Groupe de travail Réseau
Request for Comments : 3835
Catégorie : Information

Traduction Claude Brière de L'Isle

A. Barbir & R. Penno, Nortel Networks
R. Chen, AT&T Labs
M. Hofmann, Bell Labs/Lucent Technologies
H. Orman, Purple Streak Development
août 2004

Architecture pour les services marginaux à connexion libre (OPES)

Résumé
Le présents mémoire définit une architecture qui permet la création d'un service d'application dans lequel un fournisseur de données, un consommateur de données, et zéro, une ou plusieurs entités d'application mettent coopérativement en œuvre un service de flux de données.

1. Introduction

Lorsque on fournit un service de flux de données entre un fournisseur et un consommateur, il peut se manifester un besoin de provisionner l'utilisation d'autres entités d'application, en plus du fournisseur et du consommateur. Par exemple, une partie peut souhaiter personnaliser un flux de données comme service à un consommateur. L'étape de personnalisation peut être fondée sur la disponibilité de la ressource du consommateur (par exemple., des capacités d'affichage).

Dans certains cas, il peut être avantageux de fournir un service de personnalisation au sein du réseau entre l'hôte fournisseur et l'hôte consommateur plutôt qu'à un de ces points d'extrémité. Pour certains services effectués au nom de l'utilisateur final, ceci peut être la seule option de déploiement de service. Dans ce cas, zéro, une ou plusieurs entités d'application supplémentaires peuvent participer au service de flux de données. Il y a de nombreux scénarios de provisionnement possibles qui rendent attractif un service de flux de données. Le document sur les cas d'utilisation et scénarios de déploiement des OPES [RFC3752] fournit des exemples de services OPES. Ce document discute des services qui modifient les demandes, qui modifient les réponses, et qui créent des réponses. Il est recommandé que le document sur les cas d'utilisation et les scénarios de déploiement des OPES [RFC3752] soit lu avant le présent document.

Ce document présente les composants architecturaux des services marginaux à connexion libre (OPES) qui sont nécessaires afin d'effectuer un service de flux de données. L'architecture répond aux considérations de l'IAB décrites dans la [RFC3238]. Ces considérations sont couvertes dans diverses parties du document. Le paragraphe 2.5 traite du traçage, la Section 3 traite des considérations de sécurité. La Section 4 donne un résumé des considérations de l'IAB et explique la façon dont l'architecture y répond.

Le document est organisé comme suit : la Section 2 introduit l'architecture OPES. La Section 3 discute des considérations de sécurité et de confidentialité des OPES. La Section 4 répond aux considérations de l'IAB sur les OPES. La Section 5 discute des considérations de sécurité. La Section 6 traite des considérations relatives à l'IANA. La Section 7 donne un résumé de l'architecture et des exigences d'interopérabilité.

2. Architecture

L'architecture des services marginaux à connexion libre (OPES) peut être décrite selon les termes de trois concepts en relations étroites, à savoir :
- o les entités OPES : processus fonctionnant dans le réseau ;
- o les flux OPES : flux de données qui sont réalisés de façon coopérative par les entités OPES ;
- o les règles des OPES : elles spécifient quand et comment exécuter les services OPES.

2.1 Entités OPES

Une entité OPES est une application qui fonctionne sur un flux de données entre une application de fournisseur de données et une application de consommateur de données. Les entités OPES peuvent être :

- o une application de service OPES, qui analyse et éventuellement transforme les messages échangés entre l'application de fournisseur de données et l'application du consommateur de données ;
- o un répartiteur de données, qui invoque une application de serveur OPES sur la base d'un ensemble de règles OPES et des connaissances spécifiques de l'application.

Le comportement coopératif des entités OPES introduit des fonctionnalités supplémentaires pour chaque flux de données pourvu qu'il satisfasse aux règles OPES. Dans le réseau, les entités OPES résident à l'intérieur des processeurs OPES. Dans le travail actuel, un processeur OPES DOIT inclure un répartiteur de données. De plus, les applications de fournisseur et de consommateur de données ne sont pas considérées comme des entités OPES.

Pour assurer une intégrité de système vérifiable (voir le paragraphe 3.1 sur les domaines de confiance) et pour faciliter le déploiement du chiffrement de bout en bout et le contrôle de l'intégrité des données, les processeurs OPES DOIVENT être :

- o explicitement adressables à la couche IP par l'utilisateur final (l'application de consommateur de données). Cette exigence n'empêche pas une chaîne de processeurs OPES dont le premier de la chaîne soit explicitement adressé à la couche IP par l'utilisateur final (l'application de consommateur de données).
- o acceptés par l'application de consommateur de données ou du fournisseur des données. Les détails de ce procès sortent du domaine d'application du présent travail.

L'architecture OPES est largement indépendante du protocole utilisé par l'application de fournisseur de données et consommateur de données) pour échanger les données. Cependant, le présent document a choisi HTTP [RFC2616] comme exemple de protocole sous-jacent dans les flux OPES.

2.1.1 Répartiteur de données

Les répartiteurs de données incluent un ensemble de règles qui peut être compilé à partir de plusieurs sources et DOIT se résoudre en un résultat non ambigu. L'ensemble de règles combiné permet à un processeur OPES de déterminer quelles applications de service invoquer pour un certain flux de donnés. En conséquence, le répartiteur de données constitue un point d'application de politique amélioré, où les règles de politique sont évaluées et des traitements de données spécifiques du service et des informations d'état sont conservées, comme le montre la Figure 1.

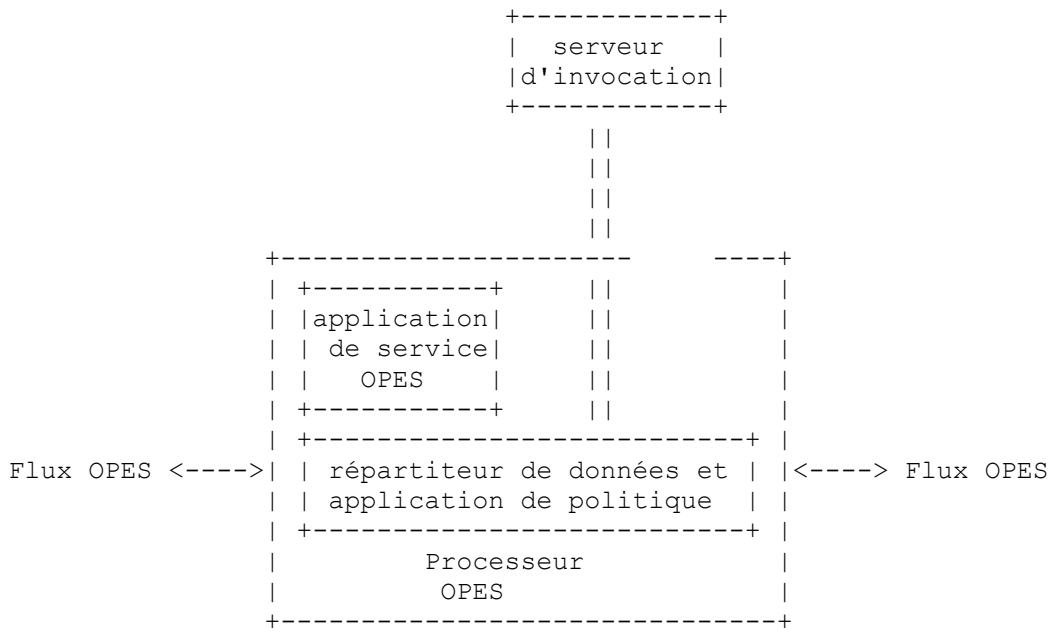

Figure 1 : Répartiteurs de données

L'architecture permet que plus d'un point d'application de politique soit présent sur un flux OPES.

2.2 Flux OPES

Un flux OPES est une entreprise coopérative entre une application de fournisseur de données, une application de consommateur de données, zéro, une ou plusieurs applications de service OPES, et un ou plusieurs répartiteurs de données.

Comme les politiques sont appliquées par les répartiteurs de données, la présence d'au moins un répartiteur de données est nécessaire dans le flux flux OPES.

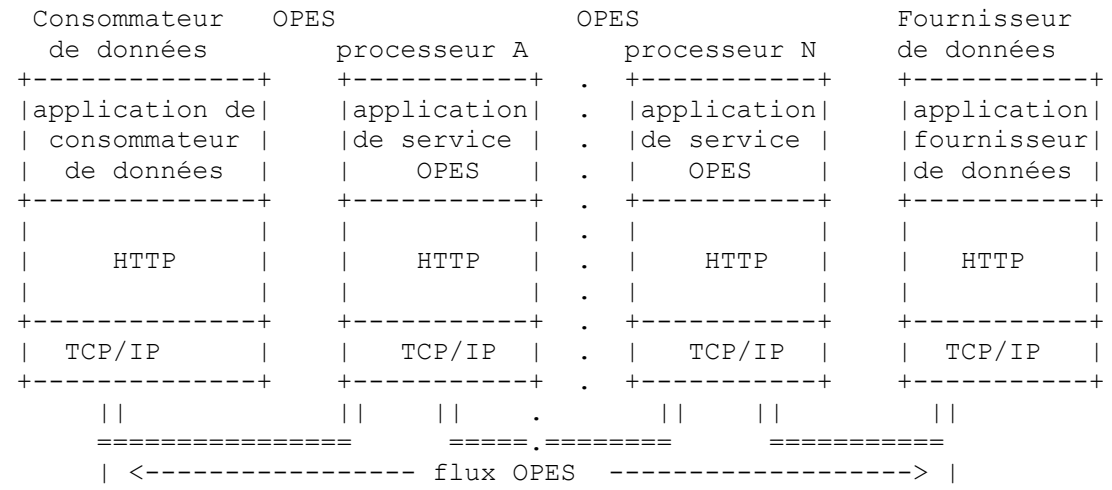

Figure 2 : Flux OPES

La Figure 2 décrit deux répartiteurs de données qui sont présents dans le flux OPES. L'architecture permet qu'un ou plusieurs répartiteurs de données soient présents dans tout flux.

2.3 Règles des OPES

La politique des OPES concernant les services et les données qui leurs sont fournies est déterminée par un jeu de règles consistant en règles OPES. Les règles consistent en un ensemble de conditions et d'actions qui s'y rapportent. Le jeu de règles est le sur ensemble de toutes les règles OPES sur le processeur. Le jeu de règles OPES détermine quelles applications de service vont opérer sur un flux de données. Dans ce modèle, tous les répartiteurs de données sont impliqués pour tous les flux.

Afin d'assurer un comportement prévisible, l'architecture OPES exige l'utilisation d'un schéma normalisé afin de définir et interpréter le jeu de règles. L'architecture OPES n'exige pas un mécanisme pour configurer un jeu de règles dans un répartiteur de données. Ceci est traité comme une affaire locale pour chaque mise en œuvre (par exemple, par l'utilisation d'un éditeur de texte ou un protocole de téléchargement sûr) pour autant qu'un tel mécanisme se conforme aux exigences de la Section 3.

2.4 Serveurs d'invocation

L'évaluation du jeu de règles OPES détermine quelles applications de service vont opérer sur un flux de données. Comment le jeu de règles est évalué n'est pas le sujet de l'architecture, sauf à noter qu'il DOIT en résulter le même résultat non ambigu dans toutes les mises en œuvre.

Dans certains cas, il peut être utile que le processeur OPES répartisse la responsabilité de l'exécution du service en communiquant avec un ou plusieurs serveurs d'invocation. Un répartiteur de données invoque les services d'un serveur d'invocation en utilisant le protocole d'invocation d'OPES (OCP, *OPES callout protocol*). Les exigences pour OCP figurent dans la [RFC3836]. OCP est ignorant de l'application, étant ignorant de la sémantique du protocole d'application encapsulé (par exemple, HTTP). Cependant, le répartiteur de données DOIT incorporer une capacité de vectorisation en relation avec le service qui analyse le flux de données conformément au jeu de règles et livre les données à l'application de service OPES, soit locale, soit distante.

La situation d'interaction générale est décrite à la Figure 3, qui illustre les positions et interactions des différents composants de l'architecture OPES.

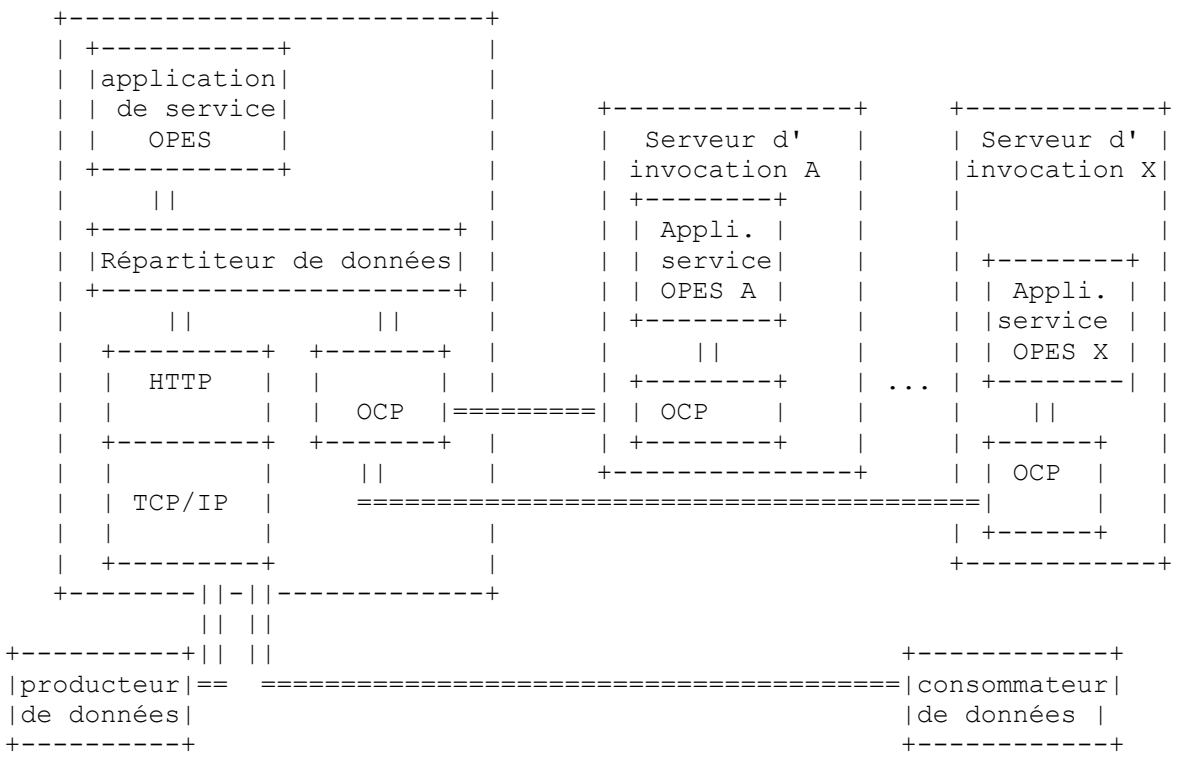

Figure 3 : Interaction des entités OPES

2.5 Facilité de traçage

L'architecture OPES exige que chaque répartiteur de données fournisse des facilités de traçage qui permettent la vérification appropriée de son fonctionnement. L'architecture OPES exige que le traçage soit faisable sur le flux OPES, par processeur OPES, en utilisant une annotation dans la bande. Une de ces annotations pourrait être un URI avec des informations plus détaillées sur les services OPES exécutés dans le flux OPES.

Fournir la capacité d'annotations dans la bande PEUT exiger des extensions d'en-tête au protocole d'application qui est utilisé (par exemple, HTTP). Cependant, la présence d'un processeur OPES dans le flux de demande/réponse de données NE DEVRA PAS interférer avec les opérations des clients et serveurs sans capacité OPES. Les clients et serveurs non OPES n'ont pas à prendre en charge ces extensions au protocole de base.

Les processeurs OPES DOIVENT respecter les exigences de traçage, de rapport, et de notification établies par le centre d'autorité dans le domaine de confiance auquel appartient le processeur OPES. Au titre de ces exigences, le processeur OPES peut avoir pour instruction de rejeter ou ignorer de telles exigence qui ont pour origine d'autres domaines de confiance.

3. Considérations de sécurité et de confidentialité

Chaque flux de données DOIT être sécurisé conformément à plusieurs politiques. Les principales parties prenantes sont le consommateur de données et le fournisseur de données. Les parties prenantes secondaires sont les entités auxquelles ils peuvent avoir délégué leur confiance. Les autres parties sont les propriétaires des serveurs d'invocation. Toutes ces parties peuvent participer au flux OPES.

Ces parties DOIVENT avoir un modèle, explicite ou implicite, pour décrire leur politique de confiance, quelles des autres parties sont de confiance pour opérer sur les données, et quelles améliorations de la sécurité sont exigées pour la communication. La confiance peut être déléguée pour toutes les données, ou elle peut être restreinte à une granularité allant jusqu'à une unité de données d'application.

Toutes les parties qui sont impliquées dans l'application des politiques DOIVENT communiquer les politiques aux parties impliquées. On fait confiance à ces parties pour adhérer aux politiques communiquées.

Afin de déléguer une confiance à fine granularité, les parties DOIVENT convoyer les informations de politique par un contrat implicite, par un protocole établi, par un protocole de négociation dynamique, ou en ligne avec des en-têtes de données d'application.

3.1 Domaines de confiance

La délégation d'autorité commence chez un consommateur de données ou chez un fournisseur de données et passe à des entités plus distantes "pas à pas". Pas à pas signifie que A délègue à B, et B délègue à C, et ainsi de suite. Les entités ainsi "colorées" par la délégation sont dites former un domaine de confiance par rapport à la partie délégataire originale. Ici, "coloré" signifie que si la première étape de la chaîne est le fournisseur de données, alors la délégation pas à pas "colore" la chaîne avec cette couleur "fournisseur" de données. Les seules couleurs définies sont "fournisseur" de données et "consommateur" de données. La délégation d'autorité (coloriage) se propage du producteur de contenu début de l'autorité ou du consommateur de contenu début de l'autorité, qui peuvent être différents des points d'extrémité dans le flux de données.

La Figure 4 illustre les domaines administratifs, les règles hors bande, et la distribution des politiques.

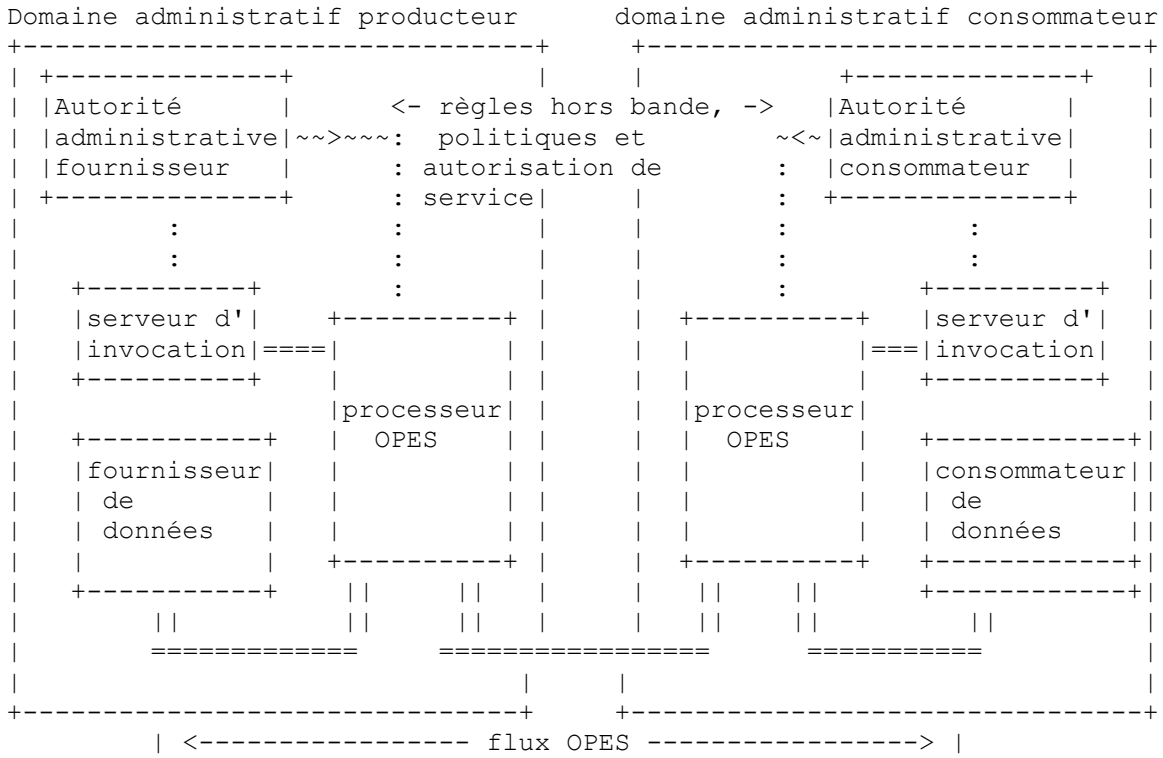

Figure 4 : domaines administratifs et distribution de politique des OPES

Afin de comprendre les relations de confiance entre les entités OPES, chacune est étiquetée comme résidant dans un domaine administratif. Les entités associées à un certain flux OPES peuvent résider dans un ou plusieurs domaines administratifs.

Un processeur OPES peut être dans plusieurs domaines de confiance à tout moment. Il n'y a pas de restriction à ce que les processeurs OPES soient autorisés par les consommateurs de données et/ou les fournisseurs de données. La partie d'origine a l'option d'interdire ou de limiter la redélégation.

Un processeur OPES DOIT avoir une représentation des membres de son domaine de confiance qu'il puisse rapporter en tout ou en partie pour les besoins du traçage. Il DOIT inclure le nom de la partie qui lui a délégué chaque privilège.

3.2 Établissement de la confiance et de l'autorisation de service

Le processeur OPES aura une politique de configuration spécifiant quels privilèges ont les serveurs d'invocation et comment ils vont être identifiés. OPES utilise des protocoles standard pour l'authentification et autre communication de sécurité avec les serveurs d'invocation.

Un processeur OPES aura une méthode de confiance pour recevoir les informations de configuration, comme des règles pour le répartiteur de données, les serveurs d'invocation de confiance, les parties principales qui ont une option d'inclusion ou d'exclusion de services individuels, etc.

Les protocoles pour la distribution de politique/règles sortent du domaine d'application du présent document, mais l'architecture OPES suppose l'existence d'un tel mécanisme.

Les exigences pour le mécanisme d'autorisation sont établies dans un document distinct [RFC3838].

Les demandes de service peuvent être faites dans la bande. Par exemple, une demande d'outrepassement des services OPES pourrait être signalée par un agent d'utilisateur avec une chaîne d'en-tête HTTP "Bypass-OPES". De telles demandes DOIVENT être authentifiées. La façon dont les entités OPES vont honorer de telles demandes est subordonnée aux politiques d'autorisation en vigueur à ce moment.

3.3 Protocole d'invocation

La détermination de si les processeurs OPES vont utiliser ou non les mesures qui sont décrites dans la section précédente durant la communication avec les serveurs d'invocation, dépend des détails de la façon dont les parties principales ont délégué la confiance aux processeurs OPES et des relations de confiance entre les processeurs OPES et le serveur d'invocation. Une authentification forte, des codes d'authentification de message, et le chiffrement DEVRAIENT être utilisés. Si les processeurs OPES sont dans un seul domaine administratif avec de fortes garanties de confidentialité et d'intégrité, la protection par chiffrement est recommandée mais facultative.

Si le mécanisme de délégation désigne les parties de confiance et leurs privilèges d'une façon qui permette l'authentification, les processeurs OPES seront alors responsables de la mise en application de la politique et de l'utilisation de l'authentification au titre de cette application.

Les serveurs d'invocation DOIVENT avoir connaissance de la politique qui gouverne le chemin de la communication. Ils NE DOIVENT PAS, par exemple, communiquer des informations confidentielles à des serveurs auxiliaires en dehors du domaine de confiance.

Une association de sécurité séparée DOIT être utilisée pour chaque canal établi entre un processeur OPES et un serveur d'invocation. Les canaux DOIVENT être séparés pour les différentes parties principales.

3.4 Confidentialité

Certaines données des points d'extrémité de flux OPES sont considérées comme "privées" ou "sensibles", et les processeurs OPES DOIVENT aviser les parties principales de leur politique de confidentialité et respecter les politiques des parties principales. Les informations privées DOIVENT être convoyées sur la base du flux. Cela peut être réalisé en utilisant les techniques de confidentialité courantes disponibles telles que P3P [W3CPREF] et les capacité de confidentialité de HTTP.

Les serveurs d'invocation DOIVENT aussi participer au traitement de données privées, ils DOIVENT être prêts à annoncer leurs propres capacités, et mettre en application la politique requise par les parties principales.

3.5 Intégrité de bout en bout

Les techniques de signature numérique peuvent être utilisées pour marquer les changements de données d'une façon telle qu'un tiers puisse vérifier que les changements sont ou non cohérents avec la politique de la partie génératrice. Ceci exige qu'une méthode en ligne spécifie la politique et ses liens avec les données, une trace des changements et l'identité de la partie qui fait les changements, et de fortes méthodes d'identification et d'authentification.

Une forte vérification d'intégrité de bout en bout peut satisfaire à certaines des fonctions requises par le "traçage".

4. Considérations d'architecture et de politique de l'IAB pour les OPES

Cette section s'adresse aux considérations de l'IAB sur les OPES [RFC3238] et résume comment l'architecture y répond.

4.1 Considération (2.1) de l'IAB : consentement d'une partie

L'IAB recommande que tous les services OPES soient explicitement autorisés par un des hôtes d'extrémité de la couche application (c'est-à-dire soit l'application de consommateur de données, soit l'application du fournisseur de données).
Le présent travail exige que soit l'application de consommateur de données, soit l' application du fournisseur de données consente aux services OPES. Ces exigences sont établies aux sections 2 (paragraphe 2.1) et 3.

4.2. Considération (2.2) de l'IAB : communications à la couche IP

L'IAB recommande que les processeurs OPES soient explicitement adressés dans la couche IP par l'utilisateur d'extrémité (application de consommateur de données).
Cette exigence est traitée au paragraphe 2.1 par l'exigence que les processeurs OPES soient adressables à la couche IP par l'application de consommateur de données.

4.3 Considérations (3.1 et 3.2) de l'IAB : Notification

L'IAB recommande que l'architecture OPES incorpore des facilités de traçage. Le traçage permet aux applications de consommateur de données et de fournisseur de données de détecter et répondre aux actions effectuées par les processeurs OPES qui sont réputés inappropriés pour les applications de consommateur de données ou de fournisseur de données.
Le paragraphe 3.2 discute des facilités de traçage et de notification qui doivent être prises en charge par les services OPES.

4.4 Considération (3.3) de l'IAB : non blocage

L'architecture OPES exige la spécification d'extensions à HTTP. Ces extensions sont permettre à l'application de consommateur de données de demander une version non OPES du contenu à l'application de fournisseur de données. Cette exigence est couverte au paragraphe 3.2.

4.5 Considération (4.1) de l'IAB : résolution d'URI

Cette considération recommande que la documentation d'OPES soit claire sur la description des services OPES appliqués au résultat de la résolution d'URI, et non à la résolution d'URI elle-même.

Cette exigence a été traitée aux paragraphes 2.5 et 3.2, en exigeant des entités OPES qu'elles documentent toutes les transformations qui ont été effectuées.

4.6 Considération (4.2) de l'IAB : validité de référence

Cette considération recommande que tous les services proposés définissent leur impact sur la validité de référence inter et intra document.

Cette exigence a été traitée au paragraphe 2.5 et tout au long du document en disant que les entités OPES sont obligées de documenter les transformations effectuées.

4.7 Considération (4.3) de l'IAB : extensions aux application d'adressage

Cette considération recommande que tout service OPES qui ne peut pas être réalisé tout en respectant les deux considérations précédentes puisse être révisé comme exigence potentielle pour les extensions d'architecture d'adressage d'application Internet, mais que cela ne doit pas être entrepris comme réparations ad hoc.

Le travail actuel n'exige pas d'extensions de l'architecture d'adressage d'application de l'Internet .

4.8 Considération (5.1) de l'IAB : confidentialité

Cette considération recommande que le cadre global des OPES fournisse des mécanismes pour que les utilisateurs finaux puissent déterminer les politiques de confidentialité des intermédiaires OPES.

Cette considération est traitée dans la Section 3.

5. Considérations sur la sécurité

Le travail proposé n'a rien à voir avec la sécurité sous ses perspectives variées. Il y a des questions de sécurité et de confidentialité qui se rapportent à l'application de consommateur de données, au protocole d'invocation, et au flux OPES. Dans la [RFC3837] il y a une analyse des menaces qui pèsent sur les entités OPES.

6. Considérations relatives à l'IANA

Le travail proposé va évaluer les protocoles courants pour OCP. Si le travail détermine qu'un nouveau protocole doit être développé, il pourra alors être nécessaire de demander de nouveaux numéros à l'IANA.

7. Résumé

Bien que l'architecture prenne en charge une large gamme de services de transformation coopératifs, les exigences pour l'interopérabilité sont peu nombreuses.

Les éléments nécessaires et suffisants sont spécifiés dans les documents suivants :
- o le schéma de l'ensemble des règles des OPES, qui définit la syntaxe et la sémantique des règles interprétées par un répartiteur de données ;
- o le protocole d'invocation d'OPES (OCP) [RFC3836], qui définit les exigences pour le protocole entre un répartiteur de données et un serveur d'invocation.

8. Références

8.1 Références normatives

[RFC2616] R. Fielding et autres, "Protocole de transfert hypertexte -- HTTP/1.1", juin 1999. *(D.S., MàJ par* 2817, 6585)

[RFC3238] S. Floyd, L. Daigle, "Considérations architecturales et de politique de l'IAB pour des services marginaux à connexion libre (OPES)", janvier 2002. *(Information)*

[RFC3752] A. Barbir et autres, "Services marginaux à connexion libre (OPES) : cas d'utilisation et scénarios de développement", avril 2004. *(Information)*

[RFC3836] A. Beck et autres, "Exigences pour les protocoles d'invocation de services marginaux à connexion libre (OPES)", août 2004. *(Information)*

[RFC3837] A. Barbir et autres, "Menaces et risques pour la sécurité des services marginaux à connexion libre (OPES)", août 2004. *(Information)*

[RFC3838] A. Barbir et autres, "Exigences de politique, d'autorisation, et de mise en application des services marginaux à connexion libre (OPES)", août 2004. *(Information)*

8.2 Références pour information

[W3CPREF] Cranor, L. et. al, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification", W3C Recommendation 16 http://www.w3.org/TR/2002/REC-P3P-20020416/ , avril 2002.

9. Remerciements

Le présent document a été produit par le groupe de travail OPES. Oskar Batuner (consultant indépendant) et Andre Beck (Lucent) sont également les auteurs qui ont contribué au présent document.

Les versions antérieures de ce travail ont été réalisées par Gary Tomlinson (The Tomlinson Group) et Michael Condry (Intel).

Les auteurs témoignent de leur gratitude à John Morris, Mark Baker, Ian Cooper et Marshall T. Rose pour leurs contributions.

10. Adresse des auteurs

Abbie Barbir
Nortel Networks
3500 Carling Avenue
Nepean, Ontario K2H 8E9
Canada
téléphone : +1 613 763 5229
mél : abbieb@nortelnetworks.com

Yih-Farn Robin Chen
AT&T Labs - Research
180 Park Avenue
Florham Park, NJ 07932
US
téléphone : +1 973 360 8653
mél : chen@research.att.com

Markus Hofmann
Bell Labs/Lucent Technologies
Room 4F-513
101 Crawfords Corner Road
Holmdel, NJ 07733
téléphone : +1 732 332 5983
mél : hofmann@bell-labs.com

Reinaldo Penno
Nortel Networks
600 Technology Park Drive
Billerica, MA 01821
USA
mél : rpenno@nortelnetworks.com

Hilarie Orman
Purple Streak Development
mél : ho@alum.mit.edu

11. Déclaration complète de droits de reproduction

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