Groupe de travail Réseau
Request for Comments : 3838
Catégorie : Information

A. Barbir, Nortel Networks
O. Batuner, Consultant
A. Beck, Lucent Technologies
T. Chan, Nokia
H. Orman, Purple Streak Development

Traduction Claude Brière de L'Isle
août 2004

Exigences de politique, d'autorisation et d'application des services marginaux à connexion libre (OPES)

Résumé
Le présent document décrit les exigences de politique, d'autorisation, et de mise en application pour le choix des services à appliquer à un certain flux de services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*).

Table des matières

1. Introduction

L'architecture des services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*) [RFC3835] permet des services d'application (services OPES) coopératifs entre un fournisseur de données, un consommateur de données, et zéro, un ou plusieurs processeurs OPES. Les services d'application considérés analysent et éventuellement transforment les messages de niveau application échangés entre le fournisseur de données et le consommateur de données. Le processeur OPES peut répartir la responsabilité de l'exécution du service en communiquant et en collaborant avec un ou plusieurs serveurs d'invocation distants.

L'exécution de tels services est gouvernée par un jeu de règles installé sur le processeur OPES. L'évaluation de la règle peut déclencher l'exécution d'applications de service locales au processeur OPES ou sur un serveur d'invocation distant.

Les politiques expriment les buts d'un processeur OPES comme un jeu de règles utilisé pour administrer, gérer, et contrôler l'accès aux ressources. Les exigences dans le présent document gouvernent le comportement des entités OPES pour déterminer quels services disponibles sont à appliquer à un certain message, si il en est.

La portée des politiques OPES décrites dans le présent document est limitée à celles qui décrivent quels services invoquer et, si c'est approprié, avec quels paramètres. Ces politiques n'incluent pas celles qui prescrivent le comportement des services invoqués. Il est souhaitable de permettre un cadre de gestion commun pour spécifier les politiques pour l'invocation et pour le comportement d'un service. L'intégration d'une telle fonction est le domaine des applications d'interaction d'utilisateur d'administration de politique.

Le document est organisé comme suit : la Section 2 considère le cadre de la politique. La Section 3 discute les exigences pour les interfaces, tandis que la Section 4 examine l'authentification des principaux et les autorisations des services.

2. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119]. Quand ils sont utilisés avec une signification normative, ces mots clés seront en majuscules. Les occurrences de ces mots en minuscules indiquent l'usage normal de la prose, sans implication normative.

3. Architecture de politique

Cette Section décrit les exigences de décomposition de la politique architecturale. Elle décrit aussi les exigences pour les interfaces entre les composants de la politique. Beaucoup des règles présentées ici ont été déterminées sous l'influence de la [RFC3238].

3.1 Composants et fonctions de politique

Les fonctions de politique sont décomposées en trois composants : un auteur de règle, un point de décision de politique (PDP, *Policy Decision Point*) [RFC3198], et un point de mise en application de politique (PEP, *Policy Enforcement Point*) [RFC3198]. L'auteur de règle fournit les règles qui vont être utilisées par une entité OPES. Ces règles contrôlent l'invocation des services au nom de l'auteur de règles. Le PDP et le PEP interprètent les règles collectées et les mettent en application de façon appropriée. La décomposition est illustrée par la Figure 1.

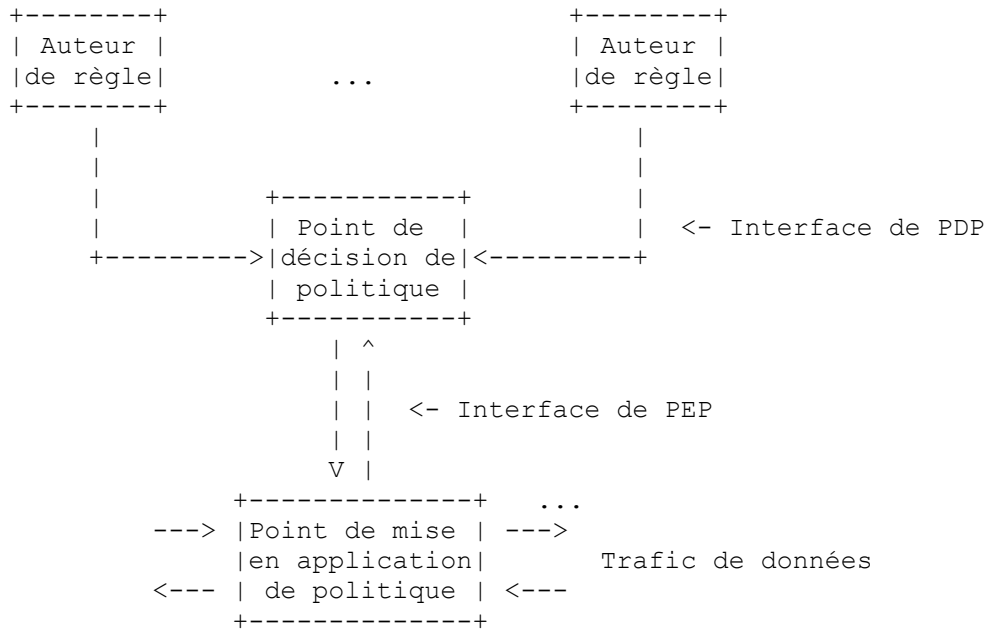

Figure 1 : Composants de politique

La décomposition du contrôle de politique en PDP et PEP permet le téléchargement de certaines tâches à un service administratif qui peut être localisé sur un serveur séparé des services d'application en temps réel du PEP qui résident sur le processeur OPES.

Le PDP assure l'authentification et l'autorisation des auteurs de règles et la validation et la compilation des règles.

Le PEP réside dans le filtre de données où les données provenant d'un flux OPES sont évaluées par rapport aux règles compilées et où les appels appropriés aux services demandés sont effectués.

Les interfaces entre ces composants architecturaux sont des points d'interopérabilité. L'interface entre les auteurs de règles et les points de décision de politique (Interface de PDP) DOIT utiliser le format qui peut résulter des exigences décrites dans le présent document.

L'interface entre les points de décision de politique et les points d'application de politique (Interface de PEP) peut être interne à une mise en œuvre spécifique de fabricant d'un processeur OPES. Les mises en œuvre DOIVENT n'utiliser l'interface standard que si le PDP et le PEP résident sur des processeurs OPES différents.

3.2 Exigences pour les points de décision de politique

Le point de décision de politique est essentiellement un compilateur de politique. Le PDP DOIT être un service qui fournit un soutien administratif aux points d'application. Le service de PDP DOIT authentifier les auteurs de règles.

Le PDP DOIT vérifier que les règles spécifiées sont dans la portée de l'autorité des auteurs de règles. Le PDP DOIT être un composant de l'autorité d'administration OPES.

3.3 Exigences pour les points d'application de politique

Dans l'architecture OPES, le filtre de données représente un point d'application de politique (PEP). À ce point, les données provenant d'un flux OPES sont évaluées par rapport aux règles compilées, et les appels appropriés aux services demandés sont effectués.
Dans le PEP, les règles PEUVENT enchaîner ensemble des actions, où une série de services à invoquer sont spécifiés. La mise en œuvre DOIT s'assurer de passer les informations d'un service invoqué à l'autre. La mise en œuvre NE DOIT PAS interdire la réévaluation d'un message pour déterminer si un autre service ou ensemble de services devrait être invoqué.
L'exécution d'une action (c'est-à-dire, le déclenchement d'une règle) peut conduire à la modification des valeurs des propriétés du message. Par exemple, un service OPES qui dans certaines circonstances convertit des images JPEG en images GIF modifie le type de contenu de l'objet de la Toile demandé.

De telles modifications des valeurs de propriété de message peuvent changer le comportement des actions OPES effectuées ultérieurement. Le filtre de données DEVRAIT agir sur les règles qui correspondent avant qu'il évalue les règles suivantes. Plusieurs règles qui correspondent peuvent être déclenchées simultanément si le filtre de données peut déterminer à l'avance qu'il n'y a pas d'effets collatéraux découlant de l'exécution de toute règle spécifique.

Un filtre de données PEUT évaluer plusieurs fois les messages dans le cours du traitement d'un flux OPES. Les points de traitement des règles PEUVENT être définis par des noms donnés administrativement. La définition de ces noms peut servir de sélecteur pour que des règles de politique déterminent l'applicabilité d'une règle ou d'un jeu de règles à chaque point de traitement.

Les règles de politique ([RFC3060] et [RFC3198]) DEVRAIENT être utilisées lorsque elles aident au développement du modèle de politique OPES.

La Figure 2 exprime un flux de données de message typique entre une application de consommateur de données, un processeur OPES, et une application de fournisseur de données. Il y a quatre points de traitement couramment utilisés identifiés par les numéros de 1 à 4.

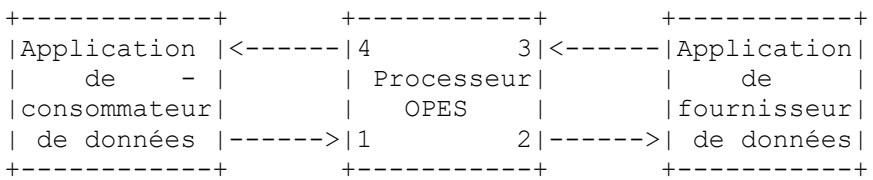

Figure 2 : Points d'exécution de traitement

Tout filtre de données (PEP) ou toute mise en œuvre administrative (PDP) DOIT prendre en charge les quatre points de traitement de règles.

- rôle de traitement de demande de consommateur de données : cela inclut le traitement des demandes quand elles sont reçues de l'application de consommateur de données.
- rôle de traitement de demande de processeur OPES : cela inclut le traitement des demandes avant de les transmettre à l'application de fournisseur de données
- rôle de traitement de demande de fournisseur de données : cela inclut de traiter les réponses lors de leur transmission à l'application de consommateur de données.
- rôle de traitement de réponse de processeur OPES : cela inclut de traiter les réponses lors de leur transmission à l'application de consommateur de données.

4. Exigences pour les interfaces

L'interface entre le système de politique et les services OPES doit inclure la capacité de passer les informations d'état du système ainsi que le message sujet.

4.1 Exigences de liens de service

Les services OPES invoqués DOIVENT pouvoir être spécifiés d'une façon indépendante de la localisation. C'est-à-dire que les auteurs de règles n'ont pas besoin de savoir ni de spécifier l'instance d'un service OPES dans les règles.

L'auteur de règle DEVRAIT être capable d'identifier le service demandé à un niveau de détail approprié à ses besoins. L'auteur de règle DEVRAIT être capable de spécifier un type de service ou être capable de spécifier tout service qui convient à une catégorie générale de service à appliquer à son trafic.

Le lien d'un nom de service OPES à un service spécifique PEUT être réparti entre le PDP et le PEP. Comme les règles sont compilées et validées par le PDP, elles DOIVENT se résoudre en un ensemble homogène de services OPES d'une installation spécifique.

Le choix d'une instance spécifique PEUT être différé et laissé au PEP pour choisir soit le moment d'installation de la règle, soit au démarrage. Pour réaliser l'interopérabilité, le PEP DOIT prendre en charge la résolution d'un nom générique en une instance spécifique. Il est possible d'utiliser des services tels que SLP ou UDDI pour résoudre des noms de service génériques en instances de service OPES spécifiques.

Le système de politique PEUT prendre en charge la découverte dynamique des liens de service. L'auteur de règle peut ne pas connaître les liens de service spécifiques, comme le protocole et les paramètres, quand une règle (comme spécifié sur l'interface de PDP) est de nature générale. Les informations de lien requises DOIVENT être fournies par le PDP et portées sur l'interface de PEP. Une méthodologie de description de service comme [WSDL] DOIT être présente dans le système de politique.

4.1.1 Variables d'environnement

Il peut être nécessaire de définir et prendre en charge le moyen de conserver les informations d'état qui peuvent être utilisées dans l'évaluation des conditions et dans l'exécution de l'action. Selon l'environnement d'exécution, les services OPES PEUVENT avoir la liberté de définir les variables nécessaires et utiliser ces variables pour mieux définir leur comportement de service sans le soutien du filtre de données.

4.1.2 Exigences pour l'utilisation des informations d'état

Les règles de politique PEUVENT spécifier que les informations d'état vont être utilisées au titre de l'évaluation des règles par rapport à un certain message dans un flux OPES. Donc, le système de politique DEVRAIT prendre en charge la maintenance des groupes qui peuvent être utilisés pour évaluer les conditions des règles. L'appartenance à de tels groupes peut être utilisée comme déclencheurs d'action.

Par exemple, un service autorisé à bloquer un site peut conclure qu'un certain utilisateur ne devrait pas être autorisé à accéder à un certain site de la Toile. Plutôt que d'invoquer le service pour chaque demande envoyée par cet utilisateur, une règle pourrait être créée pour déterminer si un utilisateur est membre des utilisateurs bloqués et si un site demandé est membre des sites bloqués, et ensuite invoquer un service bloquant local pour retourner un message approprié à l'utilisateur.

4.1.3 Exigences pour passer des informations entre services

Des variables d'environnement peuvent être utilisées pour passer des informations d'état entre services. Par exemple, l'analyse de la demande ou des modifications à la demande peuvent être capturées comme informations d'état qui peuvent être passées aux autres services sur le chemin de la demande ou aux services sur la ou les réponses associées à cette demande.

Dans le PEP, il DEVRAIT y avoir des dispositions pour permettre d'établir des variables lors du retour d'une invocation de service et de passer des variables aux autres services invoqués sur la base de la politique.

4.2 Exigences pour les règles et la gestion des règles

Ce paragraphe décrit les exigences pour la gestion des règles. Les règles sont divisées en deux groupes. Certaines règles sont fournies par l'application de consommateur de données, et d'autres règles sont fournies par l'application de fournisseur de données.

4.2.1 Exigences pour les fournisseurs de données

Les exigences pour les fournisseurs de données sont :

- Les fournisseurs de règles DOIVENT être authentifiés et autorisés pour les règles qui s'appliquent à leur rôle de réseau.
- Les fournisseurs de règles NE DOIVENT PAS être capables de spécifier des règles qui NE sont PAS dans la portée de leur autorité.
- Les fournisseurs de règles DEVRAIENT être capables de spécifier seulement ce qui est nécessaire pour leurs services.
- La compilation de règles provenant de différentes sources NE DOIT PAS conduire à l'exécution de règles contradictoires.
- La résolution de ces conflits de règles sort du domaine d'application du présent document.

4.2.2 Exigences pour les formats et protocoles de règles

Il est souhaitable de choisir des technologies standard comme XML pour spécifier le format de langage des règles.

Les règles doivent être envoyées des auteurs de règles au serveur administratif OPES pour les autorisations de service, les validations de règle, et la compilation. Les mécanismes pour le faire sortent du domaine d'application de ce travail.

Une fois que les règles sont autorisées, validées, et compilées par le serveur administratif, elles doivent être envoyées au processeur OPES. Les mécanismes pour le faire sortent du domaine d'application de ce travail.

4.2.3 Exigences pour les conditions de règles

Les conditions de règles DOIVENT être confrontées aux valeurs d'attributs du protocole encapsulé ainsi qu'aux valeurs des variables d'environnement. Les valeurs d'attributs du protocole encapsulé incluent les valeurs d'en-tête de protocole et éventuellement aussi les valeurs de corps de protocole.

Certains services OPES peuvent devoir être invoqués pour toutes les demandes d'utilisateur ou réponses de serveur, comme les services avec des fonctions d'enregistrement, par exemple. Le système de règles DEVRAIT permettre des règles inconditionnelles plutôt que d'exiger que les auteurs de règles spécifient des conditions de règles qui sont toujours vraies.

4.2.4 Exigences pour les actions de règles

Le système de règles DOIT permettre la spécification d'actions de règles qui sont déclenchés si les conditions d'une règle sont satisfaites. Les règles satisfaites conduisent normalement à l'invocation de services locaux ou distants .Les actions de règles DOIVENT identifier le service OPES qui est à exécuter pour la demande ou réponse actuelle de message.

Les actions de règles PEUVENT contenir des paramètres de démarrage qui peuvent être utilisés pour contrôler le comportement d'un service OPES. Si il en est de spécifiés, ces paramètres DOIVENT être passés au service OPES exécuté.

4.3 Exigences pour l'expression de politique

Les processeurs OPES DOIVENT appliquer les exigences de politique établies par les consommateurs de données et/ou publieurs de données en accord avec l'architecture [RFC3835] et le présent document. Ils ne peuvent le faire de façon cohérente que si il y a une sémantique sans ambiguïté et une représentation des éléments de données mentionnés dans la politique. Par exemple, le présent document mentionne la protection des informations "d'identité" et de "profil"

d'utilisateur. Si un utilisateur spécifie que son identité ne doit pas être communiquée à d'autres domaines administratifs OPES de confiance, et découvre ensuite que son nom de famille a été communiqué, il pourrait s'en plaindre. Si on lui a dit que "les noms de famille ne sont pas considérés comme des "identités" par le site", il va probablement estimer qu'il a des raisons de se plaindre. Ou, on a pu lui dire quand il a sélectionné "ne pas partager l'identité" sur un formulaire de la Toile proposé par le fournisseur de service OPES, que cela couvrait seulement son nom de connexion, et qu'une partie différente du formulaire devait être remplie pour protéger le nom de famille. Un autre souci peut surgir si les informations de configuration fournies par un formulaire de la Toile sont traduites en éléments de configuration donnés à un processeur OPES, et si ces éléments de configuration sont pour un ingénieur logiciel difficiles à traduire en application de politique. Les éléments de données peuvent avoir des noms ambigus ou être partagés selon des groupements difficiles à mettre en relation les uns avec les autres.

Les exemples illustrent pourquoi la politique OPES DOIT avoir des définitions des éléments de données, leurs relations, et comment ils se rapportent à la mise en application. Cette sémantique d'éléments essentiels n'exige pas un protocole distinct, mais elle DOIT faire l'objet d'un accord de tous les fournisseurs de service OPES, et les utilisateurs de services OPES DOIVENT avoir l'assurance qu'ils ont la capacité de connaître leurs réglages, de les changer si la politique du fournisseur de services permet les changements, et une assurance raisonnable qu'ils sont appliqués selon des interprétations raisonnables.

Les exigences pour les éléments de données de politique dans la spécification OPES n'ont pas à être "tout compris", mais elles DOIVENT couvrir l'ensemble minimal d'éléments qui permettent aux politiques de protéger les données des utilisateurs finaux et des publieurs.

5. Authentification des principaux et autorisation de services

Cette Section examine l'autorisation et l'authentification des services OPES.

5.1 Utilisateurs finaux, publieurs et autres considérations

5.1.1 Considérations sur les utilisateurs finaux

Une règle OPES détermine quels attributs de trafic vont déclencher l'application de services OPES. L'auteur du service peut fournir les règles, mais il ne peut pas fournir la partie nécessaire de précondition de la règle qui détermine quels utilisateurs du réseau auront les services OPES appliqués pour eux. Cette section discute comment les utilisateurs sont identifiés dans les préconditions de la règle, et comment les utilisateurs peuvent choisir et supprimer les services OPES pour leur trafic, comment un fournisseur de service OPES DEVRAIT identifier les utilisateurs, et comment ils déterminent si il faut ou non ajouter leur choix de services à un point d'application OPES.

Un fournisseur de service OPES DOIT satisfaire ces exigences majeures :
- o Permettre à tous les utilisateurs de demander d'ajouter, supprimer, ou bloquer des services OPES pour leur trafic (bloquer signifie "ne pas utiliser ce service pour mon trafic").
- o Empêcher des utilisateurs non fiables de causer l'interférence de services OPES avec le trafic d'autres utilisateurs.
- o Permettre aux utilisateurs de voir leurs profils de service OPES et leur notifier les changements.
- o Garder un enregistrement de toute activité du profil pour les besoins d'audit.
- o Adhérer à une politique de confidentialité gardant les profils d'utilisateurs.

L'administrateur du PDP est un tiers de confiance et peut régler la politique pour des individus ou des groupes en utilisant une communication hors bande et des fichiers de configuration. Cependant, les utilisateurs DOIVENT toujours être capables d'interroger le PDP afin d'apprendre quelles règles s'appliquent à leur trafic.

Les règles peuvent être déposées dans le PDP sans précondition relative aux utilisateurs du réseau. C'est la façon dont les règles sont conditionnées dans un service OPES quand il est livré pour installation. Le PDP est responsable de l'allocation d'identités aux règles et de leur transmission au PEP. L'identité utilisée par le PDP pour les décisions de politique DOIT être strictement transposée en l'identité utilisée par le PEP. Donc, si un usager passe par une procédure d'identification et d'authentification auprès du PDP et est connu sous l'identité "A", et si le PEP utilise des adresses IP pour les identités, le PDP DOIT alors fournir au PEP un lien entre "A" et l'adresse IP actuelle de A.

5.1.2 Considérations sur les sites de publication

Un fournisseur de service OPES agissant au nom de différents sites de publication DEVRAIT garder en mémoire toutes les considérations ci-dessus lorsque il met en œuvre un site OPES. Comme chaque site de publication ne peut être représenté

que par une seule identité, les bases de données d'authentification et d'autorisation peuvent être plus faciles à traiter pour le PEP.

5.1.3 Autres considérations

L'authentification peut être nécessaire entre les PDP et les PEP, les PEP et les serveurs d'invocation, les PEP et les autres PEP, et les serveurs d'invocation et les autres serveurs d'invocation, pour les besoins de validation des politiques de confidentialité. Dans tous les cas où les données ou le trafic d'utilisateur traversent les frontières d'un domaine de confiance, le domaine de confiance d'origine DEVRAIT avoir une politique décrivant quels autres domaines sont de confiance, et il DEVRAIT authentifier les domaines et leurs politiques avant de transmettre des informations.

5.2 Authentification

Quand un individu choisit (ou supprime) un service OPES, il DOIT être authentifié par le fournisseur de service OPES. Cela signifie qu'un lien entre le canal de communication de l'utilisateur et une identité connue du fournisseur de services est fait de façon sûre. Cela DEVRAIT être fait en utilisant une méthode d'authentification forte avec un certificat de clé publique pour l'utilisateur ; cela va aider à résoudre des problèmes ultérieurs. Il est recommandé que le fournisseur de services garde un enregistrement de toutes les demandes de services OPES. Le fournisseur de services DEVRAIT utiliser des certificats de clé publique pour authentifier les réponses aux demandes.

Le fournisseur de services peut avoir des utilisateurs de confiance qui par un contrat explicite ou implicite peuvent allouer, retirer, ou bloquer des services OPES pour des utilisateurs particuliers. Les utilisateurs de confiance DOIVENT être authentifiés avant qu'il leur soit permis des actions qui vont modifier la base de politique, et donc, les actions des PEP.

À cause de la sensibilité des profils d'utilisateur, l'interface de PEP entre le PEP et le PDP DOIT utiliser un protocole de transport sûr. Les PEP DOIVENT respecter les préférences de confidentialité des utilisateurs.

Quand un fournisseur de service OPES accepte un service OPES, il DOIT y avoir un nom unique pour le service fourni par l'entité qui publie le service. Les utilisateurs PEUVENT se référer au nom unique quand ils demandent un service. Le nom unique DOIT être utilisé pour notifier aux utilisateurs leurs profils de service. Les PEP DOIVENT avoir connaissance du nom unique de chaque service qui peut être accédé à partir de leur domaine. Il DOIT y avoir un lien cryptographique entre le nom unique et l'entité responsable du comportement fonctionnel du service, c'est-à-dire que si c'est un service de traduction d'un langage humain, le nom de la société qui a écrit le logiciel DEVRAIT être lié au nom unique.

5.3 Autorisation

En plus de demander ou terminer des services spécifiques, les utilisateurs PEUVENT bloquer des services particuliers, en indiquant que les services ne devraient pas être appliqués à leur trafic. La directive "bloquer tout OPES" DOIT être prise en charge utilisateur par utilisateur.

Une réponse à une demande d'un service OPES peut être positive ou négative. Les raisons pour une réponse négative incluent "service inconnu" ou "service refusé par la politique du PDP". Les réponses positives DEVRAIENT inclure l'identité du demandeur, le service, et le type de demande.

Comme décrit dans l'architecture OPES [RFC3835], les demandes de services OPES ont pour origine l'utilisateur final ou le domaine du publieur. Le PDP fonde sa décision d'autorisation sur le demandeur et sur le domaine. Il y a des cas où la décision peut être compliquée :

- L'utilisateur final a bloqué un service, mais un utilisateur de confiance du PDP veut quand même qu'il soit appliqué. Dans ce cas, l'utilisateur final DEVRAIT l'emporter, sauf si il y a des raisons de sécurité ou juridiques pour le laisser en place.
- Le publieur et l'utilisateur final sont dans le même domaine. Si le publieur et l'utilisateur final sont tous deux clients d'un PDP, peuvent-ils faire des demandes qui affectent mutuellement leur traitement ? Dans ce cas, le PDP DOIT avoir des règles de politique désignant les identités qui ont la permission d'établir de telles règles.
- Le publieur demande un service pour un utilisateur final. Dans le cas où le PDP et le PEP sont dans le domaine administratif du publieur, celui-ci a le moyen d'identifier l'utilisateur final et son trafic, et le PDP DOIT permettre au PEP d'appliquer la politique. Ceci est autorisé, mais le PDP DOIT utiliser des méthodes fortes pour identifier l'utilisateur et son trafic. L'utilisateur DOIT être capable de demander et recevoir des informations sur le profil de service qu'un site publieur conserve sur lui.
- L'utilisateur final demande un service spécifique à une identité de publieur (par exemple, nfl.com) mais le publieur interdit le service (par exemple, par un en-tête d'application "NO OPES"). Comme dans le cas ci-dessus, le publieur DOIT être capable de demander et recevoir des informations de profil qu'un utilisateur conserve sur un publieur.

En général, le PDP DEVRAIT tenir sa base de politique d'une manière qui facilite la compréhension de la procédure de décision pour tous les cas.

5.4 Intégrité et chiffrement

5.4.1 Intégrité et confidentialité de l'authentification et demandes/réponses de service

Les demandes et réponses DEVRAIENT être cryptographiquement liées aux identités du demandeur et répondeur, et les messages NE DEVRAIENT PAS être altérables sans détection. Une signature numérique fondée sur le certificat est fortement recommandée au titre du procès d'authentification. Un lien entre demande et réponse DEVRAIT être établi en utilisant un moyen de chiffrement aux bases solides, pour montrer que la réponse est faite à une demande spécifique.

5.4.2 Intégrité et confidentialité du contenu d'application

Comme indiqué par le PEP, le contenu va être transformé en tout ou en partie par les services OPES. Cela signifie que les protections cryptographiques de bout en bout ne peuvent pas être utilisées. C'est probablement acceptable pour la grande majorité du trafic, mais dans les cas où une forme inférieure de protection du contenu est désirable, des protections bond par bond peuvent être utilisées à la place. Les exigences pour de telles protections sont :

- L'intégrité en utilisant des secrets partagés DOIT être utilisée entre tous les points de traitement, les deux bouts (c'est-à-dire, les deux extrémité d'un "bond" DOIVENT partager un secret, mais le secret peut être différent entre les "bonds"). Les points de traitement incluent les serveurs d'invocation.
- Le chiffrement peut être demandé séparément, avec la même exigence de partage de secret entre les "bonds". Lorsque nécessaire, le chiffrement s'applique à tous les points de traitement, serveurs d'invocation inclus.
- Le signal pour l'intégrité (et facultativement le chiffrement) DOIT être généré par le demandeur (dans ce cas c'est aussi appliqué à la réponse) ou par le répondeur (auquel cas, il couvre seulement la réponse).
- Les secrets partagés DOIVENT être uniques (avec une très grande certitude probabiliste) pour chaque paire demandeur/répondeur. Cela aide à protéger la confidentialité des données de l'utilisateur contre des attaques d'infiltré ou contre des erreurs de configuration pendant le transit sur le réseau du fournisseur.

5.5 Confidentialité du demandeur

Le PDP DOIT avoir une politique de confidentialité à l'égard des données d'OPES comme les profils d'utilisateur pour les services. Les utilisateurs DOIVENT être capables de limiter la divulgation de leurs données de profil et de leurs identités.

Les limitations prises en charge DOIVENT inclure :

- La capacité d'empêcher l'identité d'être donnée aux serveurs d'invocation.
- La capacité d'empêcher les informations de profil d'être partagées.
- La capacité d'empêcher les données de trafic d'être envoyées aux serveurs d'invocation gérés par des tiers.
- La capacité d'empêcher le trafic provenant de sites particuliers d'être donné aux serveurs d'invocation OPES.

Quand un service OPES est fourni par un tiers, il DOIT avoir une politique de confidentialité et s'identifier aux parties amont et aval, et leur dire comment accéder à sa politique de confidentialité. Un mécanisme est nécessaire pour spécifier ces préférences et un protocole pour les distribuer (paragraphe 3.3).

6. Considérations sur la sécurité

Le présent document discute des exigences de politique, d'autorisation et d'application des OPES. Dans la [RFC3837] plusieurs questions de sécurité et de confidentialité relatives aux services OPES sont discutées.

7. Références

7.1 Références normatives

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

[RFC3060] B. Moore et autres, "Spécification du modèle d'information de cœur de politique -- version 1", février 2001. (*MàJ par* RFC3460) *(P.S.)*

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

[RFC3835] A. Barbir et autres, "Architecture pour les 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)*

7.2 Références pour information

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

[RFC3198] A. Westerinen et autres, "Terminologie pour la gestion fondée sur la politique", novembre 2001. *(Information)*

[WSDL] Christensen, et al., "Web Services Description Language (WSDL) 1.1", W3C Note, 15 mars 2001, http://www.w3.org/TR/wsdl

8. Remerciements

Tous nos remerciements à Andreas Terzis, L. Rafalow (IBM), L. Yang (Intel), M. Condry (Intel), Randy Presuhn (Mindspring), et B. Srinivas (Nokia).

9. Adresse des auteurs

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

Oskar Batuner
Consultant
mél : batuner@attbi.com

Andre Beck
Lucent Technologies
101 Crawfords Corner Road
Holmdel, NJ 07733
mél : abeck@bell-labs.com

Tat Chan
Nokia
5 Wayside Road
Burlington, MA 01803
USA
mél : Tat.Chan@nokia.com

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

10. Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org .

Remerciement

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