Groupe de travail Réseau
**Request for Comments : 3325**
Catégorie : Information
Traduction Claude Brière de L'Isle

C. Jennings, Cisco Systems
J. Peterson, NeuStar, Inc.
M. Watson, Nortel Networks
novembre 2002

# Extensions privées au protocole d'initiation de session (SIP) pour une identité validée au sein de réseaux de confiance

**Statut de ce mémoire**
Le présent mémoire fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.



**Résumé**
Le présent document décrit les extensions privées au protocole d'initiation de session (SIP, *Session Initiation Protocol*) qui permettent à un réseau de serveurs SIP de confiance de valider l'identité d'usagers authentifiés, et l'application des mécanismes existants de confidentialité au problème de l'identité. L'utilisation de ces extensions n'est applicable qu'à l'intérieur d'un domaine administratif avec un accord préalable sur les politiques de création, transport et usage de telles informations. Le présent document N'OFFRE PAS un modèle général de confidentialité ou d'identité convenable pour une application entre differents domaines de confiance, ou une utilisation Internet au sens large.

## Table des matières



## 1. Déclaration d'applicabilité

Le présent document décrit les extensions privées à SIP [1] qui permettent à un réseau de serveurs SIP de confiance de certifier l'identité des utilisateurs finaux ou des systèmes d'extrémité, et de porter les indications de confidentialité exigées de l'utilisateur final. L'utilisation de ces extensions n'est applicable qu'à l'intérieur d'un domaine de confiance, comme défini dans les exigences à court terme pour l'assertion d'identité par le réseau [5]. Les nœuds dans un tel domaine de confiance sont explicitement de confiance pour les utilisateurs et les systèmes d'extrémité pour certifier publiquement l'identité de chaque partie, et sont responsables de la dissimulation de cette identité hors du domaine de confiance lorsque la

confidentialité est requise. Les moyens par lesquels le réseau détermines l'identité à certifier sont en dehors du domaine d'application du présent document (bien que cela entraîne normalement certaines formes d'authentification).

Une exigence clé de [5] est que le comportement de tous les nœuds au sein d'un domaine de confiance donné "T" soit connu pour se conformer à un certain ensemble de spécifications appelé "Spec(T)". La Spec(T) DOIT spécifier le comportement pour ce qui suit :

1. La manière dont les usagers sont authentifiés.
2. Les mécanismes utilisés pour sécuriser la communication entre les nœuds au sein du domaine de confiance.
3. Les mécanismes utilisés pour sécuriser la communication entre les UA et les nœuds au sein du domaine de confiance.
4. La manière utilisée pour déterminer quels hôtes font partie du domaine de confiance.
5. Le traitement par défaut de la confidentialité lorsque aucun champ d'en-tête de confidentialité n'est présent.
6. Que les nœuds dans le domaine de confiance sont conformes à SIP [1].
7. Que les nœuds dans le domaine de confiance sont conformes au présent document.
8. Le traitement de la confidentialité pour l'identité est celui décrit à la Section 7.

Un exemple de Spec(T) convenable est donné à la Section 11.

Le présent document N'OFFRE PAS un modèle général de confidentialité ou d'identification convenable pour une utilisation inter-domaine ou une utilisation dans l'Internet en général. Ses hypothèses sur les relations de confiance entre l(utilisateur et le réseau peuvent ne pas s'appliquer dans de nombreuses applications. Par exemple, ces extensions ne s'accommodent pas d'un modèle dans lequel les utilisateurs finaux peuvent certifier indépendamment leur identité en utilisant les extensions définies ici. De plus, comme l'assertion d'identité n'est pas certifiée cryptographiquement, elle est sujette à des tromperies, répétitions, et falsifications dans toute architecture qui ne satisfait pas aux exigences de [5].

Il manque aussi aux assertions d'identité l'indication de qui fait spécifiquement l'assertion d'identité, et on doit donc supposer que c'est le domaine de confiance qui certifie l'identité. Les informations ne sont donc significatives que lorsque elles sont reçues en toute sécurité d'un nœud connu pour être un membre du domaine de confiance.

En dépit de ces limitations, il y a suffisamment de déploiements spécialisés utiles qui satisfont aux hypothèses décrites ci-dessus, et qui peuvent accepter les limitations qui en résultent, pour garantir la publication pour information de ce mécanisme. Un exemple de déploiement serait un réseau clos qui émule un réseau téléphonique traditionnel à commutation de circuits.

## 2. Conventions

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

Tout au long de ce document, les exigences pour les serveurs mandataires, ou leurs références, ou au comportement de mandataire, s'appliquent également aux autres intermédiaires au sein du domaine de confiance (par exemple, les UA B2B).

Dans le présent document, les termes "identité", "identité certifiée par le réseau" et "domaine de confiance" ont les significations définies dans [5].

## 3. Introduction

Plusieurs fournisseurs offrant un service de téléphonie sur réseau IP ont choisi SIP comme protocole d'établissement d'appel. Leurs environnements exigent un moyen pour que des éléments de réseau de confiance gérés par les fournisseurs de service (par exemple des serveurs mandataires SIP) communiquent l'identité des abonnés à un tel service, tout en dissimulant cette information aux entités qui ne sont pas de confiance lorsque nécessaire. De tels réseaux supposent normalement un certain niveau de confiance transitive entre les fournisseurs et les appareils qu'ils gèrent.

Ces réseaux ont besoin de prendre en charge certains services traditionnels de téléphonie et de satisfaire aux exigences règlementaires et de sécurité publique de base. Cela inclut des services de présentation de l'identité de l'appelant, de blocage de la présentation de l'identité de l'appelant, et la capacité à retracer l'origine d'un appel. Bien que le service SIP de base puisse prendre en charge chacun de ces services indépendamment, certaines combinaisons ne peuvent pas être prises en charge sans les extensions décrites dans le présent document. Par exemple, un appelant qui veut garder son appel confidentiel et par conséquent fournit des informations limitées dans le champ d'en-tête SIP From ne sera pas identifiable par les receveurs de l'appel sauf s'ils s'appuient sur d'autres moyens pour découvrir l'identité de l'appelant. Masquer les

informations d'identité chez l'agent d'utilisateur d'origine va empêcher certains services, par exemple, la trace de l'appel, de fonctionner sur le réseau téléphonique public commuté (RTPC) ou d'être effectués à des intermédiaires qui ne sont pas instruits de l'identité authentifiée de l'usager.

Le présent document essaye de fournir un service d'identité certifiée par le réseau en utilisant un mécanisme très limité et simple, fondé sur les exigences de [5]. Ce travail découle d'une tentative précédente, [6], pour résoudre plusieurs problèmes en rapport avec la confidentialité et l'identité dans les domaines de confiance. Un mécanisme plus complet, [7] qui utilise le chiffrement pour régler ce problème fait actuellement l'objet d'une étude de la part du groupe de travail SIP.

Fournir la confidentialité dans un réseau SIP est plus compliqué que dans le RTPC. Dans les réseaux SIP, les participants à une session sont normalement capables d'échanger du trafic IP directement sans impliquer de fournisseur de service SIP. Les adresses IP utilisées pour ces sessions peuvent elles-mêmes révéler des informations privées. Un mécanisme d'utilisation générale pour fournir la confidentialité dans un environnement SIP est exposé dans [2]. Le présent document applique ce mécanisme de confidentialité au problème de l'assertion de l'identité par le réseau.

## 4. Généralités

Le mécanisme proposé dans le présent document s'appuie sur un nouveau champ d'en-tête appelé "P-Asserted-Identity" qui contient un URI (normalement un URI SIP) et un nom d'affichage facultatif, par exemple:

P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

Un serveur mandataire qui traite un message peut, après avoir authentifier l'utilisateur d'origine d'une certaine façon (par exemple, l'authentification par résumé) insère un tel champ d'en-tête P-Asserted-Identity dans le message et le transmet aux autres mandataires de confiance. Un mandataire qui est sur le point de transmettre un message à un serveur mandataire ou UA qui n'est pas de confiance DOIT retirer toutes les valeurs de champ d'en-tête P-Asserted-Identity si l'utilisateur a demandé que ces informations restent confidentielles. Les utilisateurs peuvent demander ce type de confidentialité comme décrit à la Section 7.

La syntaxe formelle pour l'en-tête P-Asserted-Identity est présentée à la Section 9.

## 5. Comportement de mandataire

Un mandataire dans un domaine de confiance peut recevoir un message d'un nœud qui est de confiance, ou d'un nœud qui n'est pas de confiance. Lorsque un mandataire reçoit un message d'un nœud qui n'est pas de confiance et qu'il souhaite ajouter à un champ d'en-tête P-Asserted-Identity, le mandataire DOIT authentifier l'origine du message, et utiliser l'identité qui résulte de cette authentification pour insérer un champ d'en-tête P-Asserted-Identity dans le message.

Si le mandataire reçoit un message (demande ou réponse) d'un nœud qui est de confiance, il peut utiliser les informations qui sont dans le champ d'en-tête P-Asserted-Identity, s'il en est, comme si il avait authentifié lui-même l'utilisateur.

Si aucun champ d'en-tête P-Asserted-Identity n'est présent, un mandataire PEUT en ajouter un qui contient au plus un URI SIP ou SIPS, et au plus un URL tel. Si le mandataire reçoit le message d'un élément qui n'est pas de confiance et qu'un en-tête P-Asserted-Identity est présent et qu'il contient un URI SIP ou SIPS, le mandataire DOIT remplacer cet URI SIP ou SIPS par un seul URI SIP ou SIPS ou retirer ce champ d'en-tête. De même, si le mandataire reçoit le message d'un élément qui n'est pas de confiance et si un en-tête P-Asserted-Identity est présent et contient un tel URI, le mandataire DOIT remplacer cet URI par un seul URI tel ou retirer le champ d'en-tête.

Lorsque un mandataire transmet un message à un autre nœud, il doit d'abord déterminer si il a confiance en ce nœud ou non. Si il a confiance dans le nœud, le mandataire ne retire aucun champ d'en-tête P-Asserted-Identity qu'il a lui-même généré, ou qu'il a reçu d'une source de confiance. Si l'élément n'est pas de confiance, le mandataire DOIT alors examiner le champ d'en-tête Privacy (s'il est présent) pour déterminer si l'utilisateur demandait que les informations sur l'identité affirmée soient gardées confidentielles.

## 6. Conseils pour des identités multiples

Si un champ d'en-tête P-Preferred-Identity est présent dans le message qu'un mandataire reçoit d'une entité qui n'est pas de confiance, le mandataire PEUT utiliser ces informations comme un conseil suggérant laquelle devrait être affirmée parmi

plusieurs identités valides pour l'utilisateur authentifié. Si un tel conseil ne correspond à aucune identité valide connue du mandataire pour cet utilisateur, le mandataire peut ajouter un en-tête P-Asserted-Identity de sa propre construction, ou il peut rejeter la demande (par exemple, avec un 403 Interdit. Le mandataire DOIT retirer l'en-tête P-Preferred-Identity fourni par l'utilisateur de tout message qu'il transmet.

Un agent d'utilisateur envoie seulement un champ d'en-tête P-Preferred-Identity aux serveurs mandataires dans un domaine de confiance; les agents d'utilisateur NE DOIVENT PAS remplir le champ d'en-tête P-Preferred-Identity dans un message qui n'est pas envoyé directement à un mandataire qui est de confiance pour l'agent d'utilisateur. Si un agent d'utilisateur devait envoyer un message contenant un champ d'en-tête P-Preferred-Identity à un nœud en dehors d'un domaine de confiance, l'identité conseillée pourrait n'être pas gérée de façon appropriée par le réseau, qui pourrait avoir des ramifications néfastes pour la confidentialité.

## 7. Demande de confidentialité

Les parties qui souhaitent demander le retrait des champs d'en-tête P-Asserted-Identity avant qu'ils soient transmis à un élément qui n'est pas de confiance peuvent ajouter au champ d'en-tête Privacy le jeton de confidentialité "id" défini dans le présent document. Le champ d'en-tête Privacy est défini dans [6]. Si ce jeton est présent, les mandataires DOIVENT retirer tous les champs d'en-tête P-Asserted-Identity avant de transmettre les messages aux éléments qui ne sont pas de confiance. Si la valeur du champ d'en-tête Privacy est réglée à "aucune", le mandataire NE DOIT alors PAS retirer les champs d'en-tête P-Asserted-Identity.

Lorsque un mandataire transmet la demande à un élément qui n'est pas de confiance et qu'il n'y a pas de champ d'en-tête, le mandataire PEUT inclure le champ d'en-tête P-Asserted-Identity, ou il PEUT le retirer. Cette décision est une question de politique du domaine de confiance et DOIT être spécifiée dans la Spec(T). Il est RECOMMANDÉ que les champs d'en-tête P-Asserted-Identity NE DEVRAIENT PAS être retirés sauf si des politiques locales de confidentialité l'empêchent, parce que le retrait peut causer l'échec de services fondés sur l'identité affirmée.

Cependant, on devrait noter que sauf si tons les utilisateurs du domaine de confiance ont accès aux services de confidentialité appropriés, la transmission de la P-Asserted-Identity peut résulter en la divulgation d'informations que l'utilisateur n'a pas demandées et qu'il ne peut pas empêcher. Il est donc FORTEMENT RECOMMANDÉ que tous les utilisateurs aient accès aux services de confidentialité qui sont décrits dans le présent document.

La spécification formelle de la valeur de l'en-tête de confidentialité "id" est décrite au paragraphe 9.3. Des lignes directrices générales sur les conditions dans lesquelles les utilisateurs exigent la confidentialité figurent dans [2].

Si plusieurs valeurs de champ d'en-tête P-Asserted-Identity sont présentes dans un message, et si la confidentialité du champ d'en-tête P-Asserted-Identity est requise, toutes les instances des valeurs du champ d'en-tête DOIVENT alors être retirées avant la transmission de la demande à une entité qui n'est pas de confiance.

## 8. Comportement de serveur d'agent d'utilisateur

Normalement, un agent d'utilisateur restitue la valeur d'un champ d'en-tête P-Asserted-Identity qu'il reçoit à son utilisateur. Il peut considérer que l'identité fournie par un domaine de confiance est à privilégier, ou est par nature plus digne de confiance que celle du champ d'en-tête From d'une demande. Cependant, tout comportement spécifique relève de la mise en œuvre ou des services. Le présent document ne rend pas non plus obligatoire par l'agent d'utilisateur un traitement particulier de valeurs multiples de champ d'en-tête P-Asserted-Identity qui se trouveraient apparaître dans un message (comme un URI SIP à côté d'un URL tel).

Cependant, si un serveur d'agent d'utilisateur reçoit un message provenant d'un élément précédent qui n'est pas de confiance, il NE DOIT PAS utiliser le champ d'en-tête P-Asserted-Identity.

Si un UA fait partie du domaine de confiance d'où est reçu un message contenant un champ d'en-tête P-Asserted-Identity, il peut alors utiliser librement la valeur mais il DOIT s'assurer qu'il ne transmet pas les informations à quelque élément qui ne ferait pas partie du domaine de confiance, si l'utilisateur a demandé que les informations sur l'identité affirmée restent confidentielles.

Si un UA ne fait pas partie du domaine de confiance d'où il a reçu un message qui contient un champ d'en-tête P-Asserted-Identity, il peut alors supposer que ces informations n'ont pas besoin de rester confidentielles.

# 9. Syntaxe formelle

La spécification de syntaxe qui suit utilise la forme Backus-Naur augmentée (ABNF) décrite dans la RFC2234 [4].

## 9.1 En-tête P-Asserted-Identity

Le champ d'en-tête P-Asserted-Identity est utilisé entre des entités SIP de confiance (normalement des intermédiaires) pour porter l'identité de l'utilisateur qui envoie un message SIP car il a été vérifié par authentification.

PAssertedID = "P-Asserted-Identity" HCOLON PAssertedID-value *(COMMA PAssertedID-value)
PAssertedID-value = name-addr / addr-spec

Une valeur de champ d'en-tête P-Asserted-Identity DOIT consister en exactement une name-addr ou addr-spec. Il peut y avoir une ou deux valeurs de P-Asserted-Identity. Si il y a une valeur, elle DOIT être un URI sip, sips, ou tel. Si il y a deux valeurs, une valeur DOIT être un URI sip ou sips et l'autre DOIT être un URI tel. On notera que les mandataires peuvent (et vont) ajouter et retirer ce champ d'en-tête.

Le présent document ajoute l'entrée suivante au tableau 2 de la RFC3261 [1] :

| Champ d'en-tête | où | mandataire | ACK | BYE | CAN | INV | OPT | REG | SUB | NOT | REF | INF | UPD | PRA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P-Asserted-Identity | | adr | - | o | - | o | o | - | o | o | o | - | - | - |

## 9.2 En-tête P-Preferred-Identity

Le champ d'en-tête P-Preferred-Identity est utilisé d'un agent d'utilisateur à un mandataire de confiance pour porter l'identité que l'utilisateur envoyant le message SIP souhaite voir utilisée pour la valeur du champ P-Asserted-Header que va insérer l'élément de confiance.

PPreferredID = "P-Preferred-Identity" HCOLON PPreferredID-value *(COMMA PPreferredID-value)
PPreferredID-value = name-addr / addr-spec

Une valeur de champ d'en-tête P-Preferred-Identity DOIT consister en exactement une name-addr ou addr-spec. Il peut y avoir une ou deux valeurs de P-Preferred-Identity. Si il y a une valeur, elle DOIT être un URI sip, sips, ou tel. Si il y a deux valeurs, une valeur DOIT être un URI sip ou sips et l'autre DOIT être un URI tel. On notera que les mandataires peuvent (et vont) retirer ce champ d'en-tête.

Le présent document ajoute l'entrée suivante au Tableau 2 de la RFC3261 [1] :

| Champ d'en-tête | où | mandataire | ACK | BYE | CAN | INV | OPT | REG | SUB | NOT | REF | INF | UPD | PRA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P-Preferred-Identity | | adr | - | o | - | o | o | - | o | o | o | - | - | - |

## 9.3 Type de confidentialité "id"

La présente spécification ajoute un nouveau type de confidentialité ("priv-value") à l'en-tête Privacy, défini dans [2]. La présence de ce type de confidentialité dans un champ d'en-tête Privacy indique que l'utilisateur aimerait que l'identité affirmée par le réseau reste secrète par rapport aux entités SIP extérieures au domaine de confiance que l'utilisateur a authentifié. Noter qu'un usager qui demande plusieurs types de confidentialité DOIT inclure tous les types de confidentialité demandés dans sa valeur de champ d'en-tête Privacy.

priv-value = "id"

Exemple :

Privacy: id

# 10. Exemples

## 10.1 Identité affirmée par le réseau et passée à une passerelle de confiance

Dans cet exemple, proxy.cisco.com crée un champ d'en-tête P-Asserted-Identity à partir d'une identité qu'il a découverte dans l'authentification de résumé SIP. Il transmet ces informations à un mandataire de confiance qui les transmet à une passerelle de confiance. Noter que ces exemples consistent en messages SIP partiels qui n'illustrent que les en-têtes pertinents pour le problème de l'identité authentifiée.

* F1 useragent.cisco.com -> proxy.cisco.com

```
INVITE sip:+14085551212@cisco.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
```

* F2 proxy.cisco.com -> useragent.cisco.com

```
SIP/2.0 407 Proxy Authorization
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
To: <sip:+14085551212@cisco.com>;tag=123456
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Proxy-Authenticate: .... realm="sip.cisco.com"
```

* F3 useragent.cisco.com -> proxy.cisco.com

```
INVITE sip:+14085551212@cisco.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 70
Privacy: id
Proxy-Authorization: .... realm="sip.cisco.com" user="fluffy"
```

* F4 proxy.cisco.com -> proxy.pstn.net (trusted)

```
INVITE sip:+14085551212@proxy.pstn.net SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 69
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000
Privacy: id
```

* F5 proxy.pstn.net -> gw.pstn.net (trusted)

```
INVITE sip:+14085551212@gw.pstn.net SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
```

Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
Via: SIP/2.0/TCP proxy.pstn.net;branch=z9hG4bK-a1b2
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 68
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000
Privacy: id

### 10.2 Identité affirmée par le réseau retirée

Dans cet exemple, l'agent d'utilisateur envoie un INVITE qui indique qu'il préfèrerait l'identité sip:fluffy@cisco.com au premier mandataire, qui authentifie cela avec le résumé SIP. Le premier mandataire crée un champ d'en-tête P-Asserted-Identity et le transmet à un mandataire de confiance (outbound.cisco.com). Le mandataire suivant retire le champ d'en-tête P-Asserted-Identity et la demande de confidentialité avant de transmettre cette demande vers le serveur mandataire biloxi.com qui n'est pas de confiance pour lui.

* F1 useragent.cisco.com -> proxy.cisco.com

INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

* F2 proxy.cisco.com -> useragent.cisco.com

SIP/2.0 407 Proxy Authorization
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
To: <sip:bob@biloxi.com>;tag=123456
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Proxy-Authenticate: .... realm="cisco.com"

* F3 useragent.cisco.com -> proxy.cisco.com

INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 70
Privacy: id
P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
Proxy-Authorization: .... realm="cisco.com" user="fluffy"

* F4 proxy.cisco.com -> outbound.cisco.com (trusted)

INVITE sip:bob@biloxi SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
Via: SIP/2.0/TCP mandataire.cisco.com;branch=z9hG4bK-b234
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748

Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 69
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@vovida.org>
Privacy: id

* F5 outbound.cisco.com -> proxy.biloxi.com (not trusted)

INVITE sip:bob@biloxi SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 68
Privacy: id

* F6 proxy.biloxi.com -> bobster.biloxi.com

INVITE sip:bob@bobster.biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234
Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345
Via: SIP/2.0/TCP proxy.biloxi.com;branch=z9hG4bK-d456
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 67
Privacy: id

## 11. Exemple de Spec(T)

L'intégrité du mécanisme décrit dans le présent document repose sur le fait qu'un nœud sait (par configuration) que tous les nœuds d'un domaine de confiance vont se comporter d'une façon prévisible. Cela exige que le comportement prédéterminé soit clairement défini et que tous les nœuds dans le domaine de confiance soient conformes. On appelle "Spec(T)" la spécification à laquelle doivent se conformer tous les nœuds d'un domaine de confiance.

La suite de la présente section est un exemple de Spec(T), qui n'est d'aucune manière normatif.

1. Exigences de protocole

Les spécifications suivantes DOIVENT être prises en charge :

   1. RFC 3261
   2. RFC 3325

2. Exigences d'authentification

Les utilisateurs DOIVENT être authentifiés avec SIP Digest Authentication.

3. Exigences de sécurité

Les connexions entre les nœuds au sein du domaine de confiance et entre les agents d'utilisateurs et les nœuds dans le domaine de confiance DOIVENT utiliser TLS avec une suite de chiffrement de RSA_WITH_AES_128_CBC_SHA1. L'authentification mutuelle entre les nœuds dans le domaine de confiance DOIT être effectuée et la confidentialité DOIT être négociée.

4. Portée du domaine de confiance

Le domaine de confiance spécifié dans cet accord consiste en hôtes qui possèdent un certificat valide qui est a) signé par examplerootca.org ; b) dont le subjectAltName se termine par un des noms de domaine suivants : trusted.div1.carrier-a.net, trusted.div2.carrier-a.net, sip.carrier-b.com ; et c) dont le nom de domaine correspond au nom d'hôte du subjectAltName dans le certificat.

5. Traitement implicite lorsque aucun en-tête de confidentialité n'est présent
Les éléments qui sont dans le domaine de confiance doivent prendre en charge le service de confidentialité "id", donc l'absence d'un en-tête Privacy peut être supposée indiquer que l'utilisateur ne demande aucune confidentialité. Si aucun champ d'en-tête Privacy n'est présent dans une demande, les éléments dans ce domaine de confiance DOIVENT agir comme si aucune confidentialité n'était demandée.

## 12. Considérations pour la sécurité

Le mécanisme fourni dans le présent document est une prise en compte partielle du problème de l'identité et de la confidentialité dans SIP. Par exemple, ces mécanismes ne fournissent pas de moyen aux utilisateurs finaux pour partager en toute sécurité les information d'identité de bout en bout sans un fournisseur de service de confiance. Les informations d'identité que l'utilisateur désigne comme "privées" peuvent être inspectées par tout intermédiaire participant au domaine de confiance. Ces informations sont sécurisées par la confiance transitive, qui n'est fiable qu'autant que l'est le maillon le plus faible de la chaîne de confiance.

Lorsque une entité de confiance envoie un message à une destination quelconque avec l'identité de cette partie dans un champ d'en-tête P-Asserted-Identity, l'entité DOIT prendre des précautions pour protéger les informations d'identité contre l'espionnage et l'interception afin de protéger la confidentialité et l'intégrité de ces informations d'identité. L'utilisation de mécanismes de sécurité bond par bond de couche transport ou réseau, tels que TLS ou IPsec, avec des suites de chiffrement appropriées, peut satisfaire cette exigence.

## 13. Considérations relatives à l'IANA

### 13.1 Enregistrement de nouveaux champs d'en-tête SIP

Le présent document définit deux nouveaux champs d'en-tête privés SIP, "P-Asserted-Identity" et "P-Preferred-Identity". Comme recommandé par la politique du domaine Transport, ces en-têtes ont été enregistrés par l'IANA dans le registre des en-têtes SIP, en utilisant le numéro de RFC du présent document comme référence.

| | |
|---|---|
| Nom de l'en-tête | P-Asserted-Identity |
| Forme abrégée : | aucune |
| Déposant : | Cullen Jennings |
| | luffy@cisco.com |
| Description normative : | paragraphe 9.1 du présent document |
| Nom de l'en-tête : | P-Preferred-Identity |
| Forme abrégée : | aucune |
| Déposant : | Cullen Jennings |
| | luffy@cisco.com |
| Description normative : | Paragraphe 9.2 du présent document |

### 13.2 Enregistrement du type de confidentialité "id" pour l'en-tête de confidentialité SIP

| | |
|---|---|
| Nom du type de confidentialité : | id |
| Description brève : | Confidentialité demandée pour une identité affirmée par un tiers |
| Déposant : | Cullen Jennings |
| | luffy@cisco.com |
| Description normative : | paragraphe 9.3 du présent document |

## 14. Remerciements

Merci à Bill Marshall et Flemming Andreason [6], Mark Watson [5], et Jon Peterson [7] pour la rédaction des projets qui représentent la plus grande partie du texte qui constitue le présent document. Merci aux nombreuses personnes qui ont fourni des commentaires utiles, parmi lesquelles Jonathan Rosenberg, Rohan Mahy et Paul Kyzivat.

## Références normatives

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

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

[3] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[4] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", RFC2234, novembre 1997.

## Références pour information

[5] M. Watson, "Exigences de court terme pour l'assertion d'identité par le réseau", RFC3324, novembre 2002. *(Info.)*

[6] F. Andreasen, "Extensions de SIP pour l'identité d'appelant validée par le réseau et la confidentialité au sein des réseaux de confiance", Non publié.

[7] J. Peterson, "Améliorations à la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", Non publié.

**Adresse des auteurs**

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/3
San Jose, CA 95134
USA
téléphone : +1 408 527-9132
mél : fluffy@cisco.com

Jon Peterson
NeuStar, Inc.
1800 Sutter Street, Suite 570
Concord, CA 94520
USA

téléphone : +1 925/363-8720
mél : Jon.Peterson@NeuStar.biz

Mark Watson
Nortel Networks
Maidenhead Office Park (Bray House)
Westacott Way
Maidenhead, Berkshire
UK
téléphone : +44 (0)1628-434456
mél : mwatson@nortelnetworks.com

## Déclaration de droits de reproduction



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