Groupe de travail Réseau
Request for Comments : 2848
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Petrack, MetaTel
L. Conroy, Siemens Roke Manor Research
juin 2000

Protocole du service PINT : Extensions à SIP et SDP pour accès IP aux services d'appel téléphonique

Résumé
Le présent document contient la spécification du protocole du service PINT 1.0, qui définit un protocole pour invoquer certains services de téléphone à partir d'un réseau IP. Ces services incluent de passer des appels de base, d'envoyer et de recevoir des télécopies, et de recevoir un contenu sur le téléphone. Le protocole est spécifié comme un ensemble d'améliorations et d'ajouts aux protocoles SIP 2.0 et SDP.

Table des Matières

1. Introduction

Le désir d'invoquer certains services d'appel téléphonique à partir de l'Internet a été identifié par de nombreux groupes différents (utilisateurs, opérateurs de réseaux publics et privés, fournisseurs de service de centre d'appel, vendeurs de matériels, voir la [RFC2458]). Le scénario générique est le suivant (lorsque l'invocation réussit) :

1. un hôte IP envoie une demande à un serveur sur un réseau IP ;
2. le serveur relaye la demande dans un réseau téléphonique ;
3. le réseau téléphonique effectue le service d'appel demandé.

Par exemple, considérons un usager qui souhaite avoir un rappel sur son téléphone. Il se peut qu'un consommateur veuille que quelqu'un dans le service d'assistance d'une entreprise le rappelle. De même, un usager peut vouloir entendre une annonce d'une alerte météorologique envoyée d'un service météorologique automatique distant en cas de tempête.

On utilise le terme de service d'interfonctionnement RTPC/Internet (PINT, *PSTN/Internet Interworking*) pour noter une telle transaction complète, qui commence par l'envoi d'une demande d'un client IP et qui inclut l'appel téléphonique lui-même. Les services PINT se distinguent par le fait qu'ils impliquent toujours deux réseaux séparés : un réseau IP pour demander de faire un appel, et le réseau mondial de téléphone commuté (GSTN, *Global Switched Telephone Network*) pour exécuter l'appel réel. Il est entendu que les systèmes de réseau intelligent, les commutateurs privés, les réseaux de téléphone cellulaires, et le RNIS peuvent tous être utilisés pour livrer des services PINT. Aussi, la demande de service peut venir de l'intérieur d'un réseau IP privé qui est déconnecté de l'Internet global.

Les exigences du protocole PINT ont été délibérément restreintes à la fourniture de la capacité d'invoquer un petit nombre de services d'appel téléphonique fixés. Ces "services PINT de base" sont spécifié à la section 2. On a cependant pris grand soin de développer un protocole aligné lorsque possible sur les autres protocoles de l'Internet, afin que de futures extensions à PINT puissent être développées avec les conférences Internet.

Au sein de l'architecture de conférence Internet, l'établissement des supports d'appels est fait via une combinaison de protocoles. SIP [RFC2543] est utilisé pour établir l'association entre les participants à l'appel (cette association entre participants à l'appel est appelée une "session") et SDP [RFC2327] est utilisé pour décrire les supports de l'échange au sein de la session. Le protocole PINT utilise ces deux protocoles ensemble, en fournissant des extensions et des améliorations pour permettre aux clients et serveurs SIP de devenir des clients et serveurs PINT.

Un utilisateur PINT qui souhaite invoquer un service au sein du réseau téléphonique utilise SIP pour inviter un serveur PINT distant à une session. L'invitation contient une description SDP des supports de la session que l'utilisateur aimerait voir utiliser. Cela peut être un "envoi d'une session de télécopie" ou une "session d'appel téléphonique", par exemple. Dans une session d'exécution de service PINT, le support est transporté sur le système téléphonique, alors que dans une session SIP, le support est normalement transporté sur l'Internet.

Lorsque il est utilisé pour invoquer un service PINT, SIP établit une association entre un client PINT demandeur et le serveur PINT qui est responsable d'invoquer le service au sein du réseau téléphonique. Ces deux entités ne sont pas les mêmes entités que celles du réseau téléphonique impliquées dans le service du réseau téléphonique. Les messages SIP portent au sein de leurs charges utiles SDP une description des supports de la session du réseau téléphonique.

Noter que le fait qu'un serveur PINT accepte une invitation et qu'une session soit établie ne garantit pas que le support soit bien transporté. (Ceci est analogue au fait que si une invitation SIP est bien acceptée, il n'est pas garanti qu'il n'y aura pas un échec ultérieur du matériel audio).

Les exigences particulières des utilisateurs PINT conduisent à quelques nouveaux messages. Lorsque un serveur PINT accepte d'envoyer une télécopie au téléphone B, il se peut que la transmission de télécopie échoue après l'envoi d'une partie de la télécopie. Donc, le client PINT peut souhaiter recevoir des informations sur l'état de la session d'appel téléphonique réelle qui a été impliquée au titre de l'établissement de la session PINT. Trois nouvelles demandes, SUBSCRIBE, UNSUBSCRIBE, et NOTIFY, sont ajoutées ici au SIP traditionnel pour le permettre.

Les améliorations et les ajouts spécifiés ici ne sont pas destinés à altérer de quelque façon que ce soit le comportement du SIP ou SDP de base. L'objet des extensions PINT est d'étendre les services SIP/SDP usuels au monde du téléphone. À part l'intégration dans les protocoles et les architectures existantes, et les avantages de la réutilisation, cela signifie que le protocole spécifié ici peut traiter une classe de services d'appels plus large que les simples services de base.

La suite du présent document est organisée comme suit : la Section 2 décrit les services de base de PINT ; la Section 3 spécifie l'architecture fonctionnelle et le protocole de PINT ; la Section 4 donne des exemples des extensions PINT 1.0 de SIP et SDP ; la Section 5 contient des considérations sur la sécurité pour PINT. La dernière section contient des descriptions de la façon dont le protocole PINT peut être utilisé pour fournir des services sur le GSTN.

Pour un résumé des extensions à SIP et SDP spécifiées dans le présent document, le paragraphe 3.2 donne une liste combinée, décrivant les extensions respectivement à SIP et à SDP.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119]. De plus, la construction "DOIT .... OU ...." implique que c'est une exigence absolue de la présente spécification de mettre en œuvre une des deux possibilités déclarées (représentées par des points dans la phrase ci-dessus). Une mise en œuvre DOIT être capable d'interopérer avec une autre mise en œuvre qui choisit l'une ou l'autre des deux possibilités.

1.1 Glossaire

Demandeur - Hôte Internet qui est à l'origine d'une demande de service.

Service PINT - Service invoqué au sein d'un système téléphonique en réponse à une demande reçue d'un client PINT.

Client PINT - Hôte Internet qui envoie des demandes pour invoquer un service PINT, conformément au présent document.

Passerelle PINT - Hôte Internet qui accepte des demandes de service PINT et les répartit sur un réseau téléphonique.

Système exécutif - Système qui s'interface à un serveur PINT et à un réseau téléphonique qui exécute un service PINT. Il n'a pas besoin d'être directement associé à l'Internet, et est représenté par le serveur PINT dans les transactions avec les entités de l'Internet.

Usager demandeur - Initiateur d'une demande de service. Ce rôle peut être distinct de celui de la "partie" à tout appel au réseau téléphonique qui résulte de la demande.

Partie (à un service d'appel) - Personne qui est impliquée dans un appel au réseau téléphonique résultant de l'exécution d'une demande de service PINT, ou une ressource fondée sur le réseau téléphonique qui est impliquée (comme un envoyeur automatique de télécopie ou une unité de transformation de texte en parole).

2. Services de base PINT

La motivation originelle de la définition de ce protocole était le désir d'invoquer les trois services du réseau téléphonique suivants depuis un réseau IP :

2.1 Demande d'appel

Une demande est envoyée depuis un hôte IP qui provoque l'exécution d'un appel téléphonique, connectant la partie A à une partie B distante.

2.2 Demande de contenu de télécopie

Une demande est envoyée d'un hôte IP qui cause l'envoi d'une télécopie au télécopieur B. La demande PEUT contenir un pointeur sur les données de la télécopie (qui pourraient résider dans le réseau IP ou dans le réseau téléphonique) OU les données de la télécopie elle-même. Le contenu de la télécopie PEUT être du texte OU quelques autres données d'image plus générales. Les détails de la transmission de télécopie ne sont pas accessibles au réseau IP, mais restent entièrement au sein du réseau téléphonique.

Noter que ce service ne se rapporte pas à la "télécopie sur IP" : le réseau IP n'est utilisé que pour envoyer la demande que soit envoyée une certaine télécopie. Bien sûr, il est possible que l'appel résultant de télécopie au réseau téléphonique se trouve utiliser une solution de télécopie IP en temps réel, mais ceci est complètement transparent pour la transaction PINT.

2.3 Demande de parole/envoi/contenu de jeu

Une demande est envoyée d'un hôte IP qui cause l'envoi d'un appel téléphonique à l'usager A, et pour une certaine sorte de contenu à discuter de vive voix. La demande DOIT soit contenir un URL pointant sur le contenu, SOIT inclure le contenu lui-même. Le contenu PEUT être du texte OU quelques autres données d'application plus générales. Les détails de la transmission du contenu ne sont pas accessibles au réseau IP, mais restent entièrement au sein du réseau téléphonique. Ce service pourrait également être appelé "demande d'entendre un contenu" ; le but de l'usager est d'entendre le contenu qui lui est dit. Le mécanisme par lequel la demande est formulée sort du domaine d'application du présent document ; cependant, un exemple pourrait être qu'une page de la Toile a un bouton qui lorsque il est pressé cause l'envoi d'une demande PINT au RTPC *(réseau téléphonique public commuté)* résultant en la diction du contenu de la page (ou d'autres détails) à la personne.

2.4 Relation entre les services de base PINT et les services traditionnels de téléphone

Il y a de nombreuses versions et variations différentes de chaque service d'appel téléphonique invoqué par une demande PINT. Considérons comme exemple ce qui arrive lorsque un usager demande d'appeler le 1-800-2255-287 via le service Demande-d'appel PINT.

Il peut y avoir des milliers d'agents dans le centre d'appel, et il peut y avoir un nombre indéterminé d'algorithmes et d'équipements sophistiqués utilisés pour décider exactement quel agent va retourner l'appel. Et une fois que ce choix est fait, il peut y avoir de nombreuses façons différentes pour établir l'appel : le téléphone de l'agent peut d'abord sonner, et c'est seulement ensuite que l'usager d'origine sera appelé ; ou peut-être que l'usager sera appelé en premier, et va entendre une horrible musique ou un message préenregistré, pendant que l'agent est localisé.

De même, lorsque une demande PINT cause l'envoi d'une télécopie, il y a des centaines de détails du protocole de télécopie à négocier, ainsi que de détails de transmission au sein des réseaux téléphoniques utilisés.

Les demandes PINT ne spécifient pas trop précisément le service exact du côté téléphone. Les détails du fonctionnement des événements individuels au sein du réseau téléphonique qui exécute la demande sortent du domaine d'application de PINT. Cela n'empêche pas d'exprimer certains détails de haut niveau de la session de réseau téléphonique au sein d'une demande PINT. Par exemple, il est possible d'utiliser l'attribut "lang" de SDP pour exprimer une préférence de langage pour le service Demande d'écouter un contenu. Si un système PINT particulier souhaite permettre à des demandes de contenir des détails du service du côté du réseau téléphonique, il utilisera le mécanisme de l'attribut SDP (voir le paragraphe 3.4.2).

3. Architecture fonctionnelle et du protocole de PINT

3.1 Architecture fonctionnelle de PINT

On suppose une certaine familiarité avec SIP 2.0 [RFC2543] et SDP [RFC2327].

Les clients et serveurs PINT sont des clients et serveurs SIP. SIP est utilisé pour porter la demande sur le réseau IP au serveur PINT correct d'une manière sûre et fiable, et SDP est utilisé pour décrire la session du réseau téléphonique qui sera invoquée ou dont l'état est à retourner.

Un système PINT utilise des serveurs mandataires SIP et des serveurs de redirection pour leurs objets usuels, mais à un certain moment, il doit y avoir un serveur PINT qui a les moyens de relayer les demandes reçues dans un système

téléphonique et de recevoir les accusés de réception de ces demandes relayées. Un serveur PINT qui a cette capacité est appelé une "passerelle PINT". Une passerelle PINT apparaît à un système SIP comme un serveur d'agent d'utilisateur. On remarquera qu'une passerelle PINT apparaît à l'infrastructure PINT comme si elle représentait un "usager", alors qu'en fait elle représente une infrastructure de réseau téléphonique entière qui fournit un ensemble de services du réseau téléphonique.

Ainsi, le système PINT peut apparaître à un client PINT individuel comme suit :

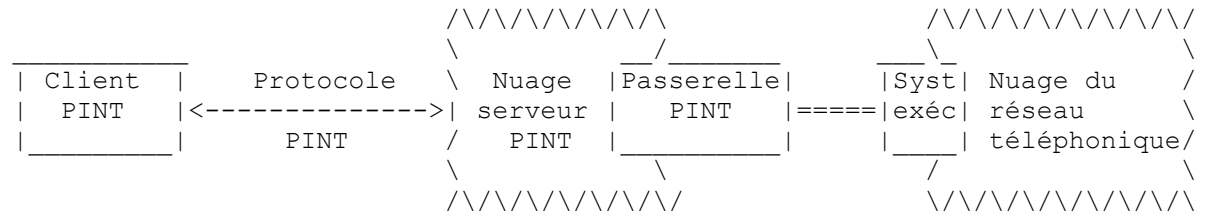

Figure 1 : Architecture fonctionnelle de PINT

Le système des serveurs PINT est représenté comme un nuage pour souligner qu'une seule demande PINT peut passer par une série de serveurs de localisation, de serveurs mandataires, et de serveurs de redirection, avant d'atteindre finalement la passerelle PINT correcte qui peut réellement traiter la demande en la passant au nuage du réseau de téléphone.

La passerelle PINT peut avoir une vraie interface de réseau téléphonique, ou elle peut être connectée via quelque autre protocole ou API à un "système exécutif" qui est capable d'invoquer des services au sein du nuage du téléphone.

Par exemple, au sein d'un système de réseau intelligent (I.N, *Intelligent Network*) la passerelle PINT peut paraître réaliser la fonction de passerelle de contrôle de service. Dans un environnement de bureau, ce peut être un serveur adjoint à l'autocommutateur du bureau, connecté à la fois au LAN du bureau et à l'autocommutateur.

Le système exécutif qui se tient au delà de la passerelle PINT sort du domaine d'application de PINT.

3.2 Architecture du protocole PINT

Ce paragraphe explique comment SIP et SDP fonctionnent en combinaison pour convoyer les informations nécessaires pour invoquer une session de réseau téléphonique.

La liste qui suit résume les caractéristiques d'extension utilisées dans PINT 1.0.Les caractéristiques sont ensuite examinées séparément pour SDP puis pour SIP :

1) Des URL Téléphonie dans les champs Contact de SDP.
2) Précision aux URL Téléphonie de SIP/SDP * Inclusion de plans de numérotation privés.
3) Spécification du fournisseur de service téléphonique (TSP, *Telephone Service Provider*) et/ou paramètres d'URL de contexte téléphonique.
4) Objets de données comme support de session.

4a) Formats de transport de protocole pour indiquer le traitement du support au sein du GSTN.

5) Flux de support implicites (indirects) et arguments opaques.
6) Objets de données en ligne utilisant des multiparties/mime.
7) Précision/éclaircissement sur les arguments opaques passés aux systèmes exécutifs.
   * Cadre pour la présentation des indications de restrictions.
   * Cadre pour les arguments Q.763.
8) Mécanisme d'extension pour que SDP spécifie les structures et force l'échec lorsque un receveur ne prend PAS en charge les extensions spécifiées, en utilisant les en-têtes "require".
9) Prise en charge obligatoire pour les en-têtes "Warning" pour donner des informations plus détaillées sur la disposition de la demande.
10) Mécanisme pour noter un intérêt pour la disposition d'un service demandé, et recevoir des indications sur cette disposition.

PINT et SIP s'appuient tous deux sur les caractéristiques de MIME [RFC2046]. L'utilisation de SIP 2.0 est impliquée par PINT 1.0, et cela implique aussi la conformité à la version 1.0 de MIME.

3.2.1 Fonctionnement de SDP dans PINT

La charge utile SDP contient une description de la session particulière de réseau téléphonique que le demandeur souhaite voir survenir sur le GSTN. Ces informations incluent des choses comme l'adresse du réseau téléphonique (c'est-à-dire, le "numéro de téléphone") du ou des terminaux impliqués dans l'appel, une indication du type de support à transporter (par exemple, audio, texte, image ou données d'application) et une indication de si les informations sont à transporter sur le réseau téléphonique via un transport vocal, de télécopie, ou de message. Une indication du contenu à envoyer au terminal téléphonique distant (si il y en a un) est aussi incluse.

SDP est assez souple pour convoyer des paramètres indépendamment. Par exemple, une demande d'envoi de texte via un transport vocal sera satisfaite en invoquant un service de texte en parole sur le téléphone, et une demande d'envoi de texte via une télécopie sera satisfaite en invoquant un service de texte à télécopie.

Voici une liste des améliorations et ajouts de PINT 1.0 à SDP :
a. un nouveau type de réseau (TN, *network type*) et d'adresses "RFC2543" et "X-..." (paragraphe 3.4.1).
b. de nouveaux types de supports "texte", "image", et "application", de nouveaux mots clés de transport de protocole "voix", "fax" et "pager" et les étiquettes associées de types de format et d'attribut (paragraphe 3.4.2).
c. de nouveaux attributs spécifiques du format pour les données de contenu incluses (paragraphe 3.4.2.4).
d. de nouvelles étiquettes d'attribut, utilisées pour passer les informations au réseau téléphonique (paragraphe 3.4.3).
e. une nouvelle étiquette d'attribut "require", utilisée par un client pour indiquer que la prise en charge d'un attribut est exigée du serveur (paragraphe 3.4.4).

3.2.2 Fonctionnement de SIP dans PINT

SIP est utilisé pour porter la demande de service de téléphone du client PINT à la passerelle PINT, et peut inclure un numéro de téléphone si nécessaire pour le service particulier. Voici une liste complète d'améliorations PINT et d'ajouts à SIP :
f. les charges utiles multiparties MIME (paragraphe 3.5.1).
g. la prise en charge obligatoire des en-têtes "Warning:" (paragraphe 3.5.2).
h. les demandes SUBSCRIBE et NOTIFY, et UNSUBSCRIBE (paragraphe 3.5.3).
i. les en-têtes "Require:" (paragraphe 3.5.4).
j. un format pour les URL PINT au sein d'une demande PINT (paragraphe 3.5.5).
k. les paramètres de réseau téléphonique au sein des URL PINT (paragraphe 3.5.6).

Le paragraphe 3.5.8 contient des remarques sur la façon dont la demande BYE est utilisée au sein de PINT. Ce n'est pas une extension au SIP de base ; elle est incluse ici pour préciser seulement sa sémantique lorsque utilisée avec des sessions de réseau téléphonique.

3.3 Éléments EXIGÉS et FACULTATIFS pour la conformité à PINT

Parmi eux, seuls le type de réseau TN (qui est associé au type d'adresse de la RFC2543) et l'attribut "require" DOIVENT être pris en charge par les clients et serveurs PINT 1.0. En pratique, la plupart des demandes de service PINT vont utiliser d'autres changements, parmi lesquels des références aux objets de données dans les demandes vont très vraisemblablement apparaître dans les demandes PINT.

Chacune des autres nouvelles constructions PINT permet une fonction différente, et un client ou serveur qui souhaite activer cette fonction particulière DOIT le faire au moyen de la construction spécifiée dans le présent document. Par exemple, construire un client et serveur PINT qui ne fournissent que le service d'appel téléphonique Demande d'appel, sans prendre en charge les autres services de base, est permis.

L'en-tête SIP "Require:" et l'attribut "require" fournissent un mécanisme qui peut être utilisé par les clients et serveurs pour signaler leur besoin et/ou leur capacité à prendre en charge des éléments spécifiques "nouveaux" du protocole PINT.

On devrait noter que de nombreuses caractéristiques facultatives de SIP et SDP ont un sens lorsque spécifiées dans le contexte de PINT. Un exemple est l'attribut SDP a=lang:, qui peut être utilisé pour décrire le langage préféré de l'appelé. Un autre exemple est l'utilisation du paramètre "t=" pour indiquer l'heure à laquelle le service PINT doit être invoqué. C'est l'utilisation normale du champ "t=". Un troisième exemple est celui des attributs de qualité. Toutes les options ou facilités SIP ou SDP sont disponibles sans changement aux clients et serveurs PINT.

À l'inverse, la prise en charge des objets de données au sein des sessions de conférence Internet peut être utile, même si le but n'est pas de fournir une demande de service GSTN. Dans ce cas, les extensions qui couvrent ces éléments peuvent être

incorporées dans une invitation SIP/SDP par ailleurs "vraie". De même, la prise en charge du "require" SDP peut être utile, comme un cadre pour l'ajout de caractéristiques à une infrastructure SIP/SDP "traditionnelle". Là encore, il peut être pratique de les incorporer dans des mises en œuvre SIP/SDP qui ne seraient pas utilisées pour des demandes de service PINT. De tels ajouts vont cependant au delà du domaine d'application du présent document.

3.4 Extensions PINT à SDP

PINT 1.0 ajoute à SDP la possibilité de décrire des sessions de téléphone audio, fax, et pageur. Il est délibérément conçu pour cacher les détails techniques sous-jacents et la complexité du réseau téléphonique. Le seul type de réseau défini pour PINT est le "TN" générique. Des étiquettes plus précises comme "RNIS", "GSM", ne sont pas définies. De même, les protocoles de transport sont désignés simplement comme "télécopie", "voix", et "pageur" ; il n'y a pas d'identifiants plus spécifiques pour les divers protocoles vocaux, de télécopie, ou de pageur du réseau téléphonique. De façon similaire, les données à transporter sont identifiées seulement par un type de contenu MIME, comme données "texte", données "image", ou des données "application" plus générales. Un important exemple de transport de données "application" est le service de base "Accès vocal au contenu de la Toile". Dans ce cas, les données à transporter sont pointées par un URI, le type de contenu des données est application/URI, et le protocole de transport serait "voix". Une sorte de facilité de synthèse de la parole, parlant par un téléphone, devrait être impliquée pour effectuer ce service.

Le paragraphe suivant donne des détails sur les nouveaux mots clés SDP.

3.4.1 Type réseau "TN" et type d'adresse "RFC2543"

Le type de réseau (TN, *Telephone Network*) est utilisé pour indiquer que le terminal est connecté à un réseau téléphonique. Les types d'adresse permis pour le type de réseau TN sont "RFC2543" et les types d'adresse privées, qui DOIVENT commencer par un "X-".

Le type d'adresse RFC2543 est suivi par une chaîne conforme à un sous-ensemble du BNF "abonné téléphonique" spécifié à la figure 4 de SIP [RFC2543). Noter que ce BNF N'EST PAS identique à celui qui définit le "numéro-de-téléphone" dans le champ "p=" de SDP.

Exemples :

```
c= TN  RFC2543  +1-201-406-4090
c= TN  RFC2543  12014064090
```

Une chaîne abonné-téléphonique est d'un de ces deux types : numéro de téléphone mondial ou numéro de téléphone local. Ils sont distingués en faisant précéder un numéro de téléphone mondial d'un signe "plus" ("+"). Un numéro de téléphone mondial est à interpréter par défaut comme une adresse du plan de numérotage de la Recommandation UIT-T E.164 à signification internationale, comme défini par [E.164], tandis qu'un numéro de téléphone local est un numéro spécifié dans le plan de numérotage par défaut dans le contexte de la passerelle PINT receveuse.

Une mise en œuvre PEUT utiliser des types d'adressage privés, qui peuvent être utiles dans un domaine local. Ces types d'adresse DOIVENT commencer par un "X-", et DEVRAIENT contenir un nom de domaine après le X-, par exemple "X-mytype.mydomain.com". Un exemple d'une telle ligne de connexion est le suivant :

```
c= TN X-mytype.mydomain.com  A*8-HELEN
```

où "X-mytype.mydomain.com" identifie ce type d'adresse privée, et "A*8-HELEN" est le numéro dans ce format. Un tel format est défini comme une "OtherAddr" dans l'ABNF de l'Appendice A. Noter que la plupart des numéros de téléphone composables peuvent être exprimés par des numéros de téléphone locaux dans les adresse RFC2543 ; de nouveaux types d'adresse DEVRAIENT n'être utilisés que pour des formats qui ne peuvent pas être écrits ainsi.

3.4.2 Prise en charge des objets de données dans PINT

Un changement significatif de PINT par rapport aux sessions de conférence Internet SIP/SDP traditionnelles est qu'une demande de service PINT peut se référer à un objet de données à utiliser comme source d'informations dans cette demande. Par exemple, une demande de service PINT peut spécifier un document à traiter au titre d'un service GSTN par lequel est envoyée une télécopie. De façon similaire, un service GSTN peut prendre une page de la Toile et résulter en un traitement de vocodeur qui transmet et exprime le contenu sur un téléphone.

La spécification SDP ne prend pas explicitement en charge, pour référence ou transport, des objets de données dans les demandes. Afin d'utiliser SDP pour PINT, il est besoin de décrire de telles sessions de support comme un "appel

téléphonique à un certain numéro durant lequel telle et telle image sont envoyées par télécopie".

Pour prendre cela en charge, deux extensions au format de description de session sont spécifiées. Ce sont de nouvelles valeurs permises pour le champ Media, et une description du paramètre "fmtp" lorsque utilisé avec les valeurs du champ Media (dans le contexte du type "TN" champ Contact).

Un ajout est aussi fait au format de message SIP pour permettre l'inclusion d'objets de données comme sous-parties dans le message de demande lui-même. La syntaxe SDP originale (de la [RFC2327]) pour media-field est donnée comme :

media-field = "m=" accès d'espace support ["/" entier] espace proto 1*(espace fmt) CRLF

Lorsque elle est utilisée dans des demandes PINT, la définition des sous-champs est légèrement étendue. La définition du sous-champ Media est assouplie pour accepter tous les types de supports discrets de "niveau supérieur" définis dans la [RFC2046]. Dans les services de base le type discret "vidéo" n'est pas utilisé, et les types supplémentaires "data" et "control" ne sont pas non plus nécessaires. L'utilisation de ces types n'est pas interdite, mais le comportement attendu d'une passerelle PINT qui reçoit une demande incluant un tel type n'est pas défini ici.

Le sous-champ Port n'a pas de signification dans les demandes PINT car les terminaux de destination sont spécifiés somme utilisant l'adressage "TN", de sorte que la valeur du sous-champ Port dans les demandes PINT est normalement réglé à "1". Une valeur de "0" peut être utilisée comme dans SDP pour indiquer que le terminal ne reçoit pas le support. C'est utile pour indiquer qu'un terminal téléphonique est passé temporairement "en garde". De même, le sous-champ facultatif Entier n'est pas utilisé dans PINT.

Comme mentionné dans la [RFC2327], le sous-champ Protocole de transport est spécifique du type d'adresse associé. Dans le cas où le type d'adresse dans le champ Contact précédent est un de ceux qui sont définis pour être utilisés avec le type de réseau "TN", les valeurs suivantes sont définies pour le sous-champ Protocole de transport : "voix", "fax", et "pageur".

L'interprétation de ce sous-champ dans les demandes PINT est le traitement ou la disposition du service GSTN résultant. Donc, pour le protocole de transport "voix", l'intention est que le service résulte en un appel GSTN vocal, tandis que pour le protocole "fax" le résultat sera une transmission de télécopie GSTN, et un protocole "pageur" va résulter en l'envoi d'un message de radiomessagerie.

Noter que ce sous-champ n'impose nécessairement le type et le sous-type de support d'aucune données de source ; par exemple, un des services de base d'appels à une source de texte pour la vocaliser et la dire dans un appel résultant du service téléphonique. La valeur du protocole de transport serait dans ce cas "voix", tandis que le type de support serait "texte".

Le sous-champ Fmt est décrit dans la [RFC2327] comme étant un protocole spécifique du transport. Lorsque utilisé dans les demandes PINT qui ont une des valeurs de protocole ci-dessus, ce sous-champ consiste en une liste de une ou plusieurs valeurs, dont chacune est un sous-type MIME défini de la valeur du sous-champ Media associé. La valeur spéciale "-" est permise, qui signifie qu'il n'y a pas de sous-type MIME. Ce sous-champ conserve (de la [RFC2327]) sa signification qui est que la liste va contenir un ensemble d'autres sous-types, dont le premier est la valeur préférée.

À des fins expérimentales et par accord mutuel de l'envoyeur et du receveur, une valeur de sous-type peut être spécifiée comme un <jeton X->, c'est-à-dire une chaîne de caractères commençant par "X-". L'utilisation de telles valeurs est déconseillée, et si une telle valeur devait trouver une utilisation courante, elle DEVRAIT être enregistrée auprès de l'IANA en utilisant le processus d'enregistrement standard de type de contenu (voir l'Appendice C).

Lorsque le paramètre Fmt est le seul caractère, "-" (tiret) c'est interprété comme signifiant qu'un sous-type non spécifié ou par défaut peut être utilisé pour ce service. Donc, la valeur du champ Media "m=audio 1 voix -<CRLF>" est interprétée comme signifiant qu'un appel vocal est demandé, en utilisant tout sous-type audio réputé approprié par le système exécutif. Le service PINT est un cas particulier, en ce que la demande vient du réseau IP mais que le service d'appel est fourni au sein du GSTN.
Donc, la demande de service ne va normalement pas être capable de définir le codec particulier utilisé pour l'appel de service GSTN résultant. Si une telle intention est requise, l'attribut quality peut alors être utilisé (voir la section "Attributs suggérés" de la [RFC2327]).

3.4.2.1 Utilisation des attributs fmtp dans les demandes PINT

Pour chaque élément du sous-champ Fmt, il DOIT y avoir un attribut fmtp qui suit. Lorsque utilisé dans les demandes PINT, l'attribut fmtp a une structure générale définie comme suit :

"a=fmtp:" <subtype> <espace> resolution *(<espace> resolution) (<espace> ";" 1(<attribut>) *(<espace> <attribut>))

où <resolution> := (<uri-ref> | <opaque-ref> | <sub-part-ref>)

Un attribut fmtp décrit les sources utilisées avec une certaine entrée Fmt dans le champ Media. Les entrées dans un sous-champ Fmt sont alternatives (la préférée étant la première de la liste). Chaque entrée aura un attribut fmtp correspondant. La liste des résolutions dans un attribut fmtp décrit l'ensemble des sources qui résolvent le choix Fmt qui correspond ; tous les éléments de cet ensemble seront utilisés.

On devrait noter que, pour l'utilisation dans les services PINT, les éléments dans un tel ensemble seront envoyés à la suite ; il est peu probable qu'un essai d'envoi en parallèle réussisse.

Un attribut fmtp peut contenir un mélange de différentes sortes d'éléments. Donc, un attribut peut contenir une sub-part-ref *(référence de sous-partie)* qui indique les données incluses dans une telle sous-partie du message en cours, suivie par une opaque-ref *(référence opaque)* se référant à un contenu sur le GSTN, suivi par une uri-ref *(référence d'URI)* pointant sur des données détenues en externe sur le réseau IP.

Pour indiquer quelle forme prend chaque élément de résolution, chacun d'eux commence par sa propre étiquette littérale. La syntaxe détaillée de chaque forme est décrite dans les sous-paragraphes qui suivent.

3.4.2.2 Prise en charge des références d'objet de données distant dans PINT

Lorsque des objets de données mémorisés ailleurs dans le réseau IP sont à utiliser comme sources pour un traitement au sein d'un service PINT, ils peuvent être référencés en utilisant la forme uri-ref. C'est simplement un identifiant de ressource universel (URI, *Uniform Resource Identifier*) comme décrit dans la [RFC2396].

Noter que la référence DEVRAIT être un URI absolu, car il peut n'y avoir pas assez d'informations contextuelles pour que le serveur receveur résolve une référence relative ; toute utilisation de références relatives exige des accords privés entre l'envoyeur et le receveur du message, et DEVRAIT être évitée sauf si l'envoyeur peut être sûr que le receveur est celui qui était prévu et que la référence est non ambiguë dans ce contexte.

Ceci tient aussi pour les URI partiels (comme"uri:http://aNode/index.htm") car ils devront être résolus dans le contexte du receveur éventuel du message.

La syntaxe générale d'une référence à un objet de données externe fondé sur l'Internet dans une ligne fmtp au sein d'une description de session PINT est :

<uri-ref> := ("uri:" URI-reference)

où URI-reference est défini dans l'Appendice A de la [RFC2396]

Par exemple :

```
c= TN RFC2543 +1-201-406-4090
m= text 1  fax plain
a=fmtp:plain  uri:ftp://ftp.isi.edu/in-notes/rfc2468.txt
ou :
c= TN RFC2543 +1-201-406-4090
m= text 1  fax plain
a=fmtp:plain
uri:http://www.ietf.org/meetings/glance_minneapolis.txt
```

signifie prendre cet objet de données sur l'Internet et l'utiliser comme source pour le service de télécopie GSTN demandé.

3.4.2.3 Prise en charge des objets de données fondés sur le GSTN dans PINT

Les services PINT peuvent se référer aux données qui sont détenues non sur le réseau IP mais plutôt dans le GSTN. La façon dont ces éléments sont indiqués n'a pas besoin d'avoir une signification dans le contexte du demandeur ou de la passerelle PINT ; la référence est simplement des données qui peuvent être utilisées par le système exécutif pour indiquer le contenu destiné à faire partie de la demande. Ces données forment une référence opaque, en ce qu'elles sont envoyées "intouchées" à travers l'infrastructure PINT.

Une référence à des objets de données détenus sur le GSTN a la définition générale suivante :

<opaque-ref> := ("opr:" *uric)

où uric est défini dans l'Appendice A de la [RFC2396].

Par exemple :
c= TN RFC2543 +1-201-406-4090
m= text 1 fax plain
a=fmtp:plain opr:APPL.123.456

signifie d'envoyer les données qui sont indexées SUR le GSTN par la valeur de référence "APPL.123.456" au télécopieur répondant au +1-201-406-4090. Le système exécutif peut aussi prendre en compte l'URL Téléphone contenu dans le champ To: du message SIP conteneur lorsque il décide du contexte à utiliser pour l'objet de données de référence.

Bien sûr, une référence opaque peut aussi être utilisée pour d'autres objets ; elle pourrait, par exemple, être nécessaire pour autoriser l'accès à un document détenu sur le GSTN plutôt que d'être requis pour simplement rendre sans ambiguïté l'objet de données. La raison pour laquelle on met une référence opaque sort cependant du domaine d'application du présent document. C'est simplement un indicateur porté dans une demande PINT.

Une référence opaque peut n'avoir aucune valeur dans le cas où la valeur à utiliser est implicite dans le reste de la demande. Par exemple, supposons qu'une société souhaite utiliser PINT pour mettre en œuvre un "service de rappel de télécopie". Dans leur mise en œuvre actuelle, les images à télécopier sont entièrement définies par le numéro de téléphone composé. Dans la demande PINT, ce numéro de téléphone va apparaître dans le champ "To:" de la demande PINT, et il n'est donc pas besoin d'une valeur de référence opaque.

Si il y a plusieurs résolutions pour une demande de service PINT, et si une d'elles est une référence opaque sans valeur jointe, cette référence opaque DOIT alors être incluse dans la ligne d'attributs, mais avec un champ valeur vide.

Par exemple :

c= TN RFC2543 +1-201-406-4090
m= text 1 fax plain
a=fmtp:plain uri:http://www.sun.com/index.html opr:

pourrait être utilisé pour faire précéder des données à télécopier d'une note d'ouverture.

Dans ce cas particulier où une référence opaque est la seule résolution d'une demande de service PINT, ET où cette référence n'a pas besoin d'une valeur, il n'y a pas besoin du tout d'une liste Fmt ; l'intention du service est sans ambiguïté sans autre résolution.

Par exemple :

c= TN RFC2543 +1-201-406-4090
m= text 1 fax -

signifie qu'il y a un contenu impliqué mémorisé dans le GSTN, et qu'il est identifié de façon univoque par la combinaison du To-URI SIP et du champ Contact de la description de session.

3.4.2.4 Prise en charge de la description de session pour les objets de données inclus

Une solution de remplacement au pointage sur les données via un URI ou une référence opaque à un élément de données détenues sur le GSTN, est la possibilité d'inclure les données de contenu dans la demande SIP elle-même. Ceci est fait en utilisant multiparties MIME pour la charge utile SIP. La première partie MIME contient la description SDP de la session du réseau téléphonique à exécuter. Les autres parties MIME contiennent les données de contenu à transporter.

Les lignes d'attribut spécifique du format de la description de session sont utilisées pour indiquer quelle autre partie MIME de la demande contient les données de contenu. Au lieu d'un URI ou d'une référence opaque, l'attribut spécifique du format indique l'identifiant de contenu de la partie MIME de la demande qui contient les données réelles, et est défini par :

<sub-part-ref> := ("spr:" Content-ID)

où Content-ID est comme défini dans l'Appendice A de la [RFC2045] et dans la [RFC0822]).

Par exemple :

```
c= TN RFC2543 +1-201-406-4090
m= text 1  fax plain
a=fmtp:plain  spr:<Content-ID>
```

Le paramètre <Content-ID> est l'identifiant de contenu d'une des parties MIME dans le message, et ce fragment signifie que le demandeur aimerait que l'objet de données détenu dans la sous-partie de ce message étiquetée <Content-ID> soit télécopiée à la machine qui a le numéro de téléphone +1- 201-406-4090.

Voir aussi au paragraphe 3.5.1 la discussion sur la prise en charge nécessaire dans la demande SIP des objets de données inclus.

3.4.3 Étiquettes d'attribut pour passer les informations au réseau téléphonique

On peut désirer inclure dans la demande PINT des paramètres de service qui ne peuvent être compris que par certaines entités dans le "nuage du réseau téléphonique". Les paramètres d'attribut SDP sont utilisés à cette fin. Ils PEUVENT apparaître dans une description de support particulière ou en dehors d'une description ou d'un support.

Ces attributs peuvent aussi apparaître comme paramètres au sein des URL PINT (voir le paragraphe 3.5.6) au titre d'une demande SIP.

Ceci est nécessaire afin que les terminaux téléphoniques qui exigent que les attributs à définir puissent apparaître dans la ligne To: d'une demande PINT aussi bien que dans les descriptions de session PINT.

L'objet de ces attributs est de permettre au client de spécifier du contexte supplémentaire dans lequel un numéro de téléphone particulier est à interpréter. Les raisons pour lesquelles il peut être nécessaire d'interpréter du contexte supplémentaire pour un certain numéro de téléphone sont nombreuses :

a. le numéro de téléphone peut être joignable de nombreuses façons différentes (comme via des fournisseurs de service téléphonique concurrents) et le client PINT souhaite indiquer son choix de fournisseur de service ;
b. le numéro de téléphone pourrait n'être joignable qu'à partir d'un nombre limité de réseaux (comme un numéro 'vert' de libre appel) ;
c. le numéro de téléphone pourrait n'être joignable que dans un seul réseau téléphonique (comme le service consommateur '152' de BT). De même, le numéro pourrait être une extension interne d'entreprise joignable uniquement du sein du PABX.

Cependant, comme noté plus haut, il n'est habituellement pas nécessaire d'utiliser des attributs SDP pour spécifier le contexte téléphonique. Les URL tels que 152@pint.bt.co.il dans les en-têtes To: et From: et/ou les URI de demande, offrent normalement un contexte suffisant pour résoudre les numéros de téléphone.

Si le client souhaite que la demande échoue si les attributs ne sont pas acceptés, ces attributs DEVRAIENT être utilisés en conjonction avec l'attribut "require" (paragraphe 3.4.4) et l'en-tête "Require:org.ietf.sdp.require" (paragraphe 3.5.4).

Il n'est pas possible de normaliser tous les paramètres internes possibles du réseau téléphonique. Les attributs PINT 1.0 ont été choisis pour cette spécification parce qu'ils sont assez courants pour que de nombreux systèmes PINT différents puissent vouloir les utiliser, et l'interopérabilité sera donc accrue en ayant une seule spécification.

Les lignes d'attribut propriétaire "a=", qui par définition ne sont pas interopérables, peuvent néanmoins être utiles lorsque il est nécessaire de transporter des variables propriétaires internes du réseau téléphonique sur le réseau IP, par exemple pour identifier l'ordre dans lequel les parties de l'appel de service sont à effectuer. Ces attributs privés DEVRAIENT cependant être soumis aux mêmes procédures d'enregistrement de l'IANA que mentionné dans la spécification SDP [RFC2327] (voir aussi l'Appendice C).

3.4.3.1 Attribut phone-context

Un attribut est spécifié pour permettre la "numérotation locale distante". C'est le service qui permet au client PINT de joindre un numéro de l'extérieur de la zone ou du réseau qui peut normalement joindre le numéro. Il est utile lorsque l'envoi ou la réception d'une adresse ne peut être numéroté qu'au sein d'un certain contexte local, qui peut être distant de l'origine du client PINT.

Par exemple, si Alice veut rapporter un problème avec son téléphone, elle peut alors composer un numéro d'appel d'aide aux abonnés "national" ; chez British Telecom au Royaume-Uni, c'est le "152". Noter que dans ce cas, il ne faut aucun préfixe de zone – c'est le numéro abrégé. Si il est numéroté à partir du réseau d'un autre opérateur, il ne va pas se connecter au service des dérangements de British Telecom ; et faire le "+44 152" ne va normalement pas réussir. De tels numéros sont appelés des numéros de service spécifiques du réseau.

Dans le réseau téléphonique, le "contexte local" est fourni par la connexion physique entre le terminal de l'abonné et le commutateur central. Une association analogue entre le client PINT et le serveur PINT qui reçoit en premier la demande peut ne pas exister, ce qui est la raison pour laquelle il peut être nécessaire de fournir ce "contexte de réseau téléphonique" manquant. Cet attribut est défini comme suit :

```
a=phone-context: <phone-context-ident>
phone-context-ident  =  network-prefix / private-prefix
network-prefix =  intl-network-prefix / local-network-prefix
intl-network-prefix =  "+" 1*CHIFFRE
local-network-prefix =  1*CHIFFRE
excldigandplus  =  (0x21-0x2d,0x2f,0x40-0x7d))
private-prefix  =  1*excldigandplus 0*uric
```

Un intl-network-prefix *(préfixe de réseau international)* et un local-network-prefix *(préfixe de réseau local)* DOIVENT être un préfixe réseau de bonne foi, et un network-prefix qui est un intl-network-prefix DOIT commencer par un code de service E.164 ("code de pays").

Il est possible d'enregistrer de nouveaux "private-prefix" auprès de l'IANA afin d'éviter des collisions. Les préfixes qui ne sont pas enregistrés DOIVENT commencer par un "X-" pour indiquer leur nature privée, non standard (voir l'Appendice C).

Exemple 1 :

```
c= TN   RFC2543  1-800-765-4321
a=phone-context:+972
```

Cela décrit un terminal dont l'adresse en Israël (code de pays E.164 972) est 1-800-765-4321.

Exemple 2 :

```
c= TN   RFC2543  1-800-765-4321
a=phone-context:+1
```

Cela décrit un terminal dont l'adresse en Amérique du Nord (code de pays E.164 1) est 1-800-765-4321.

Les deux terminaux téléphoniques décrits par les exemples 1 et 2 sont différents ; en fait ils sont situés dans des pays différents.

Exemple 3 :

```
c=TN RFC2543  123
a=phone-context:+97252
```

Cela décrit un terminal dont l'adresse, lorsque elles est numérotée à partir d'un réseau identifié par +97252 est la chaîne "123". Il se trouve que +97252 définit un des fournisseurs de téléphone cellulaire d'Israël, et 123 atteint des abonnés de ce service lorsque il est numéroté dans ce réseau.

Il peut bien être utile ou nécessaire d'utiliser le paramètre SDP "require" en conjonction avec l'attribut phone-context.

Exemple 4 :

```
c= TN  RFC2543  321
a=phone-context:X-acme.com-23
```

Cela pourrait décrire le terminal de téléphone qui est à l'extension 321 du PBX numéro 23 dans le PBX du réseau privé acme.com. On s'attend à ce qu'une telle description soit compréhensible par le serveur PINT acme.com qui reçoit la demande.

Noter que si le serveur PINT qui reçoit la demande est à l'intérieur du réseau acme.com, le même terminal pourrait être adressable comme suit :

c= TN RFC2543 7-23-321

(en supposant que "7" est composé afin d'atteindre le réseau de PBX privé depuis l'intérieur de acme.com)

3.4.3.2 Attribut Restriction de présentation

Bien qu'elle n'ait pas d'effet sur le transport de la demande de service à travers le réseau IP, il peut y avoir une exigence qu'il soit permis aux générateurs d'une demande de service PINT d'indiquer si il souhaitent ou non que le numéro de téléphone de la "partie A" appelante soit présentée à la "partie B" dans l'appel de service résultant. C'est une exigence légale dans certaines juridictions qu'un appelant soit capable de choisir si son correspondant peut ou non découvrir le numéro de téléphone de l'appelant (en utilisant l'indication automatique du numéro ou l'affichage de l'appelant ou un équipement de présentation de la ligne appelante). Donc, un attribut peut être nécessaire pour indiquer la préférence de l'origine.

On ne spécifie pas si le comportement par défaut du système exécutif est de présenter ou de ne pas présenter le numéro de téléphone d'une partie au terminal GSTN correspondant, et il n'est pas obligatoire dans tous les territoires qu'une passerelle PINT ou un système exécutif agisse sur cet attribut. Il est cependant, défini ici pour être utilisé lorsque il y a des restrictions réglementaires sur le fonctionnement du GSTN, et dans ce cas, le système exécutif peut l'utiliser pour honorer la demande de l'origine.

L'attribut est spécifié comme suit : a=clir:<"vrai" | "faux">

Cette valeur booléenne est nécessaire dans l'attribut car il se peut que l'adresse GSTN soit, par défaut, réglée à NE PAS présenter son identité aux correspondants, et que l'origine veuille le faire pour cet appel particulier. Cela est en ligne avec le but de cet attribut qui est de permettre à l'origine de spécifier quel traitement est voulu pour l'appel de service demandé.

L'interprétation attendue de cet attribut est que, si il est présent et si la valeur est "faux" l'identité de la ligne appelante PUISSE être présentée au terminal correspondant, tandis que si elle est "vrai", il est alors demandé au système exécutif de NE PAS présenter, si possible, l'identité de la ligne appelante.

3.4.3.3 Paramètres de l'attribut CalledPartyAddress de l'UIT-T

Ces attributs correspondent aux champs qui apparaissent dans le champ "CalledPartyAddress" de la Recommandation UIT-T Q.763 (voir le paragraphe 3.9 de [Q.763]). Les clients PINT utilisent ces attributs afin de mieux spécifier des paramètres se rapportant aux adresses des terminaux, dans les cas où l'adresse indique un "numéro de téléphone local". Dans le cas où la demande PINT contient une référence à un terminal GSTN, il peut être exigé des paramètres qu'ils identifient correctement ce terminal distant.

La forme générale de cet attribut est : "a=Q763-<jeton>((":" <valeur>) |"")". On décrit ici trois des éléments possibles et l'utilisation de leurs attributs SDP. Lorsque d'autres éléments Q763 sont à utiliser, ils devraient alors être l'objet d'une spécification supplémentaire pour définir la syntaxe de la transposition d'attribut. Il est recommandé que toute spécification de cette sorte conserve les ensembles de valeurs donnés dans Q.763.

Les attributs définis sont :

a=Q763-nature : indique la "nature de l'indicateur d'adresse". La valeur PEUT être tout nombre entre 0 et 127. Les valeurs suivantes sont spécifiées :

"1" numéro d'abonné
"2" inconnu
"3" numéro à signification nationale
"4" numéro à signification internationale

Les valeurs ont été choisies pour coïncider avec les valeurs de Q.763. Noter que d'autres valeurs sont possibles, conformément aux règles nationales ou à l'expansion future de Q.763.

a=Q763-plan : indique le plan de numérotage auquel appartient l'adresse. La valeur PEUT être tout nombre entre 0 et 7. Les valeurs suivantes sont spécifiées :

"1" plan de numérotage téléphonique (UIT-T E.164)

"3" plan de numérotage des données (UIT-T X.121)
"4" plan de numérotage télex (UIT-T F.69)

Les valeurs ont été choisies pour coïncider avec celles de Q.763. D'autres valeurs sont permises, conformément aux règles nationales ou à l'expansion future de Q.763.

a=Q763-INN : indique si l'acheminement au numéro de réseau interne est permis. La valeur DOIT être UNE de :
"0" acheminement au numéro de réseau interne permis
"1" acheminement au numéro de réseau interne interdit

Les valeurs ont été choisies pour coïncider avec celles de Q.763. Noter qu'il est possible d'utiliser un numéro de téléphone local et d'indiquer via des attributs que le numéro est en fait un numéro E.164 à signification internationale. Normalement, cela NE DEVRAIT PAS être fait ; un numéro E.164 à signification internationale est indiqué en utilisant un "numéro de téléphone mondial" pour la chaîne d'adresse.

3.4.4 Attribut "require"

Selon la spécification SDP, un serveur PINT peut simplement ignorer les paramètres d'attribut qu'il ne comprend pas. Pour forcer un serveur à décliner une demande dont il ne comprend pas un des attributs PINT, un client DEVRAIT utiliser l'attribut "require", spécifié comme suit :

a=require:<attribute-list>

où attribute-list est une liste des attributs, séparés par des virgules, qui apparaissent ailleurs dans la description de session.

Pour bien traiter la demande, le serveur PINT doit comprendre l'attribut ET AUSSI satisfaire à la demande impliquée par la présence de l'attribut, pour chaque attribut qui apparaît dans la liste d'attributs de l'attribut require.

Si le serveur ne reconnaît pas les attributs énumérés, le serveur PINT DOIT retourner un code d'état d'erreur (comme un 420 (mauvaise extension) ou 400 (mauvaise demande)) et DEVRAIT retourner des lignes Warning: convenables expliquant le problème ou un en-tête Unsupported: *(Non pris en charge)* contenant l'attribut qu'il ne comprend pas. Si le serveur reconnaît l'attribut mentionné, mais ne peut pas satisfaire la demande impliquée par la présence de l'attribut, la demande DOIT être rejetée avec un code d'état de 606 (Non acceptable) avec un en-tête Unsupported: convenable ou une ligne Warning:.

L'attribut "require" peut apparaître n'importe où dans la description de session, et un nombre quelconque de fois, mais il DOIT apparaître avant l'utilisation de l'attribut marqué comme requis.

Comme l'attribut "require" est lui même un attribut, la spécification SIP permet à un serveur qui ne comprend pas l'attribut require de l'ignorer. Afin de s'assurer que le serveur PINT va se conformer à l'attribut "require", un client PINT DEVRAIT inclure un en-tête Require: avec l'étiquette "org.ietf.sdp.require" (paragraphe 3.5.4)

Noter que la majorité des extensions PINT sont "étiquetées" et que ces étiquettes peuvent être incluses dans des structures Require. L'exception est l'utilisation de numéros de téléphone dans les parties SDP. Cependant, ceux-ci sont définis comme de nouveaux type de réseau et d'adresse, de sorte qu'un serveur SIP/SDP receveur devrait être capable de détecter si il prend ou non en charge ces formes. Le comportement par défaut pour tout receveur SDP est qu'il va échouer à sa demande PINT si il ne reconnaît pas ou ne prend pas en charge les types de réseau et d'adresse TN et RFC2543 ou jeton X-, car si le contenu n'est pas reconnu, aucune session de support ne sera créée. Donc, une structure séparée n'est pas exigée dans ce cas.

3.5 Extensions PINT à SIP 2.0

Les demandes PINT sont des demandes SIP ; beaucoup des spécifications du présent document expliquent simplement comment utiliser les facilités SIP existantes pour les besoins de PINT.

3.5.1 Multipartie MIME (envoi de données avec une demande SIP)

Une demande PINT peut contenir une charge utile qui est une multipartie MIME. Dans ce cas, la première partie DOIT contenir une description de session SDP qui comporte au moins une des étiquettes d'attribut spécifique du format pour des "données de contenu incluses" spécifiées ci-dessus au paragraphe 3.4.3. Les parties suivantes contiennent des données de contenu qui peuvent être transférées au service d'appel téléphonique demandé. Comme exposé plus haut, au sein d'une

seule demande PINT, certaines des données PEUVENT être pointées par un URI au sein de la demande, et certaines des données PEUVENT être incluses dans la demande.

Si des données incluses sont portées dans une demande de service PINT, l'en-tête d'entité Type de contenu du message SIP englobant DOIT indiquer cela. Pour ce faire, la valeur du type de support au sein de cet en-tête d'entité DOIT être réglée à une valeur de "multipart". Il y a un sous-type de contenu qui est destiné à ces situations dans lesquelles des sous-parties sont à traiter ensemble. C'est le type multipart/related (défini dans la [RFC2387]), et son utilisation est recommandée.

Les parties de corps encloses DEVRAIENT inclure les en-têtes Type de contenu spécifiques de parties comme approprié ("application/sdp" pour la première partie de corps contenant la description de session, avec un type de contenu approprié pour chaque partie "objet de données inclus" suivante). Ceci correspond à la syntaxe standard des messages MIME multiparties comme défini dans la [RFC2046].

Par exemple, dans un message multiparties où la chaîne "------next-------" est la frontière, les deux premières parties pourraient être comme suit :

```
------next-------
Content-Type: application/sdp
  ....
c= TN RFC2543 +1-201-406-4090
m= text 1 pager plain
a=fmtp:plain spr:17@mymessage.acme.com

----------next-------
Content-Type: text/plain
Content-ID:  17@mymessage.acme.com

Ceci est le texte qui est à passer à +1-201-406-4090

----------next-----------
```

La capacité d'indiquer différentes solutions de remplacement pour le contenu à transporter est utile, même lorsque les solutions de remplacement sont incluses dans la demande. Par exemple, une demande d'envoi d'un message court à un pageur peut inclure le message en Unicode [UNICODE] et une version de remplacement du même contenu en texte en clair pour si le serveur PINT ou le réseau téléphonique n'était pas capable de traiter l'unicode.

Les clients PINT devraient faire extrêmement attention lors de l'envoi de données incluses dans une demande PINT. De telles demandes DEVRAIENT être envoyées via TCP, pour éviter la fragmentation et pour transmettre la fiabilité des données. Il est possible que le serveur PINT soit un serveur mandataire qui va dupliquer la demande, ce qui pourrait être désastreux si elle contient une grande quantité de données d'application. Les serveurs mandataires PINT devraient faire attention à ne pas créer de nombreuses copies d'une demande qui contient de grandes quantités de données.

Si le client ne connaît pas la situation réelle de la passerelle PINT, et si il utilise les services de localisation de SIP pour la trouver, et si les données incluses rendent probable que la demande PINT soit transportée sur plusieurs datagrammes IP, il est RECOMMANDÉ que la demande PINT initiale n'inclue pas l'objet de données mais plutôt une référence à celui-ci.

3.5.2 En-tête Warning

Un serveur PINT DOIT prendre en charge l'en-tête SIP "Warning:" afin qu'il puisse signaler le manque de prise en charge des caractéristiques PINT individuelles. Par exemple, supposons que la demande PINT soit d'envoyer une image jpeg à un télécopieur, mais que le serveur ne puisse pas restituer et/ou traduire les images jpeg venant de l'Internet en une transmission de télécopie.

Dans un tel cas, le serveur fait échouer la demande et inclut un Warning comme ce qui suit :

```
Warning:  305  pint.acme.com  Format de support incompatible :  jpeg
```

Les serveurs SIP qui ne comprennent pas du tout les extensions PINT sont vivement invités à mettre en œuvre les en-têtes Warning: pour indiquer que les extensions PINT ne sont pas comprises.

Les en-têtes Warning: peuvent aussi être inclus dans les demandes NOTIFY si il est nécessaire de notifier au client des conditions concernant l'invocation du service PINT (voir le paragraphe suivant).

3.5.3 Mécanisme pour marquer l'intérêt pour la disponibilité d'un service PINT, et recevoir l'indication de cette disponibilité

Il peut être très utile de trouver si une demande de service s'est ou non achevée, et si elle l'est, si elle a réussi ou non. Ceci est particulièrement vrai pour un service PINT, où la personne qui demande le service n'y est pas (nécessairement) partie, et peut n'avoir donc pas de moyen facile de découvrir la disponibilité de ce service. Également, il peut être utile d'indiquer quand le service a changé d'état, par exemple lorsque l'invocation du service a commencé.

Il n'est pas trivial d'arranger un système assez souple pour assurer un contrôle et une surveillance extensive durant un service (voir quelques problèmes au paragraphe 6.4) ; PINT 1.0 utilise un schéma simple qui devrait néanmoins fournir des informations utiles. Il est possible d'étendre le schéma de façon "rétro compatible" de sorte que si nécessaire, il puisse être amélioré ultérieurement.

Le schéma d'enregistrement et d'indication d'état PINT 1.0 utilise trois nouvelles méthodes; SUBSCRIBE, UNSUBSCRIBE, et NOTIFY. Elles sont utilisées pour permettre à un client PINT d'enregistrer son intérêt pour (ou de "s'abonner" à) l'état d'une demande de service, pour indiquer qu'un intérêt antérieur a cessé (c'est-à-dire "se désabonner" de cet état) et au serveur de retourner des indications de service. L'automate à états de SUBSCRIBE/UNSUBSCRIBE est identique à celui de INVITE/BYE ; tout comme INVITE signale le commencement et BYE signale la fin de la participation à une session de support, SUBSCRIBE signale le commencement et UNSUBSCRIBE signale la fin de participation à une session de surveillance. Durant la session de surveillance, les messages NOTIFY sont envoyés pour informer l'abonné d'un changement de l'état ou de la disposition d'une session.

3.5.3.1 Ouverture d'une session de surveillance avec une demande SUBSCRIBE

Lorsque une demande SUBSCRIBE est envoyée à un serveur PINT, elle indique qu'un usager souhaite recevoir des informations sur l'état d'une session de service. La demande identifie la session intéressante en incluant la description de session originale avec la demande, utilisant le global-session-id SDP qui fait partie du champ Origine pour identifier de façon univoque la session de service.

La demande SUBSCRIBE (comme toute autre demande SIP sur une session en cours) est envoyée au même serveur que celui auquel a été envoyée le INVITE d'origine, ou à un serveur qui a été spécifié dans le champ Contact: au sein d'une réponse ultérieure (qui peut bien être la passerelle PINT pour la session).

Bien qu'il y ait des situations dans lesquelles la réutilisation du Call-ID utilisé dans l'INVITE d'origine qui a initié la session d'intérêt soit possible, il y a d'autres situations dans lesquelles ce ne l'est pas. En particulier, lorsque l'abonnement est fait par l'usager qui a initié la demande de service d'origine, le Call-ID peut être utilisé car il sera connu du receveur pour se référer à une session établie précédemment. Cependant, lorsque la demande provient d'un usager autre que le demandeur d'origine, la demande SUBSCRIBE constitue une nouvelle branche d'appel SIP, de sorte que le Call-ID NE DEVRAIT PAS être utilisé ; le seul identifiant courant est le champ Origine de la description de session incluse dans la demande de service d'origine, et donc c'est elle qui DOIT être utilisée.

Plutôt que d'avoir deux méthodes différentes d'identification de la "session intéressante", le choix est d'utiliser le champ Origine de la sous-partie SDP incluse à la fois dans l'INVITE d'origine et dans cette demande SUBSCRIBE.

Noter que la demande NE DOIT PAS inclure de sous-partie autre que la description de session, même si ces autres sous-parties étaient présentes dans la demande INVITE d'origine. Un serveur DOIT ignorer toute sous-partie incluse dans une demande SUBSCRIBE à la seule exception de la description de session enclose.

La demande PEUT contenir un en-tête "Contact:", spécifiant le serveur d'agent d'utilisateur PINT auquel les informations devraient être envoyées.

De plus, elle DEVRAIT contenir un en-tête Expires:, qui indique pendant combien de temps le demandeur PINT souhaite recevoir la notification de l'état de session. On se réfère à la période précédant l'expiration de la demande SUBSCRIBE sous le nom de "période d'abonnement". Voir au paragraphe 5.1.4 les considérations sur la sécurité, en particulier les implications pour la confidentialité.

Une valeur de 0 dans l'en-tête Expires: indique le désir de recevoir une seule réponse immédiate (c'est-à-dire que la demande expire immédiatement). Il est possible d'ouvrir une séquence de sessions de surveillance, de la faire exister, et se terminer, se rapportant toutes à la même session de service.

Une réponse réussie à la demande SUBSCRIBE comporte la description de session, selon la passerelle. Normalement, cela

va être identique à la dernière réponse en antémémoire que la passerelle a retournée à toute demande concernant le même identifiant SDP de session mondiale (voir la section 6 de la [RFC2327], champ o=). La ligne t= peut cependant être altérée pour indiquer le début actuel ou le moment d'arrêt. La passerelle peut ajouter une ligne i= à la description de session pour indique des informations comme le nombre de pages de télécopie qui ont été envoyées. La passerelle DEVRAIT inclure un en-tête Expires: pour indiquer pendant combien de temps elle veut conserver la session de surveillance. Si c'est inacceptable pour le demandeur PINT, il peut alors clore la session en envoyant un message UNSUBSCRIBE immédiat (voir le paragraphe 3.5.3.3).

En principe, un usager peut envoyer une demande SUBSCRIBE après que le service de réseau téléphonique s'est réalisé. Cela permet, par exemple, de vérifier les "lendemains" pour voir si la télécopie a été bien transmise. Cependant, une passerelle PINT est seulement obligée de conserver l'état sur un appel pour le temps qui a été indiqué précédemment dans un en-tête Expires: envoyé dans la réponse au message INVITE d'origine qui a déclanché la session de service, dans la réponse au message SUBSCRIBE, dans la réponse à tout message UNSUBSCRIBE, ou dans son propre message UNSUBSCRIBE (mais voir le point 3 du paragraphe 3.5.8).

Si le serveur n'a plus d'enregistrement de la session à laquelle un demandeur s'est abonné, il retourne un "606 Non acceptable", avec l'en-tête Warning: 307 approprié indiquant que l'identifiant de session SDP n'est plus valide. Cela signifie qu'un client demandeur qui sait qu'il va vouloir des informations sur l'état d'une session après la fin de la session DEVRAIT envoyer une demande SUBSCRIBE avant que la session ne se termine.

3.5.3.2 Envoi d'indications d'état avec une demande NOTIFY

Durant la période d'abonnement, la passerelle peut, de temps en temps, envoyer une demande NOTIFY spontanée à l'entité indiquée dans l'en-tête Contact: de la demande SUBSCRIBE "d'ouverture". Normalement, ceci va se produire par suite d'un changement dans l'état de la session de service pour laquelle le demandeur s'est abonné.

Le serveur d'agent d'utilisateur receveur DOIT en accuser réception en retournant une réponse finale (normalement un "200 OK"). Dans cette version des extensions à PINT, la passerelle n'est pas obligée de prendre en charge les redirections (codes 3xx) et peut donc les traiter comme un échec.

Donc, si la classe de code de réponse est au-dessus de 2xx, cela peut alors être traité par la passerelle comme un échec de la session de surveillance, et dans cette situation elle va immédiatement tenter de fermer la session (voir le paragraphe suivant).

La demande NOTIFY contient la description de session modifiée. Par exemple, la passerelle peut être capable d'indiquer une heure de début ou de fin plus précise.

La passerelle peut inclure un en-tête Warning: pour décrire un problème d'invocation du service, et peut indiquer dans une ligne i= des informations sur la session de réseau téléphonique elle-même.

Exemple :

```
NOTIFY  sip:petrack@pager.com SIP/2.0
To: sip:petrack@pager.com
From: sip:R2F.pint.com@service.com
Call-ID: 19971205T234505.56.78@pager.com
CSeq: 4711 SUBSCRIBE
Warning: xxx télécopie interrompue, vais réessayer dans une heure.
Content-Type:application/sdp

c=...
i=3 pages sur 5 envoyées
t=...
```

3.5.3.3 Fermeture d'une session de surveillance avec une demande UNSUBSCRIBE

À un certain moment, le serveur d'agent d'utilisateur représentant le client ou la passerelle peut décider de terminer la session de surveillance. Ceci se réalise en envoyant la demande UNSUBSCRIBE au serveur correspondant. Une telle demande indique que l'envoyeur a l'intention de clore immédiatement la session de surveillance et, à réception de la réponse finale du serveur receveur, la session est réputée terminée.

Noter qu'à la différence de la demande SUBSCRIBE, qui n'est jamais envoyée par une passerelle PINT, une demande UNSUBSCRIBE peut être envoyée par une passerelle PINT au serveur d'agent d'utilisateur pour indiquer que la session de

surveillance est close. (Ceci est analogue au fait qu'une passerelle envoie un INVITE, bien qu'elle puisse envoyer un BYE pour indiquer qu'un appel téléphonique s'est terminé.)

Si la passerelle initie la clôture de la session de surveillance en envoyant un message UNSUBSCRIBE, elle DEVRAIT inclure un en-tête "Expires:" montrant pour combien de temps après la fermeture de la session de surveillance il veut mémoriser les informations sur la session de service. Cela constitue une durée minimum pendant laquelle le client peut envoyer un nouveau message SUBSCRIBE pour ouvrir une autre session de surveillance ; après le délai indiqué dans l'en-tête Expires:, la passerelle est libre de disposer de tout enregistrement de la session de service, de sorte que des demandes SUBSCRIBE ultérieures peuvent être rejetées avec une réponse "606".

Si la période d'abonnement spécifiée par le client a expiré, la passerelle peut alors envoyer immédiatement une demande UNSUBSCRIBE au serveur d'agent d'utilisateur représentant du client. Cela assure que la session de surveillance s'achève toujours avec un échange UNSUBSCRIBE/réponse, et que le serveur représentant d'agent d'utilisateur peut éviter de conserver l'état dans certaines circonstances.

3.5.3.4 Rythme des demandes SUBSCRIBE

Comme il s'appuie sur le fait que la passerelle a une copie de la description de session de l'INVITE, le message SUBSCRIBE se limite à quand il peut être produit. La passerelle doit avoir reçu la demande de service à laquelle cette session de surveillance doit être associée, ce qui, du point de vue du client, arrive aussitôt que la passerelle lui a renvoyé une réponse 1xx.

Cependant, une fois que ceci a été fait, il n'y a pas de raisons pour que le client n'envoie pas une demande de surveillance. Il n'a pas à attendre la réponse finale de la passerelle, et il peut certainement envoyer la demande SUBSCRIBE avant d'envoyer le ACK pour la réponse finale de demande de service. Après ce moment, le client est libre d'envoyer une demande SUBSCRIBE quand il le décide, sauf si la réponse finale de la passerelle à la demande de service initiale indiquait un temps d'expiration court dans Expires:.

Cependant, il y a de bonnes raisons (voir le paragraphe 6.4) pour qu'il soit approprié de commencer une session de surveillance immédiatement avant que le service soit confirmé par l'envoi d'un ACK par le client PINT. À ce moment, la passerelle aura décidé si elle peut ou non traiter la demande de service, mais n'aura pas passé la demande au système exécutif. Elle est donc en bonne position pour demander au système exécutif d'activer la surveillance quand elle envoie la demande de service. Dans la mise en œuvre pratique, il est probable que plus d'informations seront disponibles sur l'état de service transitoire si ceci est indiqué comme important AVANT ou LORSQUE commence la phase d'exécution du service ; une fois que l'exécution a commencé, le niveau des informations qui peuvent être retournées peut être difficile à changer.

Donc, bien qu'il soit libre d'envoyer une demande SUBSCRIBE à tout moment après la réception d'une réponse intermédiaire de la passerelle à sa demande de service, il est recommandé que le client envoie une telle demande de surveillance immédiatement avant d'envoyer un message ACK confirmant le service si il est intéressé par les messages d'état de service transitoire.

3.5.4 En-tête "Require:" pour PINT

Les clients PINT utilisent l'en-tête Require: pour signaler au serveur PINT qu'une certaine extension PINT de SIP est exigée. PINT 1.0 définit deux chaînes qui peuvent aller dans l'en-tête Require: :

org.ietf.sip.subscribe -- le serveur peut satisfaire les demandes SUBSCRIBE et les méthodes associées (§ 3.5.3)

org.ietf.sdp.require -- le serveur PINT (ou l'analyseur SDP associé) comprend l'attribut "require" défini au § 3.4.4)

Exemple : Require:org.ietf.sip.subscribe,org.ietf.sdp.require

Un client DEVRAIT n'inclure un en-tête Require: que lorsque il exige vraiment que le serveur rejette la demande si l'option n'est pas prise en charge.

3.5.5 URL PINT dans les demandes PINT

Normalement, les noms d'hôte et les noms de domaine qui apparaissent dans les URL PINT sont une affaire interne de chaque système PINT individuel. Un client utilise la charge utile SDP appropriée pour indiquer le service particulier qu'il souhaite invoquer ; il n'est pas nécessaire d'utiliser un URL particulier pour identifier le service.

Un URL PINT est utilisé de deux façons différentes au sein des demandes PINT : dans l'URI de demande, et dans les en-têtes To: et From:. L'utilisation dans l'URI de demande exige des précisions afin de s'assurer d'un inter fonctionnement en douceur avec le service du réseau téléphonique par l'infrastructure PINT, et c'est ce qui est traité ci-après.

3.5.5.1 URL PINT dans les URI de demande

Il y a certaines occasions où il peut être utile d'indiquer des informations de service au sein de l'URL sous une forme normalisée :

a. il se peut qu'il ne soit pas possible d'utiliser les informations de SDP pour acheminer la demande si elle est chiffrée ;
b. elles permettent une mise en œuvre qui utilise des "indicateurs de service" I.N. ;
c. elles permettrent à plusieurs passerelles PINT en compétition de s'enregistrer auprès d'un seul serveur "courtier" (mandataire ou de redirection) (voir le paragraphe 6.3).

Pour ces raisons, les conventions suivantes pour les URL sont offertes pour être utilisées dans les demandes PINT :

1. La portion utilisateur d'un URL sip indique le service à demander. À présent, les services suivants sont définis :
   R2C (pour Demande d'appel)
   R2F (pour Demande de télécopie)
   R2HC (pour Demande d'écoute du contenu)

   Les portions utilisateur "R2C", "R2F", et "R2HC" sont réservées pour les services de base PINT. Les autres portions utilisateur DOIVENT être utilisées au cas où le service demandé n'est pas un des services de base. Voir au paragraphe 6.2 les considérations concernant les enregistrements par des systèmes PINT concurrents pour un seul serveur mandataire PINT agissant comme un courtier de service.

2. La portion hôte d'un URL sip contient le nom de domaine du fournisseur de service PINT.

3. Un nouveau paramètre "url-parameter" est défini comme étant "tsp" (pour "fournisseur de service téléphonique"). Il peut être utilisé pour indiquer le fournisseur réel de réseau téléphonique à utiliser pour satisfaire la demande PINT.

Donc, par exemple :-

```
INVITE sip:R2C@pint.pintservice.com SIP/2.0
INVITE sip:R2F@pint.pintservice.com;tsp=telco.com SIP/2.0
INVITE sip:R2HC@pint.mycom.com;tsp=pbx23.mycom.com SIP/2.0
INVITE sip:13@pint.telco.com SIP/2.0
```

3.5.6 Paramètres de réseau téléphonique dans les URL PINT

Tout URL SIP légal peut apparaître comme URL PINT au sein de l'URI de demande ou de l'en-tête To: d'une demande PINT. Mais si l'adresse est un numéro de téléphone, on a indiqué au paragraphe 3.4.3 qu'il peut être nécessaire d'inclure plus d'informations afin d'identifier correctement le terminal ou service téléphonique distant. Les clients PINT PEUVENT inclure ces étiquettes d'attribut au sein des URL PINT si elles sont un complément nécessaire ou utile au numéro de téléphone dans l'URL SIP. Ces étiquettes d'attribut DOIVENT être incluses comme paramètres d'URL comme défini dans la [RFC2543] (c'est-à-dire séparées par un caractère point-virgule).

Voici un exemple d'un URL PINT contenant des étiquettes d'attribut supplémentaires :

```
sip:+9725228808@pint.br.com;user=phone;require=Q763-plan;a=Q763-plan:4
```

Comme on l'a noté au paragraphe 3.4.3, ces paramètres d'attribut supplémentaires ne seront normalement pas nécessaires dans un URL, parce que il y a une grande quantité de contexte disponible pour aider le serveur à interpréter correctement le numéro de téléphone. En particulier, il y a l'URL SIP dans l'en-tête To:, et il y a aussi l'URI de demande. Dans la plupart des cas, cela fournit des informations suffisantes pour le réseau téléphonique.

Les attributs SDP définis à la section 3 ne seront normalement utilisés que lorsque ils sont nécessaires pour fournir le contexte nécessaire pour identifier un terminal téléphonique.

3.5.7 Demandes REGISTER dans PINT

Une passerelle PINT est un serveur d'agent d'utilisateur SIP. Un serveur d'agent d'utilisateur utilise la demande REGISTER pour dire à un serveur mandataire ou de redirection qu'il est disponible pour "recevoir des appels" (c'est-à-dire pour servir des demandes). Donc, une passerelle PINT enregistre auprès d'un serveur mandataire ou de redirection le

service qui est accessible à travers lui, tandis que dans SIP, un usager enregistre sa présence auprès d'un serveur SIP particulier.

Il peut y avoir des serveurs PINT en concurrence pouvant offrir le même service PINT qui essayent de s'enregistrer auprès d'un seul serveur PINT. Le serveur PINT peut agir comme "courtier" entre les diverses passerelles PINT qui peuvent satisfaire une demande. Un format pour les URL PINT a été spécifié au paragraphe 3.5.5 qui permet à des systèmes PINT indépendants d'enregistrer une offre de fournir le même service. Le registraire peut appliquer ses propres mécanismes et politiques pour décider comment répondre aux INVITE des clients qui recherchent le service (voir au paragraphe 6.3 des options de déploiement possibles). Il n'y a pas de changement entre la sémantique ou la syntaxe de SIP et du REGISTER de PINT.

Bien sûr, les informations dans les URL PINT dans la demande REGISTER peuvent n'être pas suffisantes pour définir complètement le service que peut offrir une passerelle. L'utilisation de SIP et SDP dans les demandes REGISTER de PINT pour permettre à une passerelle de spécifier plus en détails les services qu'il peut offrir fera l'objet d'études ultérieures.

3.5.8 Demandes BYE dans PINT

La sémantique des demandes BYE au sein de PINT requiert des précisions supplémentaires. Une question concerne les conférences qui "ne peuvent pas se terminer", et l'autre concerne la conservation de l'état d'appel après le BYE.

La demande BYE [RFC2543] est normalement utilisée pour indiquer que l'entité d'origine ne souhaite plus être impliquée dans l'appel spécifié. La demande termine l'appel et la session support. Appliquer ce modèle à PINT, si le client PINT fait une demande qui résulte en l'invocation d'un appel téléphonique de A à B, une demande BYE de la part du client, si elle est acceptée, devrait résulter en la terminaison de l'appel téléphonique.

On peut s'attendre à ce que ce soit le cas si l'appel téléphonique n'a pas commencé lorsque la demande BYE est reçue. Par exemple, si une demande de télécopie est envoyée avec une ligne t= indiquant que la télécopie est à envoyer demain à 4 h, le demandeur peut souhaiter annuler la demande avant l'heure spécifiée.

Cependant, même si l'appel a déjà commencé, il peut n'être pas possible de terminer la session support sur le côté du système téléphonique. Par exemple, l'appel de télécopie peut être en cours lorsque le BYE arrive, et peut-être qu'il n'est tout simplement pas possible d'annuler la télécopie en session. Une autre possibilité est que le service côté téléphone entier puisse être terminé avant la réception du BYE. Dans l'exemple ci-dessus de demande de télécopie, le BYE peut être envoyé le matin suivant, et la télécopie entière a été envoyée avant que le BYE ait été reçu. Il est trop tard pour envoyer le BYE.

Dans le cas où le réseau téléphonique ne peut pas terminer l'appel, le serveur DOIT retourner au BYE une réponse "606 Non acceptable", avec une description de session qui indique la session de réseau téléphonique qui cause le problème.

Donc, dans PINT, une réponse "Non acceptable" PEUT être retournée aux demandes INVITE aussi bien que BYE. Elle indique qu'un certain aspect de la description de session rend la demande inacceptable.

En permettant à un serveur de retourner une réponse "Non acceptable" aux demandes BYE, on n'en change pas la sémantique, on en élargit juste l'utilisation.

Une combinaison d'en-têtes Warning: et de lignes i= au sein de la description de session peut être utilisée pour indiquer la nature précise du problème.

Exemple :

```
SIP/2.0 606 Non acceptable
From: ...
To: .....
.....
Warning: 399 pint.mycom.com Télécopie en cours, le service ne peut être interrompu
Content-Type: application/sdp
Content-Length: ...
v=0
...
...
i=3 pages sur 5 bien envoyées
c=TN  RFC2543  +12014064090
m=image 1 fax tif
a=fmtp:tif uri:http://tifsRus.com/yyyyyy.tif
```

Noter que le serveur peut aussi bien retourner une description de session mise à jour dans une réponse de succès à un BYE. Cela peut être utilisé, par exemple, pour indiquer les heures réelles de début et de fin de la session téléphonique, ou combien de pages ont été envoyées dans la transmission de télécopie.

La seconde question concerne la durée de conservation de l'état d'appel par un serveur après la réception d'un BYE. Une question se pose parce que les autres clients peuvent quand même souhaiter envoyer des interrogations sur la session de réseau téléphonique qui a été l'objet de la transaction PINT. La sémantique SIP ordinaire a trois importantes implications pour cette situation :

1. Un BYE indique que le client demandeur va éliminer tous les état d'appel aussitôt qu'il aura reçu une réponse de succès. Un client NE DEVRAIT PAS envoyer de demande SUBSCRIBE après avoir envoyé un BYE.

2 Un serveur peut retourner un en-tête Expires: dans une réponse de succès à une demande BYE. Cela indique pendant combien de temps un serveur va conserver l'état de session concernant la session de réseau téléphonique. À tout moment durant cette période, un client peut envoyer une demande SUBSCRIBE au serveur pour connaître l'état de la session (bien que, comme expliqué au paragraphe précédent, un client qui a envoyé un BYE ne va normalement pas envoyer de SUBSCRIBE).

3. Lorsque ils sont engagés dans une session de surveillance SUBSCRIBE/NOTIFY, les serveurs PINT qui envoient UNSUBSCRIBE à un URL mentionné dans l'en-tête Contact: d'une demande d'un client NE DEVRAIENT PAS éliminer l'état de session tant qu'ils n'ont pas reçu la réponse réussie au message UNSUBSCRIBE. Par exemple, il se peut que l'hôte du client demandeur soit débranché (ou en mode sommeil) lorsque le service téléphonique est exécuté (et n'est donc pas disponible à la localisation précédemment spécifiée dans l'attribut Contact:) pour recevoir le UNSUBSCRIBE du serveur PINT. Bien sûr, il est possible que la demande UNSUBSCRIBE arrive simplement à expiration.

4. Exemples de demandes et réponses PINT

4.1 Demande à un centre d'appel d'un utilisateur anonyme pour recevoir un appel téléphonique

```
C->S : INVITE  sip:R2C@pint.mailorder.com  SIP/2.0
       Via: SIP/2.0/UDP 169.130.12.5
       From: sip:anon-1827631872@chinet.net
       To: sip:+1-201-456-7890@iron.org;user=phone
       Call-ID: 19971205T234505.56.78@pager.com
       CSeq: 4711 INVITE
       Subject: Soldes sur les planches à repasser
       Content-type: application/sdp
       Content-Length: 174

       v=0
       o=- 2353687637 2353687637 IN IP4 128.3.4.5
       s=R2C
       i=Promotion sur les planches à repasser
       e=anon-1827631872@chinet.net
       t=2353687637 0
       m=audio 1  voice -
       c=TN  RFC2543  +1-201-406-4090
```

Dans cet exemple, le contexte qui est d'exiger d'interpréter l'adresse To: comme un numéro de téléphone n'est pas donné explicitement ; il est implicitement connu du serveur R2C@pint.mailorder.com. Mais le téléphone de la personne qui souhaite recevoir l'appel est explicitement identifié comme un numéro E.164 internationalement significatif qui tombe dans le plan de numérotage d'Amérique du Nord (à cause du "+1" dans la ligne c=).

4.2 Demande d'un consommateur nominatif (John Jones) de recevoir un appel téléphonique d'une vendeuse particulière (Mary James) concernant la planche à repasser défectueuse qu'il a acheté

```
C->S: INVITE  sip:marketing@pint.mailorder.com  SIP/2.0
```

Via: SIP/2.0/UDP 169.130.12.5
From: sip:john.jones.3@chinet.net
To: sip:mary.james@mailorder.com
Call-ID: 19971205T234505.56.78@pager.com
CSeq: 4712 INVITE

Subject: Planche à repasser défectueuse – demande de remboursement
Content-type: application/sdp
Content-Length: 150

v=0
o=- 2353687640 2353687640 IN IP4 128.3.4.5
s=marketing
e=john.jones.3@chinet.net
c= TN RFC2543 +1-201-406-4090
t=2353687640 0
m=audio 1 voice -

La ligne To: pourrait inclure le numéro de téléphone de Mary James au lieu d'une adresse en forme de messagerie électronique. Une mise en œuvre qui ne peut pas accepter des URL en forme d'adresse de messagerie électronique doit décliner la demande avec un 606 Non acceptable. Noter que le client PINT envoyeur "sait" que la passerelle PINT contactée avec l'URI de demande "marketing@pint.mailorder.com" est capable de traiter la demande du client comme prévu (Voir le paragraphe 3.5.5.1 pour la discussion de ce point).

Noter aussi qu'un tel service d'appel téléphonique pourrait être mis en œuvre sur le côté téléphone avec des détails différents. Par exemple, il se pourrait que d'abord, le téléphone de l'agent sonne, et qu'ensuite le téléphone du consommateur sonne, ou il se pourrait que d'abord ce soit le téléphone du consommateur qui sonne et qu'il entende une musique stupide jusqu'à ce que l'agent vienne en ligne. Si nécessaire, de tels détails des paramètres de service pourraient être indiqués dans des lignes d'attribut "a=" au sein de la description de session. La spécification de telles lignes d'attribut pour la cohérence du service sort du domaine d'application de la spécification de PINT 1.0.

4.3 Demande du même usager de recevoir en retour une télécopie expliquant l'assemblage de la planche à repasser

C->S: INVITE sip:faxback@pint.mailorder.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
From: sip:john.jones.3@chinet.net
To: sip:1-800-3292225@steam.edu;user=phone;phone-context=+1
Call-ID: 19971205T234505.66.79@chinet.net
CSeq: 4713 INVITE
Content-type: application/sdp
Content-Length: 218

v=0
o=- 2353687660 2353687660 IN IP4 128.3.4.5
s=faxback
e=john.jones.3@chinet.net
t=2353687660 0
m=application 1 fax URI

c=TN RFC2543 1-201-406-4091
a=fmtp:URI uri:http://localstore/Products/IroningBoards/2344.html

Dans cet exemple, la télécopie à envoyer est mémorisée dans un serveur local (localstore), dont le nom peut être seulement résoluble, ou peut seulement être accessible, de l'intérieur du réseau IP sur lequel le serveur PINT se tient. Le numéro de téléphone à taper est aussi un "numéro de téléphone local". Il n'y a pas d'attribut "phone-context", de sorte que le contexte (dans ce cas, pour quel pays le numéro est "nationalement significatif") doit être fourni par le serveur PINT faxback@pint.mailorder.com.

Si le serveur qui le reçoit ne comprend pas le numéro, il DEVRAIT décliner la demande et inclure un avertissement "Adresse réseau non comprise". Noter qu'aucun attribut "require" n'a été utilisé ici, car il est très probable que la demande

peut être servie même par un serveur qui ne prend pas en charge l'attribut "require".

4.4 Demande du même usager d'avoir les mêmes informations lues au téléphone

```
C->S: INVITE  sip:faxback@pint.mailorder.com  SIP/2.0
    Via: SIP/2.0/UDP 169.130.12.5
    From: sip:john.jones.3@chinet.net
    To: sip:1-800-3292225@steam.edu;user=phone;phone-context=+1
    Call-ID: 19971205T234505.66.79@chinet.net
    CSeq: 4713 INVITE
    Content-type: application/sdp
    Content-Length: 220

    v=0
    o=- 2353687660 2353687660 IN IP4 128.3.4.5
    s=faxback
    e=john.jones.3@chinet.net
    t=2353687660 0
    m=application 1 voice URI
    c=TN  RFC2543  1-201-406-4090
    a=fmtp:URI uri:http://localstore/Products/IroningBoards/2344.html
```

4.5 Demande d'envoi d'une page de texte incluse sur le mobile d'un ami

Dans cet exemple, le texte à envoyer est inclus dans la demande.

```
C->S: INVITE  sip:R2F@pint.pager.com  SIP/2.0
    Via: SIP/2.0/UDP 169.130.12.5
    From: sip:scott.petrack@chinet.net
    To: sip:R2F@pint.pager.com
    Call-ID: 19974505.66.79@chinet.net
    CSeq: 4714 INVITE

    Content-Type: multipart/related; boundary=--next

    ----next
    Content-Type: application/sdp
    Content-Length: 236
    v=0
    o=- 2353687680 2353687680 IN IP4 128.3.4.5
    s=R2F
    e=scott.petrack@chinet.net
    t=2353687680 0
    m=text 1 pager plain
    c= TN  RFC2543  +972-9-956-1867
    a=fmtp:plain spr:2@53655768

    ----next
    Content-Type: text/plain
    Content-ID: 2@53655768
    Content-Length:50

    Hé Joe ! S'il te plait, appelle moi aussitôt que possible au 555-1234.

    ----next--
```

4.6 Demande d'envoi d'une image par télécopie au numéro de téléphone +972-9-956-1867

```
C->S: INVITE  sip:faxserver@pint.vocaltec.com  SIP/2.0
    Via: SIP/2.0/UDP 169.130.12.5
```

From: sip:scott.petrack@chinet.net
To: sip:faxserver@pint.vocaltec.com
Call-ID: 19971205T234505.66.79@chinet.net
CSeq: 4715 INVITE
Content-type: application/sdp
Content-Length: 267

v=0
o=- 2353687700 2353687700 IN IP4 128.3.4.5
s=faxserver
e=scott.petrack@chinet.net
t=2353687700 0
m=image 1 fax tif gif
c= TN RFC2543 +972-9-956-1867
a=fmtp:tif uri:http://petrack/images/tif/picture1.tif
a=fmtp:gif uri:http://petrack/images/gif/picture1.gif

L'image est disponible comme tif ou comme gif. Le tif est le format préféré. Noter que le serveur http où réside l'image est local, et le serveur PINT est aussi local (parce qu'il peut résoudre le nom de machine "petrack")

4.7 Demande de lecture au téléphone de deux éléments de contenu à la suite

D'abord, du texte inclus est lu par du texte-en-parole. Puis est lu du texte mémorisé sur un URI sur l'Internet.

C->S: INVITE sip:R2HC@pint.acme.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
From: sip:scott.petrack@chinet.net
To: sip:R2HC@pint.acme.com
Call-ID: 19974505.66.79@chinet.net
CSeq: 4716 INVITE
Content-Type: multipart/related; boundary=next

--next
Content-Type: application/sdp
Content-Length: 316
v=0
o=- 2353687720 2353687720 IN IP4 128.3.4.5
s=R2HC
e=scott.petrack@chinet.net

c= TN RFC2543 +1-201-406-4091
t=2353687720 0
m=text 1 voice plain
a=fmtp:plain spr:2@53655768
m=text 1 voice plain
a=fmtp:plain uri:http://www.your.com/texts/stuff.doc

--next
Content-Type: text/plain
Content-ID: 2@53655768
Content-Length: 172

Hello!! Je suis sur le point de vous lire le document que vous demandez, "uri:http://www.your.com/texts/stuff.doc".
Nous espérons que vous aimerez le nouveau serveur de synthèse de la parole de acme.com.
--next--

4.8 Demande des prix du RNIS à envoyer à mon télécopieur

INVITE sip:R2FB@pint.bt.co.uk SIP/2.0 Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-12347-01@pint.bt.co.uk;user=phone;phone-context=+44

```
From: sip:hank.wangford@newts.demon.co.uk
Call-ID: 19981204T201505.56.78@demon.co.uk
CSeq: 4716 INVITE
Subject: Catalogue des prix
Content-type: application/sdp
Content-Length: 169

v=0
o=- 2353687740 2353687740 IN IP4 128.3.4.5
s=R2FB
i=Catalogue des prix RNIS
e=hank.wangford@newts.demon.co.uk
t=2353687740 0
m=text 1  fax -
c=TN  RFC2543  +44-1794-8331010
```

4.9 Demande de rappel

```
INVITE sip:R2C@pint.bt.co.uk  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-123456@pint.bt.co.uk;user=phone;phone-context=+44
From: sip:hank.wangford@newts.demon.co.uk
Call-ID: 19981204T234505.56.78@demon.co.uk
CSeq: 4717 INVITE
Subject: Combien ça coûte ?
Content-type: application/sdp
Content-Length: 176

v=0
o=- 2353687760 2353687760 IN IP4 128.3.4.5
s=R2C
i=Question sur les tarifs RNIS
e=hank.wangford@newts.demon.co.uk
c=TN  RFC2543  +44-1794-8331013
t=2353687760 0
m=audio 1  voice -
```

4.10 Envoi d'un ensemble d'informations en réponse à une enquête

```
INVITE sip:R2FB@pint.bt.co.uk  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-12347-01@pint.bt.co.uk;user=phone;phone-context=+44
From: sip:colin.masterton@sales.hh.bt.co.uk
Call-ID: 19981205T234505.56.78@sales.hh.bt.co.uk
CSeq: 1147 INVITE
Subject: Informations sur les prix, comme demandé
Content-Type: multipart/related; boundary=next

--next
Content-type: application/sdp
Content-Length: 325
v=0
o=- 2353687780 2353687780 IN IP4 128.3.4.5
s=R2FB
i=Vos documents
e=colin.masterton@sales.hh.bt.co.uk
t=2353687780 0
m=application 1  fax octet-stream
c=TN  RFC2543  +44-1794-8331010
a=fmtp:octet-stream uri:http://www.bt.co.uk/imgs/pipr.gif opr:
```

spr:2@53655768

--next
Content-Type: text/plain
Content-ID: 2@53655768
Content-Length: 352

Cher Monsieur,
Merci de votre demande. J'ai vérifié la disponibilité dans votre zone, et nous pouvons desservir votre domicile. Je vous joins le tarif des coûts d'installation, ainsi que les frais de location de la ligne. Si vous êtes d'accord avec cette proposition, prière de noter la référence ci-jointe : isdn/hh/123.45.9901.
Sincèrement votre,
Colin Masterton
--next--

Noter que dans cet exemple le contenu de retour de télécopie "implicite" est donné par une référence opaque VIDE dans le milieu de la ligne fmtp.

4.11 Message des "titres" de la chaîne sportive envoyés à votre téléphone/mobile/télécopieur

(i) téléphone

```
INVITE sip:R2FB@pint.wwos.skynet.com  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To:
sip:1-900-123-456-7@wwos.skynet.com;user=phone;phone-context=+1
From: sip:fred.football.fan@skynet.com
Call-ID: 19971205T234505.56.78@chinet.net
CSeq: 4721 INVITE
Subject: Scores finaux de la NFL par Le monde merveilleux des sports
Content-type: application/sdp
Content-Length: 220

v=0
o=- 2353687800 2353687800 IN IP4 128.3.4.5
s=R2FB
i=Scores finaux de la NFL
e=fred.football.fan@skynet.com
c=TN  RFC2543 +44-1794-8331013
t=2353687800 0
m=audio 1 voice x-pay
a=fmtp:x-pay opr:mci.com/md5:<crypto signature>
```

(ii) télécopie

```
INVITE sip:R2FB@pint.wwos.skynet.com  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:1-900-123-456-7@wwos.skynet.com;user=phone; phone-context=+1
From: sip:fred.football.fan@skynet.com
Call-ID: 19971205T234505.56.78@chinet.net
CSeq: 4722 INVITE
Subject: Scores finaux de la NFL par Le monde merveilleux des sports
Content-type: application/sdp
Content-Length: 217

v=0
o=- 2353687820 2353687820 IN IP4 128.3.4.5
s=R2FB
i=Scores finaux de la NFL
e=fred.football.fan@skynet.com
c=TN  RFC2543 +44-1794-8331010
t=2353687820 0
m=text 1 fax x-pay
```

a=fmtp:x-pay opr:mci.com/md5:<crypto signature>

(iii) pager

INVITE sip:R2FB@pint.wwos.skynet.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:1-900-123-456-7@wwos.skynet.com;user=phone; phone-context=+1
From: sip:fred.football.fan@skynet.com
Call-ID: 19971205T234505.56.78@chinet.net
CSeq: 4723 INVITE
Subject: Scores finaux de la NFL par Le monde merveilleux des sports
Content-type: application/sdp
Content-Length: 219

v=0
o=- 2353687840 2353687840 IN IP4 128.3.4.5
s=R2FB
i=Scores finaux de la NFL
e=fred.football.fan@skynet.com
c=TN RFC2543 +44-1794-8331015
t=2353687840 0
m=text 1 pager x-pay
a=fmtp:x-pay opr:mci.com/md5:<crypto signature>

Noter que tous sont TRÈS similaires.

4.12 Envoi automatique d'une télécopie de votre facture de téléphone à quelqu'un

INVITE sip:BillsRUs@pint.sprint.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:+1-555-888-1234@fbi.gov;user=phone
From: sip:agent.mulder@fbi.gov
Call-ID: 19991231T234505.56.78@fbi.gov
CSeq: 911 INVITE
Subject: Facturation détaillée pour janvier 1998
Content-type: application/sdp
Content-Length: 247

v=0
o=- 2353687860 2353687860 IN IP4 128.3.4.5
s=BillsRUs
i=Joe Pendleton's Phone Bill
e=agent.mulder@fbi.gov
c=TN RFC2543 +1-202-833-1010
t=2353687860 0
m=text 1 fax x-files-id
a=fmtp:x-files-id opr:fbi.gov/jdcn-123@45:3des;base64,<signature>

Note : Dans ce cas, la référence opaque est une collection de données utilisées pour convaincre le système exécutif que le demandeur a le droit d'obtenir des informations, plutôt que de choisir le contenu particulier (la partie A dans le champ To: de "l'enveloppe" SIP fait cela seule).

5. Considérations sur la sécurité

5.1 Principes de base de l'utilisation de PINT

Une passerelle PINT, et le ou les systèmes exécutifs avec lesquels cette passerelle est associée, existent pour fournir des services aux demandeurs PINT. Le but du protocole PINT est de passer les demandes de ces utilisateur à une passerelle PINT afin qu'un système exécutif associé puisse servir ces demandes.

5.1.1 Responsabilité des demandes de service

La facilité de passer un appel fondé sur le GSTN à des numéros spécifiés dans la demande PINT se fait cependant avec certains risques. La demande peut spécifier un numéro de téléphone ou de télécopie incorrect. Il est aussi possible que le demandeur ait volontairement entré le numéro de téléphone d'un tiers innocent. Finalement, la demande peut avoir été interceptée sur son chemin à travers une infrastructure PINT ou SIP intermédiaire, et la demande peut avoir été altérée.

Dans tous ces cas, le résultat peut être qu'un appel est incorrectement passé. Qu'il y ait intention ou négligence, cela peut être construit comme un harcèlement de la personne qui reçoit l'appel incorrect. Bien que le cadre réglementaire des abus de connexions Internet diffère tout autour du monde et ne soit pas toujours mûr, les règles selon lesquelles sont passés les appels GSTN sont beaucoup plus établies. On peut être poursuivi pour des appels erronés ou incorrects.

On peut comprendre que les opérateurs du GSTN préfèreraient que ce quelqu'un ne soit pas eux, de sorte qu'ils vont avoir besoin de s'assurer que toute combinaison de passerelle PINT et de système exécutif ne génère pas des appels incorrects à travers quelque erreur dans la passerelle ou dans la mise en œuvre de système exécutif ou une faute interne des communications GSTN. Également, il est important que l'opérateur puisse montrer qu'il n'agit que sur des demandes dont il a de bonnes raisons de penser qu'elles sont correctes. Cela signifie que la passerelle ne doit passer de demandes que si elle est sûre qu'elles n'ont pas été corrompues dans le transit depuis le demandeur.

Si on peut montrer qu'une demande vient d'un certain demandeur et qu'elle a été traitée de bonne foi par le fournisseur de service PINT, la responsabilité des demandes peut bien retomber sur le demandeur plutôt que sur l'opérateur qui a exécuté ces demandes.

Finalement, il peut être important pour le fournisseur de service PINT d'être capable de montrer qu'il n'agit que sur les demandes pour lesquelles il a un certain degré d'assurance de l'origine. Dans de nombreuses juridictions, il est exigé des opérateurs GSTN qu'ils ne passent les appels que s'ils peuvent, si c'est exigé, identifier les parties à l'appel (comme lorsque ils sont requis d'effectuer le suivi des appels malveillants). Il est au moins probable que le fournisseur de services PINT se verra confier une responsabilité similaire.

Il s'ensuit que le fournisseur de service PINT peut demander que l'identité du demandeur soit confirmée. Si une telle confirmation n'est pas disponible, il peut alors être obligé (ou avoir le choix) de ne pas fournir le service. Cette identification peut requérir une authentification personnelle de l'usager demandeur.

5.1.2 Autorité pour faire les demandes

Lorsque des ressources du GSTN sont utilisées pour fournir un service PINT, il est au moins possible que quelqu'un doive le payer. Cette personne peut n'être pas le demandeur, comme, par exemple, dans le cas des services de partage de charge existants sur le GSTN comme le libre appel dans lequel c'est le receveur d'un appel et non celui qui fait l'appel qui supporte le coût de l'appel.

Ce n'est, bien sûr, pas la seule possibilité ; par exemple, le service PINT peut être fourni par abonnement, et il y a bien d'autres modèles. Cependant, quel que soit le modèle choisi, il peut y avoir l'exigence que l'autorité d'un demandeur à faire la demande PINT soit confirmée.

Si une telle confirmation n'est pas disponible, là encore, la passerelle PINT et le système exécutif associé peuvent choisir de ne pas fournir le service.

5.1.3 Confidentialité

Même si l'identité de l'usager demandeur et l'autorité sous laquelle il fait sa demande sont connues, il reste la possibilité que la demande soit corrompue, altérée par malveillance, ou même remplacée dans le transit entre le demandeur et la passerelle PINT.

De façon similaire, les informations sur l'autorité sous laquelle une demande est faite peuvent bien être portées au sein de cette demande. Ce peuvent être des informations sensibles, car un espion pourrait les voler et les utiliser dans ses propres demandes. Une telle autorité DEVRAIT être traitée comme si c'étaient des informations financières (comme un numéro de carte de crédit ou un PIN).

Les données qui autorisent un usager demandeur à faire une demande PINT devraient n'être connues que de lui et du fournisseur de service. Cependant, ces informations peuvent être sous une forme qui ne correspond pas aux schémas normalement utilisés dans l'Internet. Par exemple, les certificats X.509 [RFC2459] sont couramment utilisés pour des transactions sécurisées sur l'Internet à la fois dans l'architecture de sécurité IP [RFC2246] et dans le protocole TLS [RFC2401], mais le fournisseur GSTN peut seulement mémoriser un code de compte et un PIN (c'est-à-dire une chaîne

fixée de numéros).

Un usager demandeur peut raisonnablement s'attendre à ce que ses demandes de service soient confidentielles. Pour certains services PINT, aucun contenu n'est porté sur l'Internet ; cependant, les numéros de téléphone ou de télécopie des parties à des appels de service résultants peuvent être considérés comme sensibles. Il en résulte qu'il est probable que le demandeur (et son fournisseur de service PINT) va exiger que toute demande de cette sorte qui est envoyée à travers l'Internet soit protégée contre l'espionnage ; en bref, la demandes DEVRAIT être chiffrée.

5.1.4 Implications de confidentialité de SUBSCRIBE/NOTIFY

Certaines considérations particulières se rapportent aux sessions de surveillance qui utilisent les messages SUBSCRIBE et NOTIFY. Le message SUBSCRIBE qui est utilisé pour enregistrer un intérêt pour la disposition d'une transaction de service PINT utilisent la description de session d'origine portée dans le message INVITE qui s'y rapporte. La présente spécification n'interdit pas la source d'un tel message SUBSCRIBE, de sorte qu'il est possible à un espion de capturer une description de session non protégée et de l'utiliser dans une demande SUBSCRIBE ultérieure. De cette façon, il est possible de découvrir sur cette transaction des détails qui pourraient bien être considérés comme sensibles.

La solution initiale à ce risque est de recommander qu'une description de session qui peut être utilisée dans un message SUBSCRIBE ultérieur DEVRAIT être protégée.

Cependant, il y a un autre risque ; si le champ Origine utilisé est "devinable" il serait alors possible à un attaquant de reconstruire la description de session et d'utiliser cette reconstruction dans un message SUBSCRIBE.

SDP (voir la section 6 de la [RFC2327], champ "o=") ne spécifie pas le mécanisme utilisé pour générer le champ sess-id, et suggère que pourrait être utilisée une méthode fondée sur des horodatages produits par le protocole de l'heure du réseau [RFC1305]. Ceci est suffisant pour garantir l'unicité, mais peut permettre de deviner une valeur, en particulier si d'autres demandes non protégées de même origine sont disponibles.

Donc, pour assurer que l'identifiant de session n'est pas devinable, la techniques décrite au paragraphe 6.3 de la [RFC1750] peut être utilisée pour générer le champ Origine d'une description de session à utiliser dans un message PINT INVITE. Si toutes les demandes (et réponses) d'une entité PINT demandeuse particulière sont protégées, cela n'est alors pas nécessaire. Lorsque une telle situation n'est pas assurée, ET lorsque la surveillance de session est prise en charge, on DEVRAIT alors utiliser une méthode pour rendre non devinable le champ Origine dans une description de session.

5.2 Procédures d'enregistrement

Un nombre quelconque de passerelles PINT peut s'enregistrer pour fournir le même service ; ceci est indiqué par les passerelles qui spécifient la même partie "userinfo" dans le champ d'en-tête To: de la demande REGISTER. Bien qu'une telle ambiguïté ait peu de chances de se produire avec les scénarios couvert pas le SIP "de base", elle est très probable pour PINT ; il pourrait y avoir un nombre quelconque de fournisseurs de service voulant tous prendre en charge un service de "Demande de télécopie", par exemple.

Sauf si une demande spécifie explicitement le nom de passerelle, un mandataire intermédiaire qui agit sur une base de données d'enregistrement à laquelle plusieurs passerelles se sont toutes enregistrées est en position de choisir entre les enregistrants en utilisant un algorithme de son choix ; en principe, toute passerelle qui s'est enregistrée comme "R2F" serait appropriée.

Cependant, cela ouvre un boulevard aux attaques, et c'est dans un de ceux-là que se tient un opérateur de passerelle "pirate" pour faire ses mauvais coups. La procédure SIP standard pour délivrer un enregistrement est d'envoyer une demande REGISTER avec un champ Contact ayant une valeur de caractère générique et un paramètre expires d'une valeur de 0. Il est important qu'un registraire PINT utilise l'authentification de l'enregistrant, car autrement un fournisseur de service PINT serait capable d'usurper l'identité d'un autre et de retirer son enregistrement. Comme cela empêcherait le mandataire de passer les demandes à ce fournisseur, cela augmenterait les demandes envoyées au pirate et arrêterait les demandes adressées à la victime.

Une autre variante de cette attaque serait d'enregistrer une passerelle en utilisant un nom qui a été enregistré par un autre fournisseur ; un opérateur pirate pourrait alors enregistrer sa passerelle comme "R2C@pint.att.com", capturant ainsi les demandes.

La solution est la même ; tous les enregistrements par les passerelles PINT DOIVENT être authentifiés ; cela inclut les nouveaux enregistrements et les remplacements apparents, et toute annulation d'enregistrement actuel. Cette

recommandation est aussi faite dans la spécification SIP, mais pour le fonctionnement correct de PINT, elle est bien sûr très importante.

5.3 Mécanismes de sécurité et implications sur le service PINT

PINT est un ensemble d'extensions à SIP [RFC2543] et à SDP [RFC2327], et va utiliser les procédures de sécurité décrites dans SIP. Cela a plusieurs implications, et elles sont traitées ici.

Pour plusieurs des services PINT, le champ d'en-tête To: de SIP est utilisé pour identifier une des parties au service d'appel résultant. Le service PINT Demande d'appel en est un exemple. Comme mentionné dans la spécification SIP, ce champ est utilisé pour acheminer les messages SIP à travers une infrastructure de serveurs, de redirection et mandataires, entre les serveurs d'agent d'utilisateur correspondants, et il ne peut donc pas être chiffré. Cela signifie que, bien que la majorité des données personnelles ou sensibles puisse être protégée lors du transit, le numéro de téléphone (ou de télécopie) de l'une des parties à un appel de service PINT ne le peut pas, et sera "visible" à toute interception. Pour les services de base PINT, cela peut être acceptable, car le nom de l'appelant dans le service To: est normalement une adresse "bien connue" de fournisseur, comme un centre d'appel.
Un autre aspect de cette question est que, même si l'usager demandeur ne considère pas les numéros de téléphone ou télécopie des parties à un service PINT comme confidentielles, ces parties le pourraient. Lorsque des serveurs PINT ont des raisons de penser que ce pourrait être le cas, elles DEVRAIENT chiffrer la demande, même si le demandeur ne l'a pas fait. Cela pourrait arriver, par exemple, si un usager demandeur dans une société a passé une demande PINT et qu'elle a été portée via l'Intranet de la société à leur mandataire/pare-feu et ensuite sur l'Internet jusqu'à une passerelle PINT située à un autre endroit.

Si une demande porte des données qui peuvent être réutilisées par un espion soit pour "usurper l'identité" du demandeur, soit pour obtenir un service PINT en insérant le jeton d'autorisation du demandeur dans une demande de l'espion, ces données DOIVENT alors être protégées. Ceci est particulièrement important si le jeton d'autorisation consiste en un texte statique (tel qu'un code de compte et/ou un PIN).

Une approche est de chiffrer la totalité de la demande, en utilisant les méthodes décrites dans la spécification SIP. Autrement, il peut être acceptable que le jeton d'autorisation soit détenu comme une référence opaque (voir le paragraphe 3.4.2.3 et les exemples 4.11 et 4.12) en utilisant des schémas propriétaires sur lesquels s'accordent le demandeur et le fournisseur du service PINT, pour autant qu'ils soient résistants à l'interception et la réutilisation. Aussi, il se peut que le jeton d'autorisation ne puisse pas être utilisé en dehors d'une demande cryptographiquement signée par le demandeur ; si il en est ainsi, cette exigence peut alors être assouplie, car dans ce cas, le jeton ne peut pas être réutilisé. Cependant, sauf si le demandeur et la passerelle sont tous deux assurés que c'est le cas, tout jeton d'autorisation DOIT être traité comme sensible, et DOIT donc être chiffré.

Une demande PINT peut contenir des données dans le corps de message SDP qui peuvent être utilisées plus efficacement pour acheminer cette demande. Par exemple, il se peut qu'une combinaison de passerelle et de système exécutif ne puisse pas traiter une demande qui spécifie une des parties comme un pageur, tandis que l'autre le peut. Les deux passerelles peuvent s'être enregistrées auprès d'un registraire PINT/SIP, et cette information peut être disponible pour des mandataires PINT/SIP intermédiaires. Cependant, si le corps de message est chiffré, la demande ne peut alors pas être décodée chez le serveur mandataire, et donc la sélection de passerelle fondée sur les informations contenues ne peut pas y être faite.

Il en résulte que le mandataire peut livrer la demande à une passerelle qui ne peut pas la traiter ; cela implique qu'un mandataire PINT/SIP DEVRAIT considérer que son choix de la passerelle appropriée est sujet à correction, et, à réception d'un rejet 501 ou 415 de la part de la première passerelle choisie, en essayer une autre. De cette façon, la demande va réussir si cela est possible, même si elle peut être retardée (et lier des ressources dans des passerelles inappropriées).

Cela ouvre une opportunité intéressante au déni de service ; envoyer une demande valide qui paraît être convenable pour un certain nombre de passerelles différentes, et occuper simplement des passerelles à déchiffrer un message demandant un service qu'elles ne peuvent pas fournir. Comme mentionné au paragraphe 3.5.5.1, le choix d'un nom de service à passer dans la portion userinfo de l'URI de demande SIP est souple, et il est RECOMMANDÉ que les noms soient choisis pour permettre à un mandataire de choisir une passerelle appropriée sans avoir à examiner la partie de corps SDP. Donc, dans l'exemple donné ici, le service pourrait être appelé "Request-To-Page" ou "R2P" plutôt que l'utilisation plus générale de "R2F", si il y a une possibilité que la partie de corps SDP soit protégée durant le transit.

Une variante de cette attaque est de produire une demande qui est syntaxiquement invalide mais qui, du fait du chiffrement, ne peut être détectée sans dépenser des ressources pour la décoder. Les effets de cette forme d'attaque peuvent être minimisés de la même façon que pour toute invitation SIP ; le mandataire devrait détecter le rejet 400 retourné de la passerelle initiale, et ne pas passer la demande à une autre.

Finalement, on note que l'usager demandeur peut n'avoir pas de relation antérieure avec une passerelle PINT, bien qu'il ait eu des relations antérieures avec l'opérateur du système exécutif qui satisfait à ses demandes. Il peut donc y avoir deux niveaux d'authentification et d'autorisation ; un effectué en utilisant les techniques décrites dans la spécification SIP (à utiliser entre le demandeur et la passerelle) et l'autre utilisé entre l'usager demandeur ou le demandeur et le système exécutif.

Par exemple, l'usager demandeur peut avoir un compte chez le fournisseur de service PINT. Ce fournisseur pourrait exiger que les demandes incluent cette identité avant qu'ils soient convaincus de fournie le service. De plus, pour contrer les attaques contre la demande pendant qu'elle est en transit à travers l'Internet, la passerelle peut exiger une certification de la demande séparée fondée sur X.509. Ce sont deux procédures séparées, et les données nécessaires pour la première seraient normalement supposées être contenues dans des références opaques au sein de la partie de corps SDP de la demande.

Le fonctionnement détaillé de ce mécanisme est, par définition, en dehors du domaine d'application d'un protocole de l'Internet, et doit donc être considéré comme une affaire privée. Cependant, une approche pour indiquer au demandeur qu'une telle authentification ou autorisation de "second niveau" est exigée par son fournisseur de service serait de demander cela dans la description textuelle portée dans une réponse 401 retournée de la passerelle PINT.

5.4 Résumé des implications de sécurité

De l'exposé qui précède, on voit que PINT porte toujours des éléments de données qui sont sensibles, et qu'il peut y avoir des considérations financières en plus des plus normales considérations de confidentialité. Il en résulte que les transactions DOIVENT être protégées dans le transit contre l'interception, la modification et la répétition.

PINT se fonde sur SIP et SDP, et peut utiliser les procédures de sécurité décrites dans la [RFC2543] (sections 13 et 15). Cependant, dans le cas de PINT, la recommandation de SIP que les demandes et réponses PUISSENT être protégées n'est pas suffisante. Les messages PINT DOIVENT être protégés, de sorte que les mises en œuvre de PINT DOIVENT prendre en charge la sécurité SIP (comme décrit aux sections 13 & 15 de la [RFC2543]) et être capables de traiter de tels messages lorsque ils sont reçus.

Dans certaines configurations, les clients, serveurs, et passerelles PINT peuvent être sûrs qu'ils fonctionnent en utilisant les services de la sécurité de niveau réseau [RFC2401], de la sécurité de couche transport [RFC2246], ou la sécurité physique pour toutes les communications entre eux. Dans ces cas, les messages PEUVENT être échangés sans la sécurité SIP, car tout le trafic est déjà protégé. Les clients et serveurs DEVRAIENT prendre en charge la configuration manuelle pour utiliser de telles facilités de sécurité de couche inférieure.
Lorsque on utilise la sécurité de couche réseau [RFC2401], la base de données de politique de sécurité DOIT être configurée à fournir une protection appropriée au trafic PINT. Lorsque on utilisé TLS, un accès configuré NE DOIT PAS être aussi configuré pour le trafic non TLS. Lorsque TLS est utilisé, l'authentification de base DOIT être prise en charge, et les certificats côté client PEUVENT être pris en charge. L'authentification du client qui fait la demande est cependant obligée, de sorte que si elle n'est pas fournie par le mécanisme sous-jacent utilisé, elle DOIT être incluse dans les messages PINT en utilisant les techniques d'authentification de SIP. À la différence de SIP, les demandes PINT sont souvent envoyées à des parties avec lesquelles des relations de communications antérieures existent (comme un opérateur de téléphonie). Dans ce cas, il peut y avoir un secret partagé entre le client et la passerelle PINT. De tels systèmes PINT PEUVENT utiliser une authentification fondée sur le secret partagé, avec "l'authentification de base" HTML. Lorsque ceci est fait, l'intégrité et la confidentialité du message doivent être garanties par un mécanisme de couche inférieure.

Cela a cependant des implications sur le fonctionnement de PINT. Si un serveur mandataire ou de redirection PINT est utilisé, il doit alors être capable d'examiner le contenu des datagrammes IP transportés. Il s'ensuit qu'une approche de bout en bout utilisant la sécurité de couche réseau entre le client PINT et une passerelle PINT empêche l'utilisation d'un mandataire intermédiaire ; la communication entre le client et la passerelle est portée via un tunnel auquel aucune entité intermédiaire ne peut obtenir l'accès, même si les datagrammes IP sont portés via ce nœud. À l'inverse, si une approche "bond par bond" est utilisée, tout mandataire PINT intermédiaire (ou serveur de redirection) est, implicitement, une entité de confiance.

Cependant, si il y a le moindre doute quant à l'existence d'une association de sécurité du réseau sous-jacent ou de couche transport, les participants à l'échange de protocole PINT DOIVENT utiliser les techniques de chiffrement et d'authentification au sein du protocole lui-même. Les techniques décrites à la section 15 de la [RFC2543] DOIVENT être utilisées, sauf si il y a un autre schéma de protection qui a fait l'objet d'un accord entre les parties. Dans l'un et l'autre cas, le contenu de tout corps de message porté dans une demande ou réponse PINT DOIT être protégé ; ceci a des implications sur les options d'acheminement des demandes via des mandataires (voir le paragraphe 5.3). Lorsque on utilise les techniques de SIP pour la protection, les champs d'en-tête Request-URI et To: dans les demandes PINT ne peuvent pas être

protégés. Dans les services PINT de base, ces champs peuvent contenir des informations sensibles. Ceci est à considérer, et si ces données sont considérées comme sensibles, cela seul va alors empêcher l'utilisation des techniques SIP ; dans une telle situation, des mécanismes de protection de couche transport [RFC2246] ou réseau [RFC2401] DOIVENT être utilisés.

Finalement, ce choix va à son tour avoir une influence sur le choix de l'utilisation d'un protocole de couche transport ; si une association TLS est disponible entre deux nœuds, TCP devra alors être utilisé. Ceci est différent du comportement par défaut de SIP (essayer UDP, puis essayer TCP si cela échoue).

6. Considérations de déploiement et relations de PINT à I.N. (Information)

6.1 Frontal de la Toile à infrastructure PINT

Il est possible que d'autres protocoles soient utilisés pour communiquer les exigences d'un usager demandeur. Du fait du grand nombre de navigateurs et serveurs disponibles sur la Toile, il semble probable que certains systèmes PINT vont utiliser HTML/HTTP comme "frontal". Dans ce scénario, HTTP sera utilisé sur une connexion depuis le navigateur de la Toile (WC, *Web Browser*) de l'usager demandeur à un serveur intermédiaire de la Toile (WS, *Web Server*). Cela va être étroitement associé à un client PINT (PC) (en utilisant un mécanisme non spécifié pour transférer les données du WS au client PINT). Le client PINT va représenter l'usager demandeur à la passerelle PINT (PG), et donc le système exécutif (XS) qui effectue l'action requise.

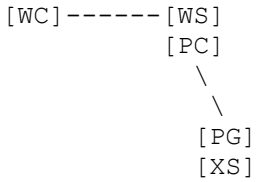

Figure 2 : Configuration de base "face à la Toile"

6.2 Redirections sur plusieurs passerelles

Il est assez possible qu'une passerelle PINT soit associée à un (ou des) systèmes exécutifs qui peuvent se connecter au GSTN à différents endroits. Également, si il y a une chaîne de serveurs PINT, chacun de ces serveurs intermédiaires ou mandataires (PP) peut être capable d'acheminer les demandes PINT aux systèmes exécutifs qui se connectent à des points spécifiques du GSTN. Il en résulte qu'il peut y avoir plus d'une passerelle PINT ou d'un système exécutif qui puisse traiter une certaine demande. Les mécanismes pour choisir où livrer une demande sortent du domaine d'application du présent document.

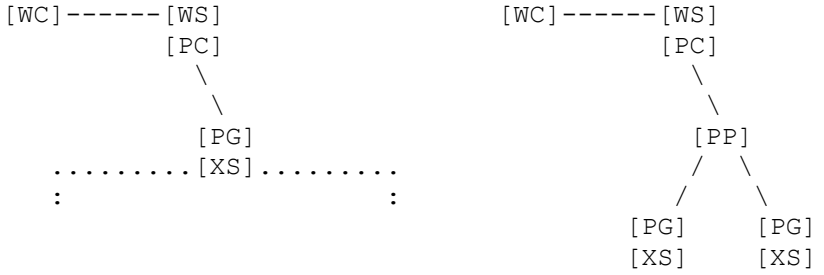

Figure 3 : Configurations d'accès multiples

Cependant, il semble bien qu'il y ait deux approches. Soit un serveur qui agit comme mandataire ou redirection va choisir lui-même la passerelle appropriée et va causer l'envoi de la demande en conséquence, soit une liste des localisations possibles va être retournée à l'usager demandeur à partir de laquelle il peut faire son choix.

Dans SIP, cela implique que si un mandataire ne peut pas résoudre la destination d'une demande en une seule correspondance, une réponse contenant une liste des choix devrait alors être retournée à l'usager demandeur pour qu'il en retienne une. Ce scénario n'est pas très probable dans l'utilisation normale de SIP.

Cependant, dans PINT, de telles ambiguïtés peuvent être assez courantes ; cela implique qu'il y a un certain nombre de fournisseurs possibles pour un service donné.

6.3 Passerelles PINT en compétition pour s'enregistrer à offrir le même service

Avec PINT, l'enregistrement n'est pas pour un individu mais plutôt pour un service qui peut être traité par un fournisseur de service. Donc, on peut envisager un enregistrement par le serveur PINT du domaine telcoA.com de sa capacité à prendre en charge le service R2C comme "R2C@telcoA.com", envoyé à un serveur intermédiaire qui agit comme registraire pour le domaine "broker.telcos.com" à partir de "R2C@pint.telcoA.com" comme suit :

```
REGISTER sip:registrar@broker.telcos.com SIP/2.0
To: sip:R2C@pint.telcoA.com
From: sip:R2C@pint.telcoA.com
...
```

C'est le service standard d'enregistrement SIP.

Cependant, qu'arrive t-il si il y a un certain nombre de fournisseurs de service différents, qui prennent tous en charge le service "R2C" ? Supposons qu'il y ait un système PINT au domaine "broker.com". Les clients PINT qui demandent un service de Demande-d'appel à broker.com peuvent très bien vouloir être redirigés ou avoir pour mandataire n'importe lequel de ces divers fournisseurs de service qui se sont précédemment enregistrés auprès du registraire. Les serveurs PINT peuvent aussi être intéressés par la fourniture de service aux demandes qui ne spécifiaient pas explicitement de fournisseur de service, ainsi que pour les demandes qui étaient dirigées "sur eux".

Pour permettre un tel service, les serveurs PINT vont faire un REGISTER au serveur courtier PINT pour des enregistrements de la forme :

```
REGISTER sip:registrar@broker.com SIP/2.0
To: sip:R2C@broker.com
From: sip:R2C@pint.telcoA.com
```

Lorsque plusieurs messages REGISTER de cette sorte apparaissent chez le registraire, ne différant chacun que par l'URL dans la ligne From:, le registraire a de nombreuses possibilités, par exemple :
(i) il écrase l'enregistrement précédent pour "R2C@broker.telcos.com" lorsque le suivant arrive ;
(ii) il rejette l'enregistrement suivant pour "R2C@broker.telcos.com" ;
(iii) il conserve tous ces enregistrements.

Dans ce dernier cas, à réception d'une invitation pour le service "général", soit :
(iii.1) il passe l'invitation à tous les fournisseurs de service enregistrés, retournant une réponse colligée avec tous les acceptants, utilisant plusieurs en-têtes Location:, ou
(iii.2) il choisit en silence un des enregistrements (utilisant, par exemple, une approche de "round robin") et achemine l'invitation et la réponse sans autre commentaire.
Comme solution à toutes les approches ci-dessus,
(iv) il peut choisir de ne pas permettre d'enregistrement pour le service "général", rejetant toutes des demandes REGISTER.

L'algorithme par lequel est fait un tel choix va dépendre de la mise en œuvre, et sort du domaine d'application de PINT. Lorsque un comportement doit être défini par les usagers demandeurs, une sorte de langage de traitement d'appel pourrait être utilisé pour permettre à ces clients, comme une opération préparatoire au service, de télécharger le comportement qu'ils attendent au serveur qui prend ces décisions. Ceci est cependant un sujet pour d'autres protocoles que PINT.

6.4 Limitations des informations disponibles et de la temporisation de demande pour SUBSCRIBE

Une configuration de référence pour PINT est que les demandes de service sont envoyées, via une passerelle PINT, à un système exécutif qui satisfait à la fonction de contrôle de service (SCF, *Service Control Function*) d'un réseau intelligent (I.N, *Intelligent Network*) (voir [Q.1204]). La réussite ou l'échec de l'appel de service résultant peut être des informations disponibles pour le SCF et donc potentiellement disponibles pour la passerelle PINT. En termes d'enregistrement d'historique de la réussite ou de l'échec d'un service, un grand SCF peut se trouver traiter un million de tentatives d'appel par heure. Avec ce volume de transactions de service, il y a des limites au delà desquelles il ne peut plus mémoriser les enregistrements de disposition de service ; espérer découvrir si une télécopie a bien été envoyé le mois dernier d'un SCF sur occupé est irréaliste.

Les autres changements d'état, comme ceux sur l'achèvement d'un appel de service réussi, exigent que le SCF arrange la surveillance de l'appel de service d'une façon que le service peut ne pas faire normalement, pour des raisons de performances. Dans la plupart des mises en œuvre, il est peu efficace d'interrompre un service pour le changer une fois que son exécution a commencé, de sorte qu'il peut être nécessaire d'avoir deux services différents ; un qui établit les ressources du GSTN pour surveiller la terminaison des appels de service, et un qui ne le fait pas. Il est improbable qu'il soit possible de décider que la surveillance est requise une fois que le service a commencé.

Ces facteurs peuvent avoir des implications à la fois sur les informations qui sont potentiellement disponibles à la passerelle PINT, et sur quand une demande d'enregistrer l'intérêt pour l'état d'un service PINT peut réussir. La solution de remplacement à l'utilisation d'un SCF général est de fournir un nœud de service dédié juste pour les services PINT. Comme ce nœud est impliqué dans l'établissement de tous les appels de service, il est en position de collecter les informations nécessaires. Cependant, il peut bien n'être quand même pas capable de réussir à répondre à un enregistrement d'intérêt pour les changements d'état d'appel une fois qu'une instance de programme logique de service fonctionne.

Donc, bien qu'un usager demandeur puisse enregistrer un intérêt pour l'état d'une demande de service, la passerelle PINT peut n'être pas en position de satisfaire cette demande. Bien que cela n'affecte pas le protocole utilisé entre le demandeur et la passerelle PINT, cela peut influencer la réponse retournée. Pour éviter le problème d'une logique de service qui change pendant le fonctionnement, tout enregistrement d'intérêt pour les changements d'état devrait être fait au plus tard au moment où est faite la demande de service.

À l'inverse, si une demande d'historique est faite sur la disposition d'un service, cela devrait être fait dans un court délai après la fin du service ; il est peu probable que le système exécutif puisse mémoriser longtemps les résultats des demandes de service ; ceux-ci devront avoir été traités rapidement comme des enregistrements de comptabilité de message automatique (AMA, *Automatic Message Accounting*) après quoi le système exécutif n'a pas de raison de les garder, et ils peuvent donc être éliminés.

Lorsque la passerelle PINT et le système exécutif sont intimement liés, la passerelle peut répondre aux demandes d'abonnement à l'état qui sont faites lors du fonctionnement d'un service. Elle peut accepter ces demandes et simplement ne pas même essayer d'interroger le système exécutif jusqu'à ce qu'il ait l'information qu'un service s'est terminé, en retournant simplement l'état final. Donc le demandeur PINT peut être dans ce qu'il croit être un état de surveillance, alors que la passerelle PINT n'a même pas informé le système exécutif qu'une demande avait été faite. Cela va augmenter la complexité interne de la passerelle PINT en ce qu'elle va avoir un ensemble complexe d'automates à états entrelacés, mais cela ne signifie pas que l'enregistrement et l'indication d'état PEUT être fournie conjointement avec un système de réseau intelligent.

6.5 Paramètres nécessaires pour invoquer les services traditionnels GSTN au sein de PINT

Cette section décrit comment les paramètres nécessaires pour spécifier certains services traditionnels du GSTN peuvent être portés dans les demandes PINT.

6.5.1 Identifiant de service

Lorsque un usager demandeur demande qu'un service soit effectué, il aura, bien sûr, à spécifier d'une certaine façon de quel service il s'agit. Cela peut être fait dans les URL au sein de l'en-tête To: et dans l'URI de demande (voir au paragraphe 3.5.5.1).

6.5.2 Parties A et B

Avec un service de demande d'appel, il y aura aussi besoin de spécifier les parties A et B qui veulent être engagées dans l'appel de service résultant. La partie A pourrait identifier, par exemple, le centre d'appel à partir duquel elle veut un rappel, tandis que la partie B est son numéro de téléphone (c'est-à-dire celui que l'agent du centre d'appel doit appeler).

Les services de demande de télécopie et de demande d'écoute d'un contenu exigent que la partie B soit spécifiée (respectivement le numéro de téléphone du télécopieur de destination ou le téléphone auquel le contenu parlé doit être délivré) mais la partie A est une ressource fondée sur le réseau téléphonique (soit un télécopieur, soit un transcodeur/envoyeur de parole) et elle est implicite ; l'usager demandeur ne la spécifie pas (et ne le peut pas).

Avec la variante "Retour de télécopie" du service de Demande de télécopie, (c'est-à-dire où le contenu à livrer réside sur le GSTN) il faudra aussi spécifier deux parties. Comme auparavant, la partie B est le numéro de téléphone du télécopieur auquel on veut qu'une télécopie soit envoyée. Cependant, dans cette variante, la partie A identifie le "contexte de document" du magasin fondé sur le GSTN duquel un document particulier doit être restitué ; l'analogie est ici qu'un usager

du GSTN compose un certain numéro de téléphone et entre ensuite le numéro du document à retourner en utilisant les chiffres de "touches de tonalité". Le numéro de téléphone qui est composé est celui du magasin de documents ou celui de la partie A, les chiffres des "touches de tonalité" choisissant le document dans ce magasin.

6.5.3 Autres paramètres de service

Pour ce qui concerne les autres paramètres de la demande, les services diffèrent là aussi. Le service Demande d'appel a seulement besoin des parties A et B. Il est aussi pratique d'affirmer que le service résultant va porter la voix, car le système exécutif dans la destination GSTN peut être capable de vérifier cette assertion à l'égard des numéros des parties A et B spécifiés et peut traiter l'appel différemment.

Avec les services de demande de télécopie et de demande d'écoute du contenu, les informations de source à décoder sont détenues sur l'Internet. Cela signifie soit que ces informations sont portées avec la demande elle-même, soit qu'est donnée une référence à la source de ces informations.

De plus, il est pratique d'affirmer que l'appel de service va porter une télécopie ou de la voix, et, si possible, spécifier le format des informations de source.

Le contenu fondé sur le GSTN ou variante "Retour de télécopie" du service de demande de télécopie doit spécifier le numéro du magasin de document et le numéro du télécopieur auquel ces informations doivent être délivrées. Il est pratique d'affirmer que l'appel va porter des données de télécopie, car le système exécutif de destination peut être capable de vérifier cette assertion à l'égard du numéro de magasin de documents et celui du télécopieur de destination.

De plus, le numéro du document peut aussi devoir être envoyé. Ce paramètre est une référence opaque qui est portée à travers l'Internet mais n'a de signification qu'au sein du GSTN. Le numéro du magasin de documents et le numéro du document spécifient ensemble de façon univoque le contenu réel à télécopier.

6.5.4 Résumé des paramètres de service

Le tableau suivant résume les informations nécessaires afin de spécifier pleinement l'intention d'une demande de service GSTN. Noter qu'il exclut tous les autres paramètres (comme les jetons d'authentification ou d'autorisation, ou les en-têtes Expires: ou CallId:) qui peuvent être utilisés dans une demande.

Service	ServiceID	partie A	partie B	CallFmt	Source	SourceFmt
R2C	x	x	x	voix	-	-
R2F	x	-	x	fax	URI/IL	ISF/ILSF
R2FB	x	x	x	fax	OR	-
R2HC	x	-	x	voix	URI/IL	ISF/ILSF

Dans ce tableau, "x" signifie que le paramètre est exigé, tandis que "-" signifie que le paramètre n'est pas requis.

Les services mentionnés sont Demande d'appel (R2C), Demande de télécopie (R2F), contenu fondé sur le GSTN ou variante "Retour de télécopie" de la demande de télécopie (R2FB) et demande d'écoute de contenu (R2HC).

Les valeurs de paramètre de format d'appel "voix" ou "fax" indiquent la sorte d'appel de service qui résulte.

L'indicateur de source "URI/IL" implique que les informations sont soit une référence de source Internet (un identifiant de ressource universel, ou URI) soit sont portées "en ligne" avec le message. L'indicateur de source "OR" signifie que la valeur passée est une référence opaque *(Opaque Reference)* qui devrait être portée avec le reste du message mais n'est à interpréter que dans le contexte de destination (GSTN). Autrement, elle pourrait être donnée comme référence "locale" avec le style "file", ou même en utilisant une référence partielle avec le style "http". Cependant, la façon dont une telle référence est interprétée est l'affaire du serveur PINT et du système exécutif receveurs ; elle reste, en fait, une référence opaque.

La valeur de format de source "ISF/ILSF" signifie que le format de la source est spécifié soit en termes d'URI, soit qu'il est porté "en ligne". Noter que, pour certaines données, le format peut être détecté par inspection ou, si tout le reste échoue, peut être supposé provenir de l'URI (par exemple, en supposant que la partie extension de fichier d'un URL indique le type de données). Pour une référence opaque, le format de source n'est pas disponible sur l'Internet, et n'est donc pas donné.

6.6 Transposition de paramètre en extensions PINT

Cette section décrit la façon dont peuvent être portés dans un message "PINT étendu" les paramètres nécessaires pour

spécifier une demande de service GSTN. Il y a d'autres choix, qui ne sont pas interdits. Cependant, afin d'assurer que l'usager demandeur reçoit le service qu'il attend, il est nécessaire d'avoir une compréhension commune des paramètres transmis et du comportement attendu du serveur PINT et de son système exécutif participant.

L'identifiant de service peut être envoyé comme l'élément userinfo de l'URI de demande. Donc, la première ligne d'une invitation PINT serait de la forme :

INVITE <Identifiant-de-service>@<serveur-pint>.<domaine> SIP/2.0

La partie A pour la demande d'appel et la variante "Retour de télécopie" du service demande de télécopie peut être détenue dans le champ d'en-tête "To:". Dans ce cas, la valeur de l'en-tête "To:" sera différente de l'URI de demande. Dans les services où la partie A n'est pas spécifiée, le champ "To:" a toute liberté pour répéter la valeur détenue dans l'URI de demande. C'est le cas pour les services Demande de télécopie et Demande d'écoute de contenu.

La partie B est nécessaire dans tous ces services de base, et peut être détenue dans la sous-partie SDP incluse, comme valeur du champ "c=".

Le paramètre format d'appel peut être détenu au titre de la valeur du champ "m=". Il se transpose en l'élément "protocole de transport" comme décrit au paragraphe 3.4.2.

La spécification du format de source se tient dans le champ "m=", comme un type et soit "-", soit sous-type. Le premier est normalement exigé pour tous les services sauf Demande d'appel ou "Retour de télécopie", où la forme "-" peut être utilisée. Comme on l'a montré précédemment, le format de source et la source ne sont pas toujours requis lors de la génération de demandes de services. Cependant, l'inclusion dans toutes les demandes d'une spécification de format de source peut rendre plus simple l'analyse de la demande et permettre que d'autres services soient spécifiés à l'avenir, de sorte que les valeurs sont toujours données. Le paramètre format de source est traité au paragraphe 3.4.2 comme élément "type de support".

La source elle-même est identifiée par une valeur de champ "a=fmtp:", lorsque nécessaire. À l'exception du service Demande d'appel, toutes les invitations vont normalement inclure un tel champ. Du point de vue des extensions à SDP, on peut le considérer comme qualifiant le sous-type de support, comme pour dire, par exemple, "quand je dis jpeg, voila ce que cela veut dire".

En résumé, les paramètres nécessaires pour les différents services sont portés dans les champs comme montré au tableau suivant :

Service	**Param. de serv.**	**Champ PINT/SIP ou SDP utilisé**	**Exemple de valeur**
R2C	ServiceID:	<informations d'utilisateur d'URI de demande SIP>	R2C
	AParty:	<champ SIP To:>	sip:123@p.com
	BParty:	<champ SDP c=>	TN RFC2543 4567
	CallFormat:	<sous-champ protocole de transport SDP d'un champ m=>	voix
	SourceFmt:	<sous-champ type de support SDP du champ m=>	audio
		(--- valeur de sous-champ de sous-type "-" seule utilisée)	---
	Source:	(--- Pas de source spécifiée)	---
R2F	ServiceID:	<informations d'utilisateur d'URI de demande SIP>	R2F
	AParty:	(--- champ SIP To: non utilisé)	sip:R2F@pint.xxx.net
	BParty:	<champ SDP c=>	TN RFCxxx +441213553
	CallFormat:	<sous-champ protocole de transport SDP du champ m=>	fax
	SourceFmt:	<sous-champ type de support SDP du champ m=>	image
		<sous-champ sous-type de support SDP du champ m=>	jpeg
	Source:	<champ SDP a=fmtp: qualifiant le précédant champ m=>	a=fmtp:jpeg<uri-ref>
R2FB	ServiceID:	<informations d'utilisateur d'URI de demande SIP>	R2FB
	AParty:	<champ SIP To:>	sip:1-730-1234@p.com
	BParty:	<champ SDP c=>	TN RFCxxx +441213553
	CallFormat:	<sous-champ SDP Protocole de transport du champ m=>	fax
	SourceFmt:	<ous-champ type de support SDP du champ m=>	image
		<sous-champ sous-type de support SDP du champ m=>	jpeg
	Source:	<champ SDP a=fmtp: qualifiant le champ précédant m=>	a=fmtp:jpeg opr:1234
R2HC	ServiceID:	<informations d'utilisateur d'URI de demande SIP>	R2HC
	AParty:	(--- champ SIP To: non utilisé)	sip:R2HC@pint.ita.il
	BParty:	<champ SDP c=>	TN RFCxxx +441213554
	CallFormat:	<sous-champ SDP protocole de transport du champ m=>	voix
	SourceFmt:	<sous-champ type de support SDP du champ m=>	texte
		<sous-champ sous-type de support SDP du champ m=>	html
	Source:	<champ SDP a=fmtp: qualifiant le champ précédant m=>	a=fmtp:html<uri-ref>

7. Références

[E.164] Recommandation UIT-T E.164, "Plan de numérotage du réseau public international", Genève, juin 1997.

[Q.763] Recommandation UIT-T Q.763 "Formats et codes pour le sous-système utilisateur du système de signalisation n° 7", Genève, août 1994.

[Q.1204] Recommandation UIT-T Q.1204 "Architecture de plan fonctionnel réparti du réseau intelligent", Genève, février 1994.

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par la* RFC6604)

[RFC1305] D. Mills, "Protocole de l'heure du réseau, version 3, spécification, mise en œuvre et analyse", STD 12, mars 1992. *(Remplacée par* RFC5905)

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par* 2184, 2231, 5335.)

[RFC2046] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 2 : Types de support", novembre 1996. *(D. S., MàJ par* 2646, 3798, 5147, 6657.)

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

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

[RFC2387] E. Levinson, "Type de contenu MIME Multiparti/Relatif", août 1998. *(P.S.)*

[RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir* RFC3986)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2458] H. Lu, et autres, "Vers l'interréseautage RTPC/Internet – Mises en œuvres pré-PINT", novembre 1998. *(Info.)*

[RFC2459] R. Housley, W. Ford, W. Polk et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de CRL pour l'Internet", janvier 1999. (*Obsolète, voir la* RFC3280) *(P.S.)*

[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.)*

[UNICODE] The Unicode Consortium, "The Unicode Standard -- Version 2.0", Addison-Wesley, 1996.

8. Remerciements

Les auteurs souhaitent remercier les membres du groupe de travail PINT de leurs commentaires qui ont été très utiles pour la préparation de la présente spécification. Les commentaires de Ian Elz ont été extrêmement utiles pour la compréhension du fonctionnement interne du RTPC. Les demandes SUBSCRIBE et NOTIFY ont d'abord été suggérées par Henning Schulzrinne et Jonathan Rosenberg. La suggestion d'utiliser un accès audio de 0 pour exprimer que le téléphone est "en garde" (c'est-à-dire qu'il ne reçoit pas la voix) est due à Ray Zibman. Finalement, merci à Bernie Hoeneisen pour sa relecture attentive.

Appendice A : ABNF collecté pour les extensions à PINT

;; --(L'ABNF est spécifié dans la [RFC2234])

;; --Variations aux définitions SDP

connection-field = ["c=" nettype space addrtype space connection-address CRLF]
; -- c'est la définition originale provenant de SDP, sont incluse pour être complet les interprétations et modifications de PINT suivantes

nettype = ("IN"/"TN") ; -- redéfini comme surensemble de la définition SDP

addrtype = (INAddrType / TNAddrType) ; -- redéfini comme surensemble de la définition SDP

INAddrType = ("IP4"/"IP6") ; -- ce non terminal est ajouté pour contenir les types d'adresse SDP originales

TNAddrType = ("RFC2543"/OtherAddrType)

OtherAddrType = (<X-Token>) ; -- X-token est défini dans la [RFC2045]

addr = (<FQDN> / <unicast-address> / TNAddr) ; -- redéfini comme surensemble de la définition SDP originale
; -- FQDN et unicast-address comme spécifié dans SDP

TNAddr = (RFC2543Addr/OtherAddr) ; -- TNAddr défini seulement dans le contexte de nettype == "TN"

RFC2543Addr = (INPAddr/LDPAddr)

INPAddr = "+" <POS-DIGIT> 0*(("-" <DIGIT>)/<DIGIT>) ; -- POS-DIGIT et DIGIT comme défini dans SDP

LDPAddr = <DIGIT> 0*(("-" <DIGIT>)/<DIGIT>)

OtherAddr = 1*<uric> ; -- OtherAdd défini dans le contexte de OtherAddrType
; -- uric est comme défini dans la [RFC2396]

media-field = "m=" media <espace> accès <espace> proto 1*(<espace> fmt) <CRLF>
; -- Note : redéfini comme sous-ensemble/assouplissement de la définition SDP d'origine
; -- espace et CRLF sont définis dans SDP

media = ("application"/"audio"/"image"/"text")
; -- Note : redéfini comme sous-ensemble de la définition SDP d'origine
; -- Ce peut être tout type MIME discret ; seuls ceux listés sont utilisés dans PINT 1.0

port = ("0" / "1") ; -- Note : redéfini à partir de la définition SDP d'origine ;
; -- 0 conserve la signification sdp usuelle de "temporairement pas de support" (c'est-à-dire "la ligne est en garde")
; -- (1 signifie qu'il y a un support)

proto = (INProto/TNProto) ; -- redéfini comme surensemble de la définition SDP originale

INProto = 1* (<alpha-numeric>) ; -- c'est le protocole SDP "classique", défini si nettype == "IN"
; -- alpha-numeric est défini dans SDP
TNProto = ("voice"/"fax"/"pager") ; -- c'est le protocole PINT, défini si nettype == "TN"

```
fmt = (<subtype> / "-")          ; -- Note : redéfini comme sous-ensemble de la définition SDP d'origine
                                 -- subtype comme défini dans la RFC2046, ou "-". DOIT être un sous-type du type détenu
                                   dans le sous-champ media associé ou la valeur spéciale "-".

attribute-fields = *("a=" attribute-list <CRLF>)   ; -- redéfini comme surensemble de la définition donnée dans SDP
                                                   -- CRLF est défini dans SDP

attribute-list = 1(PINT-attribute / <attribute>)      ; -- attribute est défini dans SDP

PINT-attribute = (clir-attribute / q763-nature-attribute / q763plan-attribute / q763-INN-attribute / phone-context-attribute /
                  tsp-attribute / pint-fmtp-attribute / strict-attribute)

clir-attribute = clir-tag ":" ("vrai" / "faux")

clir-tag = "clir"

q763-nature-attribute = Q763-nature-tag ":" q763-natures

q763-nature-tag = "Q763-nature"

q763-natures = ("1" / "2" / "3" / "4")

q763-plan-attribute = Q763-plan-tag ":" q763-plans

q763-plan-tag = "Q763-plan"

q763-plans = ("1" / "2" / "3" / "4" / "5" / "6" / "7")    ; -- la signification de 1, 3, et 4 est définie dans le texte

q763-INN-attribute = Q763-INN-tag ":" q763-INNs

q763-INN-tag = "Q763-INN"

q763-INNs = ("0" / "1")

phone-context-attribute = phone-context-tag ":" phone-context-ident

phone-context-tag = "phone-context"

phone-context-ident = network-prefix / private-prefix

network-prefix = intl-network-prefix / local-network-prefix

intl-network-prefix = "+" 1*<DIGIT>

local-network-prefix = 1*<DIGIT>

private-prefix = 1*excldigandplus 0*<uric>

excldigandplus = (0x21-0x2d,0x2f,0x40-0x7d))

tsp-attribute = tsp-tag "=" provider-domainname

tsp-tag = "tsp"

provider-domainname = <domaine>          ; -- domaine est défini dans la [RFC1035]

; -- Note : ce qui suit est redéfini par rapport à l'utilisation normale dans SDP

pint-fmtp-attribute = "fmtp:" <subtype> <space> resolution *(<espace> resolution) (<espace> ";" 1(<attribute>)
                      *(<espace> <attribute>))
                       ; -- subtype comme défini dans la [RFC2046.]
                       ; -- Noter que cette valeur DOIT correspondre à un fmt sur le dernier champ media précédant
```

-- attribute est défini dans SDP

resolution = (uri-ref / opaque-ref / sub-part-ref)

uri-ref = uri-tag ":" <URI-Reference> ; -- URI-Reference est défini dans la [RFC2396]

uritag = "uri"

opaque-ref = opr-tag ":" 0*<uric>

opr-tag = "opr"

sub-part-ref = spr-tag ":" <Content-ID> ; -- Content-ID est défini dans la [RFC2046] et la [RFC822]

spr-tag = "spr"

strict-attribute = "require:" att-tag-list

att-tag-list = 1(PINT-att-tag-list / <att-field> / pint-fmtp-tag-list) *("," (PINT-att-tag-list / <att-field> / pint-fmtp-tag-list))
; -- att-field est défini dans SDP

PINT-att-tag-list = (phone-context-tag / clir-tag / q763-nature-tag / q763-plan-tag / q763-INN-tag)

pint-fmtp-tag-list = (uri-tag / opr-tag / spr-tag)

;; --Variations aux définitions SIP

clir-parameter = clir-tag "=" ("true" / "false")

q763-nature-parameter = Q763-nature-tag "=" Q763-natures

q763plan-parameter = Q763-plan-tag "=" q763plans

q763-INN-parameter = Q763-INN-tag "=" q763-INNs

tsp-parameter = tsp-tag "=" provider-domainname

phone-context-parameter = phone-context-tag "=" phone-context-ident

SIP-param = (<transport-param> / <user-param> / <method-param> / <ttl-param> / <maddr-param> / <other-param>)
; -- les valeurs de cette liste sont toutes définies dans SIP

PINT-param = (clir-parameter / q763-nature-parameter / q763plan-parameter / q763-INN-parameter/ tsp-parameter /
phone-context-parameter)

URL-parameter = (SIP-param / PINT-param)
; -- redéfinition de URL-parameter de SIP pour inclure ceux définis dans PINT

Require-header = "require:" 1(required-extensions) *("," required-extensions)
; -- Ceci est redéfini comme sous-ensemble de la définition SIP (RFC2543, § 6.30)

required-extensions = ("org.ietf.sip.subscribe" / "org.ietf.sdp.require")

Appendice B Considérations relatives à l'IANA

Il y a trois sortes d'identifiants utilisés dans les extensions à PINT qui DEVRAIENT être enregistrées par l'IANA, si une nouvelle valeur est spécifiée. Ce sont :

* les sous-types de format de support, décrits au paragraphe 3.4.2,
* les attributs privés mentionnés au paragraphe 3.4.3,
* les valeurs de contexte de téléphone privé, décrites au paragraphe 3.4.3.1.

On notera que les types d'adresse privée (au paragraphe 3.4.1) ont été explicitement exclus de ce processus, car ils doivent être sous la forme d'un jeton X-.

B.1 Sous-types de format de support

En les prenant tour à tour, les sous-types de format de support sont utilisés dans les extensions PINT à SDP pour spécifier la ligne d'attributs qui contient les définitions de source de données. En utilisation normale, les valeurs de ce champ sont des sous-types de types MIME discrets [RFC2046]. Si une valeur autre qu'un sous-type enregistré par l'IANA doit être utilisé, il devrait alors être soit un jeton X- (c'est-à-dire commençant par "X-") soit il devrait être enregistré par l'IANA. Si l'intention est de décrire un nouveau sous-type MIME, les procédures spécifiées dans la [RFC2048] devraient alors être utilisées. On SUPPOSE que tout nouveau sous-type MIME va suivre les règles syntaxiques pour l'interprétation des lignes fmtp PINT associées définies dans le présent document.

Noter que, en ligne avec la description SDP, de tels enregistrements DEVRAIENT inclure les valeurs de champ "proto" au sein desquelles ils sont définis ; cependant, il est approprié de spécifier qu'elles ne peuvent être utilisées qu'avec "toutes les valeurs de TNProto".

À l'inverse, si l'intention est de définir une nouvelle façon d'inclure des définitions de source de données au sein de PINT, il sera alors nécessaire de spécifier, dans la documentation à l'appui de tout enregistrement d'un tel nouveau "sous-type de format de support PINT", la syntaxe de la ligne d'attribut "fmtp" associée, car l'identifiant sert à indiquer l'interprétation qui devrait être faite des lignes d'attribut spécifiques du format "étiquetées" avec un tel sous-type.

Si l'interprétation de fmtp suit celle par défaut de PINT, il est alors adéquat de le mentionner dans le document de définition plutôt que de répéter la définition de la syntaxe donnée ici (bien que, dans ce cas, on ne sait pas trop pourquoi un nouvel enregistrement serait nécessaire). Comme précédemment, le sous-type de format de support DEVRAIT spécifier les valeurs du champ "proto" au sein duquel il est défini, mais cela peut être "toutes les valeurs de TNProto".

B.2 Attributs privés

Toutes les lignes d'attribut propriétaires qui sont ajoutées peuvent être enregistrées auprès de l'IANA en utilisant les procédures mentionnées dans la [RFC2327] ; le mécanisme est le même que celui utilisé dans SDP. Si l'attribut est défini pour n'être utilisé que dans PINT, il peut alors être approprié de le mentionner dans la documentation. Noter que, dans la spécification PINT 1.0 traitée ici, il n'y a pas de mécanisme pour ajouter de telles lignes nouvellement enregistrées à une clause "require:"

B.3 Contextes de téléphone privé

Dans la description de session utilisée pour les demandes PINT, un attribut phone-context peut être utilisé pour spécifier le préfixe ou le contexte dans lequel un numéro de téléphone associé (dans une ligne de connexion) devrait être interprété.

Pour les contextes de téléphone "public", le préfixe à utiliser DOIT commencer soit par un CHIFFRE, soit par un "+". Les contextes de téléphone privé peuvent être enregistrés auprès de l'IANA mais NE DOIVENT PAS commencer par l'un ou l'autre de ces caractères. Un tel préfixe peut être utile pour identifier un réseau privé, éventuellement avec un identifiant numérique associé (voir l'exemple 4 du paragraphe 3.4.3.1). Dans l'exemple, le préfixe agit comme le contexte pour le plan de numérotage de réseau privé de X-acme.com.

Il est recommandé que tout contexte privé à enregistrer ait la forme générale d'un jeton incluant un nom de domaine, facultativement suivi par une chaîne numérique ou un autre jeton. La forme appropriée de l'espace de nom du jeton initial sera similaire à celle utilisée pour les enregistrements privés ou de fabricant pour les sous-types (par exemple vnd.acme.com). Cependant, noter que l'enregistrement sera utilisé pour spécifier le format du plan de numérotage du réseau privé d'un abonné plutôt que d'être utilisé généralement pour tous les équipements d'abonné du fabricant ; donc, fbi.gov serait approprié, mais lucent.com ne le serait pas (sauf si le réseau privé devait être utilisé en interne pas Lucent).

De plus, la documentation support DOIT déclarer qu'il n'y a pas de jeton associé, ou définir la syntaxe par laquelle ce jeton peut être analysé (par exemple, vnd.fbi.gov <espace> 1*DIGIT). Noter que l'enregistrement décrit un format, non une gamme de valeurs ; il est suffisant que le contexte privé puisse être analysé, sans que la valeur soit interprétée.

En détail, la demande d'enregistrement DEVRAIT inclure :

* la sorte d'enregistrement (c'est-à-dire l'attribut de contexte de téléphone privé à utiliser dans la description de service

des demandes de service PINT) ;
* les détails de contact de la personne responsable de la demande d'enregistrement (nom, organisation, adresse de messagerie électronique, numéro de téléphone public) ;
* nom du jeton initial de préfixe privé (par exemple vnd.fbi.gov) ;
* syntaxe du contexte privé (par exemple "vnd.fbi.gov" <espace> 1*DIGIT, ou "vnd.gtn.gov.uk") ;
* description d'utilisation (par exemple "Ce contexte de téléphone déclare un numéro de téléphone associé comme étant dans le 'réseau de télécommunications gouvernemental'" ; le numéro est dans une forme de plan de numérotage interne ou privé) ;
* type de réseau et type d'adresse auquel est associé ce contexte privé ; si les types de téléphone "normal" (comme spécifié dans ce document) sont utilisés, les valeurs vont alors se présenter comme : "nettype=TN" , addrtype="RFC2543Addr". Cependant, si ce contexte devait être utilisé avec un autre type d'adresse, une référence à ce nom de type d'adresse et la syntaxe de cette valeur d'adresse seraient alors requises.

En bref, ce contexte est l'équivalent téléphonique d'un espace d'adresse "Net 10" derrière un NAT, et le nom initial (et les informations de contact) montre le contexte dans lequel cette adresse est valide. Il spécifie aussi le format des types d'adresse et de réseau (et la syntaxe de valeur d'adresse) avec laquelle ce contexte est associé.

Bien sûr, l'IANA peut renvoyer les enregistrements demandés à l'IESG ou à un groupe de travail approprié de l'IETF pour examen, et peut demander que des révisions soient faites avant d'accepter l'enregistrement.

Adresse des auteurs

Scott Petrack
MetaTel, Inc.
45 Rumford Ave.
Waltham MA 02453-3844
USA
téléphone : +1 (781)-891-9000
mél : scott.petrack@metatel.com

Lawrence Conroy
Siemens Roke Manor Research
Roke Manor
Old Salisbury Lane
Romsey, Hampshire U.K. SO51 0ZN
téléphone : +44 (1794) 833666
mél : lwc@roke.co.uk

Déclaration complète de droits de reproduction

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