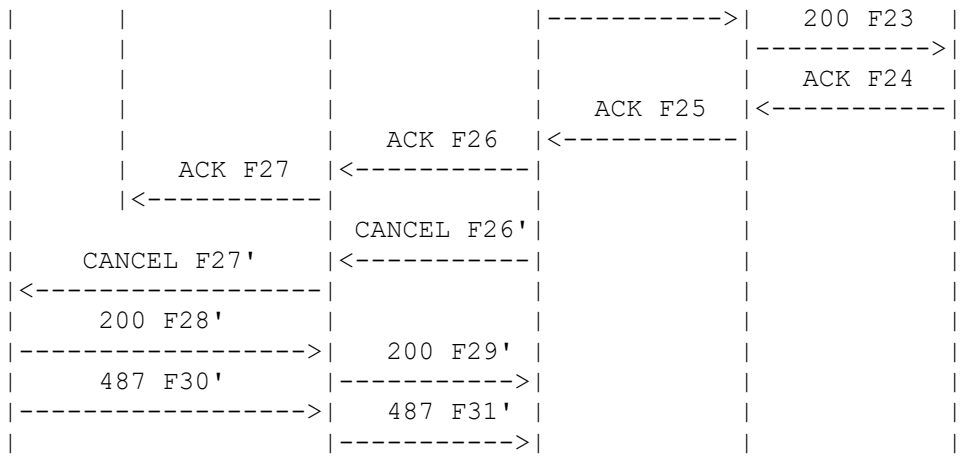
```
ACK sips:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKkmfdgk
Via: SIP/2.0/TLS pb.exemple.com:5061;branch=z9hG4bK8msdu2
Via: SIP/2.0/TLS proxya.exemple.net:5061;branch=z9hG4bKplo7hy
Via: SIP/2.0/TLS alice-1.exemple.net:5061;branch=z9hG4bKksdjf
Max-Forwards: 68
To: Bob <sips:bob@exemple.com>;tag=5551212
From: Alice <sips:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Content-Length: 0
```

6.3 Alice appelle l'AOR SIPS de Bob en utilisant TCP

L'enregistrement de Bob s'est déjà produit comme au paragraphe 6.1.

Dans le second exemple, Alice appelle plutôt l'AOR SIP de Bob (sip:bob@exemple.com) et elle utilise TCP comme transport. Le mandataire registraire/d'autorité B consulte le lien dans la base de données d'enregistrements, et trouve les deux liens de champ d'en-tête Contact. Alice s'est adressée à Bob avec un URI de demande SIP (sip:bob@exemple.com) de sorte que le mandataire registraire/d'autorité B détermine que l'appel doit être acheminé à la fois à bobpc (qui s'est enregistré avec un champ d'en-tête Contact SIP) et à bobphone (qui s'est enregistré avec un champ d'en-tête Contact SIPS) et donc la demande est fourchée à sip:bob@bobpc.exemple.com et sip:bob@bobphone.exemple.com, à travers le mandataire de bordure B. Noter que le mandataire registraire/d'autorité B a préservé le schéma SIP de l'URI de demande au lieu de le remplacer par le schéma SIPS du champ d'en-tête Contact qui était utilisé pour l'enregistrement. Le mandataire registraire/d'autorité B et le mandataire de bordure B s'insèrent dans le Record-Route. La politique du téléphone de Bob est d'accepter les appels à SIP et SIPS (c'est-à-dire, "au mieux") de sorte que son client de PC et son téléphone SIP sonnent en même temps. Bob répond sur son téléphone SIP, et la jambe fourchée de l'appel sur le client de PC est annulée.





Alice appelle l'AOR SIP de Bob

Détails du message

F9 INVITE Alice -> Mandataire A

```
INVITE sip:bob@exemple.com SIP/2.0
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 70
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Route: <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F10 100 (INVITE) Mandataire A -> Alice

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F11 INVITE Mandataire A -> Mandataire de registraire/d'autorité B

```
INVITE sip:bob@exemple.com SIP/2.0
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 69
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route: <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F12 100 (INVITE) Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 100 Trying
```

```
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F13' INVITE Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
INVITE sip:bob@bobpc.exemple.com SIP/2.0
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 68
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Route: <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>
Record-Route: <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F14' 100 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F15' INVITE Mandataire de bordure B -> Client de PC de Bob

```
INVITE sip:bob@bobpc.exemple.com SIP/2.0
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bKbiba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 67
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F16' 180 (INVITE) Client de PC de Bob -> Mandataire de bordure B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bKbiba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
```

```
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=963258
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobpc.exemple.com>
Content-Length: 0
```

F17' 180 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=963258
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobpc.exemple.com>
Content-Length: 0
```

F18' 180 (INVITE) Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=963258
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobpc.exemple.com>
Content-Length: 0
```

F19' 180 (INVITE) Mandataire A -> Alice

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=963258
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:laksdyjanseg237+fsdf+uy623hytIJ8@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobpc.exemple.com>
Content-Length: 0
```

F13 INVITE Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
INVITE sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 68
To: Bob <sip:bob@exemple.com>
```

```
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Route: <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
Record-Route: <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F14 100 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F15 INVITE Mandataire de bordure B -> Téléphone de Bob

```
INVITE sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 68
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:alice@alice-1.exemple.net>
Content-Type: application/sdp
Content-Length: {comme dans le SDP}
{SDP non montré}
```

F16 180 (INVITE) Téléphone de Bob -> Mandataire de bordure B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F17 180 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
```

```
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F18 180 (INVITE) Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F19 180 (INVITE) Mandataire A -> Alice

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F20 200 (INVITE) Téléphone de Bob -> Mandataire de bordure B

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F21 200 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
```

```
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F22 200 (INVITE) Mandataire de registraire/d'autorité B -> Mandataire A

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F23 200 (INVITE) Mandataire A -> Alice

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Record-Route:
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>,
 <sip:pb.exemple.com;lr>, <sip:proxya.exemple.net;lr>
Contact: <sip:bob@bobphone.exemple.com>
Content-Length: 0
```

F24 ACK Alice -> Mandataire A

```
ACK sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 70
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Route: <sip:proxya.exemple.net;lr>, <sip:pb.exemple.com;lr>,
 <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@edge.exemple.com;lr;ob>
Content-Length: 0
```

F25 ACK Mandataire A -> Mandataire de registraire/d'autorité B

```
ACK sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 69
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Route: <sip:pb.exemple.com;lr>,
      <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
 Content-Length: 0
```

F26 ACK Mandataire de registraire/d'autorité B-> Mandataire de bordure B

```
ACK sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 69
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Route: <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
Content-Length: 0
```

F27 ACK Mandataire B -> Téléphone de Bob

```
ACK sip:bob@bobphone.exemple.com SIP/2.0
Via: SIP/2.0/TLS eb.exemple.com:5061;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.1
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
Max-Forwards: 68
To: Bob <sip:bob@exemple.com>;tag=5551212
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 ACK
Content-Length: 0
```

F26' CANCEL Mandataire de registraire/d'autorité B -> Mandataire de bordure B

```
CANCEL sip:bob@bobpc.exemple.com SIP/2.0
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Max-Forwards: 70
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 CANCEL
Route: <sip:psodkfsj+34+kklsL+uJH-Xm816k09Kk@eb.exemple.com;lr;ob>
Content-Length: 0
```

F27' CANCEL Mandataire de bordure B -> Client de PC de Bob

```
CANCEL sip:bob@bobpc.exemple.com SIP/2.0
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Max-Forwards: 69
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 CANCEL
Content-Length: 0
```

F28' 200 (CANCEL) Client de PC de Bob -> Mandataire de bordure B

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 CANCEL
Content-Length: 0
```

F29' 200 (CANCEL) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 CANCEL
Content-Length: 0
```

F30' 487 (INVITE) Client de PC de Bob -> Mandataire de bordure B

```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/TCP eb.exemple.com:5060;branch=z9hG4bKtroubaba
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

F31' 487 (INVITE) Mandataire de bordure B -> Mandataire de registraire/d'autorité B

```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/TCP pb.exemple.com:5060;branch=z9hG4bKbalouba.2
Via: SIP/2.0/TCP proxya.exemple.net:5060;branch=z9hG4bKpouet
Via: SIP/2.0/TCP alice-1.exemple.net:5060;branch=z9hG4bKprout
To: Bob <sip:bob@exemple.com>
From: Alice <sip:alice@exemple.net>;tag=8675309
Call-ID: lzksjf8723k@sodk6587
CSeq: 1 INVITE
Content-Length: 0
```

6.4. Alice appelle l'AOR SIP de Bob en utilisant TLS

L'enregistrement de Bob s'est déjà produit comme au paragraphe 6.1.

Le troisième exemple est identique au second, sauf que Alice utilise TLS comme transport pour sa connexion à son mandataire. Un tel arrangement serait courant si l'UA d'Alice prenait en charge TLS et voulait utiliser une seule connexion avec le mandataire (comme ce serait le cas quand on utilise la [RFC5626]). Dans l'exemple ci-dessous, le mandataire A utilise aussi TLS comme transport pour communiquer avec le mandataire sortant B, mais ce n'est pas nécessairement le cas.

Quand on utilise un URI SIP dans l'URI de demande mais TLS comme transport pour envoyer la demande, le champ Via indique TLS. Le champ d'en-tête Route (si il est présent) va normalement utiliser un URI SIP (mais ce pourrait aussi être un URI SIPS). Les champs d'en-tête Contact, To et From, vont cependant aussi normalement indiquer un URI SIP.

Le flux d'appels serait exactement comme dans le second exemple (paragraphe 6.3). La seule différence serait que tous les champs d'en-tête Via utiliseraient les paramètres TLS Via. Les URI resteraient des URI SIP et non des URI SIPS.

7. Autres considérations

SIP [RFC3261] lui-même introduit des complications avec l'utilisation de SIPS, par exemple, quand Record-Route n'est pas utilisé. Quand un URI SIPS est utilisé dans un champ d'en-tête Contact dans une demande d'initiation de dialogue et que Record-Route n'est pas utilisé, cet URI SIPS pourrait n'être pas utilisable par l'autre extrémité. Si l'autre extrémité ne prend pas en charge SIPS et/ou TLS, elle ne va pas être capable de l'utiliser. L'exception du dernier bond est un exemple de quand cela peut arriver. Dans ce cas, utiliser Record-Route afin que les demandes soient envoyées par des mandataires peut aider à le faire fonctionner. Un autre exemple est que même dans le cas où le champ d'en-tête Contact est un URI SIPS, où aucun Record-Route n'est utilisé, et où l'extrémité distante prend en charge SIPS et TLS, il pourrait encore n'être pas possible à l'extrémité distante d'établir une connexion TLS avec l'extrémité SIP d'origine si le certificat ne peut pas être validé par l'extrémité distante. Cela pourrait normalement être le cas si l'extrémité d'origine avait utilisé l'authentification côté serveur,

comme décrit ci-dessous, ou si l'extrémité d'origine n'utilise pas un certificat qui peut être validé.

TLS lui-même a un impact significatif sur la façon dont SIPS peut être utilisé. L'authentification côté serveur (où le côté serveur fournit son certificat mais pas le côté client) est normalement utilisée entre l'appareil SIP d'utilisateur final agissant comme le côté client TLS (par exemple, un téléphone ou un ordinateur personnel) et son serveur SIP (mandataire ou registraire) agissant comme côté serveur TLS. L'authentification TLS mutuelle (où le côté client et le côté serveur fournissent tous deux leurs certificats respectifs) est normalement utilisée entre les serveurs SIP (mandataires, registraires) ou les appareils configurés statiquement comme des passerelles du RTPC ou des serveurs de supports. Dans le modèle d'authentification mutuelle, pour que deux entités soient capables d'établir une connexion TLS, il est exigé que les deux côtés soient capables de valider les certificats de chaque autre, par configuration statique ou en étant capable de recourir à un certificat racine valide. Avec l'authentification côté serveur, seul le côté client est capable de valider le certificat du côté serveur, car le côté client ne fournit pas de certificat. Les conséquences de tout cela sont que chaque fois qu'un URI SIPS est utilisé pour établir une connexion TLS, on s'attend qu'il soit possible à l'entité qui établit la connexion (le client) de valider le certificat provenant du côté serveur. Pour l'authentification de côté serveur, la [RFC5626] est l'approche recommandée. Pour l'authentification mutuelle, on doit s'assurer que l'architecture du réseau est telle que les connexions soient faites entre des entités qui ont accès aux certificats de chaque autre. Record-Route [RFC3261] et Path [RFC3327] sont très utiles pour s'assurer que les connexions TLS précédemment établies peuvent être réutilisées. D'autres mécanismes pourraient aussi être utilisés dans certaines circonstances : par exemple, utiliser des certificats racine largement reconnus permet de créer plus facilement les connexions TLS.

8. Considérations sur la sécurité

La plus grande partie du présent document peut être considérée comme des considérations sur la sécurité car il s'applique à l'usage de l'URI SIPS.

L'exception "de dernier bond" de la [RFC3261] introduisait un potentiel significatif de vulnérabilités dans SIP, et elle est donc déconseillée par la présente spécification.

Le paragraphe 26.4.4 de la [RFC3261] décrit les considérations sur la sécurité pour le schéma d'URI SIPS. Ces considérations sur la sécurité s'appliquent aussi ici, telles que modifiées par l'Appendice A.

9. Considérations relatives à l'IANA

La présente spécification enregistre deux nouveau codes d'avertissement, à savoir 380 "SIPS non admis" et 381 "SIPS exigé". Les codes d'avertissement sont définis comme suit, et ont été inclus dans le sous registre Codes d'avertissement (warn-codes) du registre des paramètres SIP disponible à http://www.iana.org.

380 SIPS Non admis : l'UAS ou le mandataire ne peut pas traiter la demande parce que le schéma SIPS n'est pas permis (par exemple, parce qu'il n'y a actuellement pas de contact SIPS enregistré).

381 SIPS exigé : l'UAS ou mandataire ne peut pas traiter la demande parce que le schéma SIPS est exigé.

Référence : RFC 5630

La note dans le sous registre Codes d'avertissement (est comme suit :
Les codes d'avertissement fournissent des information supplémentaire pour le code d'état dans les messages de réponse SIP.

10. Remerciements

L'auteur tient à remercier Jon Peterson, Cullen Jennings, Jonathan Rosenberg, John Elwell, Paul Kyzivat, Eric Rescorla, Robert Sparks, Rifaat Shekh-Yusef, Peter Reissner, Tina Tsou, Keith Drage, Brian Stucker, Patrick Ma, Lavis Zhou, Joel Halpern, Hisham Karthabil, Dean Willis, Eric Tremblay, Hans Persson, et Ben Campbell de leur relecture attentive et de leurs retours. Un grand merci à Rohan Mahy pour m'avoir guidé à travers les subtilités de la [RFC5626].

11. Références

11.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC5246] T. Dierks, E. Rescorla, "Version 1.2 du protocole de sécurité de la couche Transport (TLS)", août 2008. *(P.S. ; remplace* RFC3268, 4346, 4366 ; *MàJ* RFC4492 ; *rendue obsolète par la* RFC8446)

[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. *(MàJ* RFC3261, RFC3327) *(P. S.)*

11.2 Références pour information

[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.)*

[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.)*

[RFC3515] R. Sparks, "Méthode Refer du protocole d'initialisation de session (SIP)", avril 2003. *(MàJ par* RFC8217)

[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.)*

[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)

[RFC3891] R. Mahy, B. Biggs, R. Dean, "En-tête "Replaces" du protocole d'initialisation de session (SIP)", septembre 2004. *(P.S.)*

[RFC3893] J. Peterson, "Format de corps d'identité authentifiée (AIB) du protocole d'initialisation de session (SIP)", septembre 2004.

[RFC3911] R. Mahy, D. Petrie, "En-tête "Join" du protocole d'initialisation de session (SIP)", octobre 2004. *(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.)*

[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)

[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)

[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.)*

Appendice A. Correction d'erreurs de la RFC 3261

Afin de prendre en charge le matériel du présent document, cette section fait des corrections à la RFC 3261.

La dernière phrase du cinquième alinéa du paragraphe 8.1.3.5 est remplacée par : "Le client DEVRAIT réessayer la demande, cette fois, en utilisant un URI SIP sauf si l'URI de demande original utilisait un schéma SIPS, auquel cas le client NE DOIT PAS réessayer automatiquement la demande."

Le cinquième alinéa du paragraphe 10.2.1 est remplacé par : "Si l'adresse d'enregistrement dans le champ d'en-tête To d'une demande REGISTER est un URI SIPS, alors l'UAC DOIT aussi inclure des URI seulement SIPS dans toute valeur de champ d'en-tête Contact dans les demandes."

Au paragraphe 16.7 dans la description de Record-Route, le second alinéa est supprimé.

Le dernier alinéa du paragraphe 19.1 est reformulé comme suit : "Un URI SIPS spécifie que la ressource doit être contactée de façon sûre. Cela signifie que, en particulier, TLS doit être utilisé sur chaque bond entre l'UAC et la ressource identifiée par l'URI SIPS de cible. Aucune ressource décrite par un URI SIP (...)"

Dans le troisième alinéa du paragraphe 20.43, les mots "la description de session" dans la première phrase sont remplacés par "SIP". Plus loin dans cet alinéa, "390" est remplacé par "380", et "divers avertissements" est remplacé par "divers avertissements en relation avec SIP".

Le second alinéa du paragraphe 26.2.2 est reformulé comme suit : "(...) Quand il est utilisé comme URI de demande d'une demande, le schéma SIPS signifie que chaque bond sur lequel la demande est transmise, jusqu'à ce que la demande atteigne la ressource identifiée par l'URI de demande, est sécurisée avec TLS. Quand il est utilisé par le générateur d'une demande (comme ce serait le cas si il avait employé un URI SIPS comme adresse d'enregistrement de la cible) SIPS impose que le chemin entier de la demande jusqu'au domaine cible soit ainsi sécurisé."

Le premier alinéa du paragraphe 26.4.4 est remplacé par : "En fait utiliser TLS sur chaque segment du chemin d'une demande implique que l'UAS de terminaison soit accessible par TLS (en s'enregistrant avec un URI SIPS comme adresse de contact). Le schéma SIPS implique une confiance transitive. Évidemment, rien n'empêche les mandataires de mentir. Donc, SIPS ne peut pas garantir que l'usage de TLS va être vraiment respecté de bout en bout sur chaque segment d'un chemin de demande. Noter que comme de nombreux UA ne vont pas accepter les connexions TLS entrantes, même ces UA qui prennent en charge TLS vont être obligés de conserver de façon persistante les connexions TLS, comme décrit dans la section sur les limitations de TLS ci-dessus afin de recevoir les demandes sur TLS comme un UAS."

La première phrase du troisième alinéa du paragraphe 26.4.4 est remplacé par : "S'assurer que TLS va être utilisé pour tous les segments de la demande jusqu'à l'UAS cible est un peu plus complexe."

Le quatrième alinéa du paragraphe 26.4.4 est supprimé.

La dernière phrase du cinquième alinéa du paragraphe 26.4.4 est reformulé comme suit : " S/MIME ou, de préférence, la [RFC4474] peut aussi être utilisée par l'UAC d'origine pour aider à s'assurer que la forme originale du champ d'en-tête To est portée de bout en bout."

Dans le troisième alinéa du paragraphe 27.2, la phrase "quand la défaillance de la transaction résulte d'un problème du protocole de description de session (SDP) [RFC2327]" est supprimée.

Dans le cinquième alinéa du paragraphe 27.2, "390" est remplacé par "380", et "divers avertissements" est remplacé par "divers avertissements en relation avec SIP".

Adresse de l'auteur

Francois Audet
Skype Labs
mél : francois.audet@skypelabs.com