

Groupe de travail Réseau
Request for Comments : 4119
 Catégorie : En cours de normalisation
 Traduction Claude Brière de L'Isle

J. Peterson, NeuStar
 décembre 2005

Format d'objet de localisation Geopriv fondé sur la présence

Statut de ce mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

Le présent document décrit un format d'objet pour porter des informations géographiques sur l'Internet. Cet objet de localisation étend le format de données d'informations de présence (PIDF, *Presence Information Data Format*) qui a été conçu pour communiquer des informations de présence sensibles pour la confidentialité, et qui ont des propriétés similaires.

Table des Matières

1. Introduction.....	1
1.1 Conventions utilisées dans le présent document.....	2
2. Format d'objet de localisation.....	2
2.1 Utilisation de base de PIDF.....	2
2.2 Extensions à PIDF pour les règles de localisation et d'usage.....	3
2.3 Exemple d'objets de localisation.....	8
3. Portage de PIDF dans un protocole utilisateur.....	9
4. Sécurisation de PIDF.....	9
5. Considérations pour la sécurité.....	10
6. Considérations relatives à l'IANA.....	10
6.1 Jetons 'method'.....	10
6.2 Éléments 'provided-by'.....	11
6.3 Enregistrement du sous espace de noms d'URN pour urn:ietf:params:xml:ns:pidf:geopriv10.....	11
7. Remerciements.....	11
Appendice A : Schéma NENA Provided-By.....	11
A.1 Schéma XML dataProvider.....	12
Références normatives.....	13
Références pour information.....	13
Adresse de l'auteur.....	14
Déclaration complète de droits de reproduction.....	14

1. Introduction

Les informations de localisation géographique décrivent une position physique dans le monde qui peut correspondre à la localisation passée, présente, ou future d'une personne, d'un événement, ou d'un appareil. De nombreuses applications utilisées dans l'Internet aujourd'hui tirent parti du partage des informations de localisation (incluant des applications de transposition/navigation, "trouver des amis" sur les téléphones cellulaires, et ainsi de suite). Cependant, de telles applications peuvent divulguer les tenants et aboutissants sur une personne d'une manière contraire aux préférences de l'utilisateur. Des atteintes à la confidentialité peuvent résulter d'une faible sécurité du protocole (qui permettent à des observateurs de capturer des informations de localisation) de l'incapacité d'articuler ou traiter les préférences de l'utilisateur, ou de défauts similaires courants dans les systèmes existants. Les problèmes de confidentialité qui découlent de la divulgation involontaire de la localisation physique d'une personne sont parmi les plus sérieux auxquels sont confrontés les utilisateurs de l'Internet.

Par conséquent, il a été identifié un besoin de porter les informations de localisation géographique au sein d'un objet qui

inclut les préférences de confidentialité et de divulgation d'un utilisateur et qui soit protégé par une forte sécurité cryptographique. Un travail antérieur [RFC4079] a observé que ce problème a une certaine ressemblance avec le problème général de communication et de sécurisation des informations de présence sur l'Internet. La présence (définie dans la [RFC2778]) fournit une disposition de communications en temps réel pour un usager, et a donc des exigences similaires pour la distribution sélective et la sécurité.

Donc, le présent document étend le format de données d'informations de présence (PIDF, *Presence Information Data Format*) [RFC3863] fondé sur XML pour permettre l'encapsulation des informations de localisation au sein d'un document de présence.

Le présent document n'invente aucun format pour les informations de localisation elles-mêmes. De nombreux formats existants fondés sur la localisation civile, les coordonnées géographiques, et autres, ont été développés dans d'autres forums de normalisation. Le présent document définit plutôt un objet qui convient à la fois pour identifier et encapsuler les formats préexistants d'informations de localisation, et pour fournir une sécurité et des contrôles de politique adéquats pour réguler la distribution des informations de localisation sur l'Internet.

L'objet de localisation décrit dans le présent document peut être utilisé indépendamment de tout 'protocole d'utilisation', comme le terme est défini dans les exigences pour Geopriv [RFC3693]. On considère comme un avantage de cette proposition que les protocoles de présence existants (comme la [RFC3261]) vont naturellement s'accommoder du format d'objet de localisation défini dans le présent document, et être capables de composer les informations de localisation avec les autres informations de présence, parce que cet objet de localisation est une extension de PIDF. Cependant, l'usage de ce format d'objet de localisation ne se limite pas aux protocoles qui utilisent la présence -- tout protocole qui peut porter des types XML ou MIME peut porter PIDF.

Certaines des exigences des [RFC3693] et [RFC6772] concernent des collections de données et des politiques d'usage associées aux objets de localisation. Le présent document donne seulement le balisage minimum nécessaire pour qu'un utilisateur exprime les préférences de confidentialité nécessaires comme spécifiées par les exigences pour Geopriv (les trois éléments de base dans la [RFC6772]). Cependant, le présent document ne montre pas comment un ensemble complet de règles fondé sur XML, s'accommodant des besoins des serveurs de localisation, pourrait être incorporé dans PIDF. On suppose que d'autres protocoles (comme HTTP) seront utilisés pour passer les règles entre les détenteurs de règles et les serveurs de localisation, et que ces ensembles complets de règles seront définis dans un document séparé.

1.1 Conventions utilisées dans le présent document

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].

2. Format d'objet de localisation

2.1 Utilisation de base de PIDF

Les exigences pour Geopriv [RFC3693] (REQ en abrégé) spécifient le besoin d'un nom pour la personne, le lieu ou la chose que décrivent les informations de localisation (REQ 2.1). PIDF a déjà un tel identifiant : chaque document PIDF a un attribut "entity" de l'élément 'presence' qui signifie l'URI de l'entité dont le document décrit la présence. Par conséquent, si les informations de localisation sont contenues dans un document PIDF, l'URI dans l'attribut "entity" de l'élément 'presence' indique la cible de ces informations de localisation (la 'présentité'). L'URI dans l'attribut "entity" utilise généralement le schéma d'URI "pres" défini dans la [RFC3859]. De tels URI peuvent servir de pseudonymes non fiables (selon la REQ 12) aux communications de présentité.

PIDF contient facultativement un élément 'contact' qui fournit un URI où la présentité peut être jointe par des moyens de communication. Généralement le schéma d'URI dans la valeur de l'élément 'contact' donne une indication sur la façon dont la présentité peut être atteinte ; si on utilise le schéma d'URI SIP, par exemple, SIP peut être utilisé, et ainsi de suite. Les informations de localisation peuvent être fournies sans aucun moyen de communication associé. Donc, l'élément 'contact' peut ou non être présent, comme désiré par le créateur du document PIDF.

PIDF contient facultativement un élément 'timestamp' (*horodatage*) qui désigne l'heure à laquelle le document PIDF a été créé. Cet élément correspond à la REQ 2.7a.

PIDF contient un élément 'status' (*état*), qui est obligatoire. L'élément 'status' contient un élément fils facultatif, 'basic', qui décrit les dispositions de communication de la présentité (en termes très vagues : soit OUVERT, soit FERMÉ). Pour les

besoins du présent document, il n'est pas nécessaire que l'état 'basic' soit inclus. Si, cependant, les dispositions de communication sont incluses dans un document PIDF au delà de la géolocalisation, l'état 'basic' peut apparaître dans un document PIDF qui utilise ces extensions.

PIDF contient aussi un élément 'tuple' parapluie, qui contient un élément 'id' utilisé pour identifier de façon univoque un segment d'informations de présence afin que les changements de ces informations puissent être retracés au fil du temps (lorsque plusieurs notifications de présence sont reçues). Les éléments 'timestamp', 'status', et 'contact' sont composés sous 'tuple'.

2.2 Extensions à PIDF pour les règles de localisation et d'usage

Ce schéma XML étend l'élément 'status' de PIDF avec un élément complexe appelé 'geopriv'. Il y a deux sous éléments majeurs qui sont encapsulés dans geopriv : un pour les informations de localisation, et un pour les règles d'usage. Tous deux sont obligatoires, et ils sont décrits dans les paragraphes qui suivent. En composant ces deux sous éléments sous 'geopriv', les règles d'usage sont clairement et explicitement associées aux informations de localisation.

Pour l'extensibilité (voir la REQ 1.4), le schéma permet que tout autre sous élément apparaisse sous l'élément 'geopriv'. Deux autres sous éléments facultatifs sont inclus dans le présent document : un qui indique la méthode par laquelle est déterminée la localisation géographique, et un qui permet une désignation explicite de l'entité qui fournit l'information.

2.2.1 Élément 'location-info'

Chaque élément 'geopriv' DOIT contenir un élément 'location-info'. Un élément 'location-info' consiste en un ou plusieurs tronçons d'informations de localisation (selon la REQ 2.5). Le format des informations de localisation (REQ 2.6) est identifié par le schéma XML importé, qui décrit l'espace de noms en question. Tous les documents PIDF qui contiennent un élément 'geopriv' DOIVENT contenir une ou plusieurs directives d'importation qui indiquent le ou les schémas XML qui sont utilisés pour les formats de localisation géographique.

Afin d'assurer l'interopérabilité des mises en œuvre de Geopriv, il est nécessaire de choisir un format de localisation de base que prennent en charge toutes les mises en œuvre conformes (voir la REQ 3.1). Parce qu'il satisfait à la REQ 2.5.1, le présent document travaille à partir de l'hypothèse que le langage de balisage géographique (GML, *Geography Markup Language*) 3.0 [OpenGIS] sera le format obligatoire (un "DOIT mettre en œuvre" pour toutes les mises en œuvre de PIDF qui prennent en charge l'élément 'geopriv').

GML est un système extraordinairement complet et aux talents variés pour modéliser toutes les sortes de types d'objets géographiques, topologies, métadonnées, systèmes de références de coordonnées, et unités de mesures. Le plus simple paquetage de prise en charge des informations de localisation GML est le schéma 'feature.xsd'. Bien que 'feature.xsd' puisse exprimer des concepts géographiques compliqués, il exige très peu de balisage pour fournir les points de coordonnées de base pour les cas d'utilisation les plus courants. Diverses descriptions de format (incluant les informations de localisation fondées sur la latitude/longitude) sont prises en charge par 'feature.xsd' (voir des exemples au paragraphe 7.4.1.4 de [OpenGIS]) qu'on trouve à l'urn

Noter que par l'importation du schéma Feature, les schémas nécessaires du GML de base sont importés transitivement.

Des caractéristiques complexes (comme les topologies et polygones de modélisation, les directions et les vecteurs, les indications temporelles de l'heure pour laquelle une localisation particulière est valide pour une cible) sont aussi disponibles dans GML, mais exigent d'importer des schémas supplémentaires. Pour les besoins de l'interopérabilité de base comme définie dans le présent document, seule la prise en charge du schéma 'feature.xsd' de GML est EXIGÉE.

Les mises en œuvre PEUVENT prendre en charge le format de localisation civique (civicLoc) défini au paragraphe 2.2.5. Le format civicLoc fournit les éléments suivants :

Étiquette	Description	Exemple
A1	Le pays est identifié par le code ISO 3166 à deux lettres	US
A2	Subdivisions nationales (état, région, province, préfecture)	New York
A3	Comté, paroisse, gun (JP), district (IN)	Comté de King
A4	Cité, commune, shi (JP)	New York
A5	Arrondissement, bourg, district urbain, ward, chou (JP)	Manhattan
A6	Quartier, bloc	Morningside Heights
PRD	Voie	Broadway
POD	Direction de la voie	N, O
	Suffixe en queue de voie	SO

STS	Suffixe de voie	Avenue, Place,
HNO	Numéro, partie numérique seule.	123
HNS	Suffixe du numéro de maison	A, 1/2
LMK	Lieu-dit ou autre qualificatif	La petite librairie
LOC	Informations de localisation supplémentaires	Pièce 543
FLR	Étage	5
NAM	Nom (résidence, commerce ou bureau)	Coiffure Chez Joe
PC	Code postal	10027-0401

L'élément de format d'informations géographiques GML 3.0 ou l'élément de format de localisation ('civicLoc') défini dans le présent document, PEUT apparaître dans un élément 'location-info'. Tous deux PEUVENT aussi être utilisés dans le même élément 'location-info'. En résumé, le schéma feature.xsd de GML 3.0 DOIT être pris en charge par les mises en œuvre conformes à la présente spécification, et le format civicLoc PEUT être pris en charge par les mises en œuvre conformes à cette spécification.

2.2.2 Élément 'usage-rules'

Au moment de la rédaction du présent document, les exigences de politique pour les objets Geopriv n'étaient pas définitivement achevées. Cependant, l'élément 'usage-rules' (*règles d'usage*) existe pour satisfaire la REQ 2.8 et les exigences du document d'exigences de politique Geopriv [RFC6772]. Chaque élément 'geopriv' DOIT contenir un élément 'usage-rules' même si le faiseur de règles a demandé que tous les sous éléments soient donnés avec leurs valeurs par défaut.

Suivant le document d'exigences de politique (paragraphe 3.1) il y a trois champs qui doivent pouvoir être exprimés comme objets de localisation pendant tout leur cycle de vie (depuis le générateur jusqu'au receveur) : un champ qui limite les retransmissions, un qui limite la rétention, et un qui contient une référence aux ensembles de règles externes. Ces trois champs sont instanciés ici par les trois premiers éléments. Le quatrième élément donne un espace générique pour des directives de politique lisibles par l'homme. Chacun de ces champs PEUT être présent dans un élément 'usage-rules' d'objet de localisation ; aucun n'est obligé de l'être.

'retransmission-allowed' : lorsque la valeur de cet élément est 'non', le receveur de cet objet de localisation n'a pas la permission de partager les informations de localisation incluses, ou l'objet comme un tout, avec d'autres parties. Lorsque la valeur de cet élément est 'oui', la distribution de cette localisation est permise (à moins d'un accord hors bande existant ou de l'obligation du contraire). Par défaut, il DOIT être supposé que la valeur est 'non'. Les mises en œuvre DOIVENT inclure ce champ, avec la valeur de 'non', si le faiseur de règle ne spécifie pas de préférence.

'retention-expires' : ce champ spécifie une date absolue à laquelle le receveur n'a plus la permission de posséder les informations de localisation ni leur objet de localisation encapsulant ; tous deux peuvent être conservés jusqu'au moment spécifié par ce champ. Par défaut, la valeur DOIT être supposée de vingt quatre heures à partir de l'élément 'timestamp' du document PIDF, si il est présent ; si l'élément 'timestamp' est aussi absent, la valeur DOIT alors être supposée de vingt quatre heures depuis le moment où l'objet de localisation est reçu par le receveur de localisation. Si la valeur dans l'élément 'retention-expires' est déjà passée lorsque le receveur de localisation reçoit l'objet de localisation, le receveur DOIT éliminer immédiatement l'objet de localisation.

'ruleset-reference' : ce champ contient un URI qui indique où peut être trouvé un ensemble plus complet de règles de politiques, relatives à cet objet. Cet URI DEVRAIT utiliser le schéma d'URI HTTPS ; et si il le fait, le serveur qui détient ces règles DOIT authentifier toute tentative d'accès à ces règles. Les règles d'usage elles-mêmes peuvent divulguer des informations confidentielles sur une cible ou un faiseur de règle. L'URI PEUT, autrement, utiliser le schéma d'URI CID [RFC2392], et dans ce cas, il DOIT noter un corps MIME porté avec l'objet de localisation par le protocole utilisateur. Les ensembles de règles portés comme corps MIME DEVRAIENT être chiffrés et signés par le faiseur de règle ; les ensembles de règles non signés NE DEVRAIENT PAS être honorés par les serveurs de localisation ou les receveurs de localisation. Noter qu'afin d'éviter des boucles de réseau qui résulteraient en échec d'autorisation, les créateurs d'objets de localisation PEUVENT mettre des références d'ensemble de règles fondées sur HTTPS dans un corps MIME externe chiffré référencé par un CID ; de cette façon, les receveurs de l'objet de localisation qui ne sont pas capables de déchiffrer le corps MIME externe ne connaîtront l'URI HTTPS que si ils sont capables de déchiffrer le corps MIME.

'note-well' : ce champ contient un bloc de texte contenant d'autres directives génériques de confidentialité. Ces directives sont destinées seulement à être lisibles par l'homme, non à être traitées par un automate.

2.2.3 Élément 'method'

L'élément facultatif 'method' décrit la façon dont les informations de localisation ont été déduites ou découvertes. Un

exemple de cet élément (pour un système de position géographique) est : `<method>gps</method>`

Les valeurs possibles de l'élément 'method' sont énumérées dans un registre de l'IANA. Les mises en œuvre DOIVENT limiter l'utilisation de cette méthode aux valeurs enregistrées par l'IANA. Le présent document préremplit le registre IANA avec sept valeurs possibles ; voir plus d'informations au paragraphe 6.1.

L'élément 'method' est utile, par exemple, lorsque plusieurs sources rapportent des informations de localisation pour un certain usager, et des moyens de déterminer la localisation peuvent être considérés comme d'une autorité supérieure à celle d'autres (c'est-à-dire un système de position dynamique en temps réel contre un provisionnement statique associé à un appareil cible). Cependant, noter que l'inclusion de 'method' peut révéler des informations sensibles lorsque le générateur fournit intentionnellement des informations de localisation plus grossières. Par exemple, lorsque un objet de localisation est transmis avec 'DHCP' comme 'method', mais que les informations de localisation indiquent seulement la ville dans laquelle est situé le générateur, l'expéditeur a de bonnes raisons de soupçonner que des informations de localisation ont été supprimées.

2.2.4 Élément 'provided-by'

L'élément facultatif 'provided-by' décrit l'entité ou l'organisation qui a fourni ces informations de localisation (au delà des informations de domaine qui peuvent être déduites d'un certificat signant). Un exemple de cet élément (pour un système de jeu tout fait) pourrait être :

```
<provided-by>
  <test:game>
    West5
  </test:game>
</provided-by>
```

Les valeurs pour l'élément 'provided-by' DOIVENT être des espaces de noms XML enregistrés par l'IANA ; voir plus d'informations au paragraphe 6.2.

L'élément 'provided-by' n'est pas destiné à être utilisé par la plupart des entités, mais satisfait plutôt aux exigences particulières pour lesquelles des informations générales (enregistrement par l'IANA, taille de l'objet de localisation) et de potentielles fuites d'informations de localisation sont des choix acceptables.

Dans le cas général, l'entité qui a fourni des informations de localisation est communiquée par le `subjectAltName` du certificat avec lequel l'objet de localisation est signé ; donc, cet élément est inutile. 'Provided-by' est significatif dans les cas particuliers où le créateur d'un objet de localisation veut désigner un système ou partie particulier au sein d'un domaine administratif complexe, incluant des situations envisagées pour fournir des services d'urgence dans divers contextes nationaux. Il peut aider, par exemple, le receveur d'un objet de localisation malformé ou trompeur à identifier le système particulier qui a mal fonctionné.

Les utilisateurs devraient être conscients que ces informations peuvent par inadvertance fournir des informations supplémentaires au receveur, augmentant la résolution effective des informations géospatiales ou civiques, ou même révélant des informations de localisation, alors qu'elles étaient destinées à être entièrement protégées. Il faut considérer si il y a des circonstances qui ont influencé l'Université de Columbia à choisir de s'enregistrer et utiliser l'élément `provided-by`. Si un exemple de LO inclut seulement des informations de niveau état, inclure alors le fait que les informations de localisation ont été fournies par l'Université de Columbia donne une forte indication que la cible est en fait située dans une zone de quatre blocs de Manhattan. En conséquence, cet élément ne devrait être utilisé que lorsque des fonctions organisationnelles vont fortement en dépendre. Dans tous ces usages, le `subjectAltName` du certificat va suffire, et 'provided-by' NE DEVRAIT PAS être utilisé.

2.2.5 Définitions de schéma

Noter que l'espace de noms XML [RFC3688] pour cette extension à PIDF contient un numéro de version de 1.0 (selon la REQ 2.10).

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
```

```

    elementFormDefault="qualified" attributeFormDefault="unqualified">
<xs:import namespace="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy" />
<!-- Cette importation apporte dans le langage XML l'attribut xml:lang-->
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
      schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <xs:element name="geopriv" type="tns:geopriv"/>
<xs:complexType name="geopriv">
  <xs:sequence>
    <xs:element name="location-info" type="tns:locInfoType"
      minOccurs="1" maxOccurs="1"/>
    <xs:element name="usage-rules" type="gbp:locPolicyType"
      minOccurs="1" maxOccurs="1"/>
    <xs:element name="method" type="tns:locMethod"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="provided-by" type="tns:locProvidedBy"
      minOccurs="0" maxOccurs="1"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="locInfoType">
  <xs:sequence>
    <xs:any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="locMethod">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute ref="xml:lang" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:complexType name="locProvidedBy">
  <xs:sequence>
    <xs:any namespace="##other" processContents="skip"
      minOccurs="1" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

Le schéma 'geopriv10' importe, pour l'élément 'usage-rules', le schéma de politique suivant. Ce schéma a été séparé de l'objet de géolocalisation de base afin de permettre sa réutilisation. La sémantique associée à ces éléments, décrite au paragraphe 2.2.2, ne s'applique qu'à l'utilisation de ces éléments pour définir la politique pour les objets de géolocalisation ; toute autre utilisation de 'usage-rules' doit caractériser sa propre sémantique pour tous les sous éléments 'usage-rules'.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
<!-- Cette importation apporte dans le langage XML l'attribut xml:lang-->

```

```

<xs:import namespace="http://www.w3.org/XML/1998/namespace"
  schemaLocation="http://www.w3.org/2001/xml.xsd"/>

<xs:complexType name="locPolicyType">
  <xs:sequence>
    <xs:element name="retransmission-allowed" type="xs:boolean"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="retention-expiry" type="xs:dateTime"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="external-ruleset" type="xs:anyURI"
      minOccurs="0" maxOccurs="1"/>
    <xs:element name="note-well" type="tns:notewell"
      minOccurs="0" maxOccurs="1"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

  <xs:complexType name="notewell">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute ref="xml:lang" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

</xs:schema>

```

Le schéma suivant est une représentation triviale de localisation civique qui PEUT être mise en œuvre par des entités conformes à la présente spécification.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">

  <xs:complexType name="civicAddress">
    <xs:sequence>
      <xs:element name="country" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A1" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A2" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A3" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A4" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A5" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="A6" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="PRD" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="POD" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="STS" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="HNO" type="xs:string"
        minOccurs="0" maxOccurs="1"/>
      <xs:element name="HNS" type="xs:string"

```

```

    minOccurs="0" maxOccurs="1"/>
    <xs:element name="LMK" type="xs:string"
    minOccurs="0" maxOccurs="1"/>
    <xs:element name="LOC" type="xs:string"
    minOccurs="0" maxOccurs="1"/>
    <xs:element name="FLR" type="xs:string"
    minOccurs="0" maxOccurs="1"/>
    <xs:element name="NAM" type="xs:string"
    minOccurs="0" maxOccurs="1"/>
    <xs:element name="PC" type="xs:string"
    minOccurs="0" maxOccurs="1"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0"
    maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

2.3 Exemple d'objets de localisation

Noter que ces exemples montrent des documents PIDF sans qu'aucun en-tête MIME ou de sécurité ne leur soient appliqués (voir la Section 4).

Le document d'instance XML suivant est un exemple d'utilisation d'un simple balisage GML 3.0 avec quelques directives de politique spécifiées ci-dessus au sein d'un document PIDF. Les coordonnées GPS données dans l'élément 'gml' sont pour San Francisco, CA.

```

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
  entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
    <status>
      <gp:geopriv>
        <gp:location-info>
          <gml:location>
            <gml:Point gml:id="point1" srsName="epsg:4326">
              <gml:coordinates>37:46:30N 122:25:10W</gml:coordinates>
            </gml:Point>
          </gml:location>
        </gp:location-info>
        <gp:usage-rules>
          <gp:retransmission-allowed>no</gp:retransmission-allowed>
          <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
        </gp:usage-rules>
      </gp:geopriv>
    </status>
    <timestamp>2003-06-22T20:57:29Z</timestamp>
  </tuple>
</presence>

```

Le document d'instance XML suivant est un exemple d'utilisation de l'objet civicLoc avec quelques unes des directives de politique spécifiées ci-dessus dans un document PIDF.

```

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicLoc"
  entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
    <status>
      <gp:geopriv>

```



```

<gp:location-info>
  <cl:civicAddress>
    <cl:country>US</cl:country>
    <cl:A1>New York</cl:A1>
    <cl:A3>New York</cl:A3>
    <cl:A6>Broadway</cl:A6>
    <cl:HNO>123</cl:HNO>
    <cl:LOC>Suite 75</cl:LOC>
    <cl:PC>10027-0401</cl:PC>
  </cl:civicAddress>
</gp:location-info>
<gp:usage-rules>
  <gp:retransmission-allowed>yes</gp:retransmission-allowed>
  <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
</gp:usage-rules>
</gp:geopriv>
</status>
<timestamp>2003-06-22T20:57:29Z</timestamp>
</tuple>
</presence>

```

3. Portage de PIDF dans un protocole utilisateur

Un document PIDF est un document XML ; donc, PIDF peut être porté dans tout protocole capable de porter XML. Un type MIME a aussi été enregistré pour PIDF : 'application/pidf+xml'. PIDF peut donc être porté comme un corps MIME dans les protocoles qui utilisent MIME (comme SMTP, HTTP, ou SIP) avec un ensemble encapsulant d'en-têtes MIME, incluant un Content-Type de 'application/pidf+xml'.

Aller plus loin dans la spécification du comportement d'utilisation des protocoles (incluant de s'abonner ou de demander des informations de présence) sort du domaine d'application du présent document.

4. Sécurisation de PIDF

La sécurisation des documents XML peut être réalisée de diverses façons. XML prend lui-même en charge plusieurs façons de sécuriser partiellement les documents, incluant le chiffrement au niveau élément et les propriétés de signature numérique.

Pour les besoins du présent document, seule est considérée la sécurisation d'un document PIDF comme un tout, plutôt que la sécurité élément par élément. Aucune des exigences de la [RFC3693] ne suggère que seulement une partie des informations dans un objet de localisation pourrait avoir besoin de protection tandis que d'autres parties ne seraient pas protégées ; virtuellement toutes ces configurations introduiraient des potentiels de fuite de confidentialité. Par conséquent, l'utilisation de sécurité de niveau MIME est appropriée.

S/MIME [RFC3851] permet d'appliquer des propriétés de sécurité (incluant des propriétés de confidentialité, intégrité, et authentification) au contenu d'un corps MIME. Donc, toutes les mises en œuvre PIDF qui prennent en charge les extensions de schéma XML pour les informations de localisation décrites dans le présent document DOIVENT prendre en charge S/MIME ; en particulier, elles DOIVENT prendre en charge les types de contenu de CMS [RFC3852] EnvelopedData et SignedData, qui sont utilisés, respectivement, pour le chiffrement et pour les signatures numériques. On estime que ce mécanisme satisfait aux REQ 2.10, 13, 14.1, 14.2, 14.3, et 14.4.

De plus, toutes les applications conformes DOIVENT mettre en œuvre l'algorithme de chiffrement AES pour S/MIME, comme spécifié dans la [RFC3565] (et selon la REQ 15.1). Bien sûr, les mises en œuvre DOIVENT aussi prendre en charge les algorithmes de base de chiffrement et de signature numérique décrits dans la spécification S/MIME.

S/MIME englobe généralement l'utilisation de certificats X.509 [RFC3850]. Afin de chiffrer une demande pour une destination finale particulière (c'est-à-dire pour un receveur de localisation) le générateur de localisation doit posséder des accreditifs (normalement, un certificat X.509) qui ont été produits au receveur de localisation. Les mises en œuvre de la présente spécification DEVRAIENT prendre en charge les certificats X.509 pour S/MIME, et DOIVENT prendre en charge le chiffrement de CMS fondé sur le mot de passe (voir la [RFC3852]). Tous les systèmes de chiffrement symétrique DEVRAIENT déduire des clés de codage de contenu (CEK, *content encoding key*) à forte entropie. Lorsque des certificats

X.509 sont utilisés pour signer des objets de localisation PIDF, le `subjectAltName` du certificat DEVRAIT utiliser le schéma d'URI "pres".

Un modèle de déploiement envisagé pour S/MIME dans les documents PIDF est le suivant. Les serveurs de localisation détiennent des certificats X.509 et partagent des secrets avec les générateurs et les receveurs de localisation. Lorsque un générateur envoie des informations de localisation à un serveur, elle peuvent être chiffrées avec S/MIME (ou tout chiffrement de couche inférieure spécifique du protocole utilisateur). Lorsque un serveur transmet des informations de localisation à un receveur, les informations de localisation peuvent être chiffrées avec le chiffrement de CMS fondé sur le mot de passe. Cela permet l'utilisation du chiffrement lorsque le receveur de localisation ne possède pas son propre certificat X.509.

S/MIME a été conçu pour la sécurité de bout en bout entre les homologues de messagerie électronique qui communiquent à travers plusieurs serveurs (c'est-à-dire de agents de transfert de messagerie) qui ne modifient pas les corps de message. Il y a cependant au moins une instance dans laquelle les serveurs de localisation modifient les objets de localisation : quand les serveurs de localisation appliquent des politiques au nom du faiseur de règle. Par exemple, un faiseur de règle peut spécifier que des informations de localisation devraient être rendues plus grossières (moins spécifiques) avant de les transmettre à certains receveurs. Si le serveur de localisation est incapable de modifier un objet de localisation, parce qu'il est chiffré, signé, ou les deux, il sera dans l'incapacité d'accomplir cette fonction. Par conséquent, lorsque un générateur de localisation veut permettre à un serveur de localisation de modifier de tels messages, il PEUT chiffrer de tels messages avec une clé qui peut être déchiffrée par le serveur de localisation (la signature numérique peut bien sûr toujours être créée avec le matériel de chiffrement provenant du certificat du générateur de localisation). Après la modification de l'objet de localisation, le serveur de localisation peut resigner l'objet avec ses propres accreditifs (en le chiffrant avec toute clé produite par le receveur de localisation, si ils sont connus du serveur).

Noter que les politiques pour la collecte et l'usage des données d'informations de localisation, dans la mesure où elles sont portées au sein d'un objet de localisation, sont discutées au paragraphe 2.2.2.

5. Considérations pour la sécurité

Les menaces auxquelles doit faire face un protocole Internet qui porte des informations de géolocalisation sont détaillées dans la [RFC3694]. Les exigences qui ont été identifiées dans cette analyse du modèle de menaces ont été incorporées dans la [RFC3693], en particulier au paragraphe 7.4. Le présent document vise à être conforme aux exigences de sécurité déduites de ces deux engagements, dans la mesure où ils s'appliquent à l'objet de localisation lui-même (par opposition au protocole d'utilisation).

La sécurité de l'objet de localisation définie dans le présent document, incluant les exigences normatives pour les mises en œuvre, sont discutées à la Section 4. Cette sécurité se concentre sur l'intégrité de bout en bout et sur les propriétés de confidentialité qui sont appliquées à un objet de localisation pour sa durée de vie via S/MIME.

Les exigences de sécurité associées aux protocoles d'utilisation (incluant l'authentification des abonnés aux informations géographiques, etc.) sortent du domaine d'application du présent document.

6. Considérations relatives à l'IANA

6.1 Jetons 'method'

Le présent document demande que l'IANA crée un nouveau registre pour les jetons 'method' associés à l'objet PIDF-LO. Les jetons 'method' sont des chaînes de texte qui désignent la manière dont les informations de localisation dans un objet PIDF-LO ont été déduites ou découvertes. Tout le monde peut enregistrer de nouveaux jetons 'method' auprès de l'IANA, comme nécessaire, sur la base du premier arrivé, premier servi.

Cette section pré-enregistre 7 nouveaux jetons 'method' associés à l'élément 'method' décrit ci-dessus au paragraphe 2.2.3 :

GPS (*Global Positioning System*) système de positionnement mondial

A-GPS : GPS avec assistance

Manual : entré manuellement par un opérateur ou utilisateur, par exemple, sur la base d'un abonnement facturé ou d'un service d'informations de localisation

DHCP : fourni par DHCP (utilisé pour les réseaux d'accès filaires, voir 802.11 ci-dessous)

Triangulation : triangulé à partir de l'heure d'arrivée, de la force du signal, ou de mesures similaires

Cell : localisation de l'antenne radio cellulaire

802.11 : point d'accès 802.11 (utilisé pour le provisionnement DHCP sur réseau d'accès sans fil)

6.2 Éléments 'provided-by'

Le présent document demande à l'IANA de créer un nouveau registre d'espaces de noms XML pour les éléments 'provided-by' à utiliser avec les objets PIDF-LO. Les enregistrements de nouveaux espaces XML qui sont utilisés pour 'provided-by' DOIVENT être revus par un expert réviseur désigné par l'IESG.

Le présent document pré enregistre un seul espace de noms XML pour 'provided-by', qui est donné à l'Appendice A.

6.3 Enregistrement du sous espace de noms d'URN pou urn:ietf:params:xml:ns:pidf:geopriv10

Ce paragraphe enregistre un nouvel espace de noms XML, selon les directives de la [RFC3688].

URI : urn:ietf:params:xml:ns:pidf:geopriv10.

Contact de l'enregistreur : IETF, groupe de travail GEOPRIV, (geopriv@ietf.org), Jon Peterson (jon.peterson@neustar.biz).

XML :

DÉBUT

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
  "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
    content="text/html;charset=iso-8859-1"/>
  <title>GEOPRIV PIDF Extensions</title>
</head>
<body>
  <h1>PIDF Extensions of Geographical Information and Privacy</h1>
  <h2>urn:ietf:params:xml:ns:pidf:geopriv10</h2>
  <p>See <a href="ftp://ftp.rfc-editor.org/in-notes/rfc4119.txt">
    RFC4119</a>.</p>
</body>
</html>
FIN
```

7. Remerciements

Le présent document a été produit avec l'assistance de nombreux membres du groupe de travail GEOPRIV de l'IETF. Des remerciements particuliers à Carl Reed de OpenGIS pour sa relecture attentive du document.

Le format de localisation civique décrit dans le présent document a été proposé par Henning Schulzrinne pour la communication des informations de localisation dans DHCP, et a été approprié dans sa totalité pour le présent document.

James M. Polk a fourni le texte relatif à l'élément 'method', et beaucoup du texte pour l'élément 'provided-by'. Le texte de l'Appendice A a été écrit par Nadine Abbott.

Appendice A : Schéma NENA Provided-By

Ce qui suit enregistre l'espace de noms XML urn:ietf:params:xml:ns:pidf:geopriv10:dataProvider et le schéma associé ci-dessous, pour être utilisé dans l'élément 'provided-by' de PIDF-LO. L'espace de noms dataProvider a été développé par l'administration nationale du numéro d'urgence (NENA, *National Emergency Number Administration*) des USA pour les besoins des communications d'urgence de la prochaine génération.

Cet appendice n'est pas normatif pour les mises en œuvre de PIDF-LO et PEUT prendre en charge l'espace de noms dataProvider. Les autres enregistrements d'espaces de noms 'provided-by' sont invités à utiliser l'enregistrement ci-dessous comme exemple à titre d'information.

URI : l'URI pour cet espace de noms est urn:ietf:params:xml:ns:pidf:geopriv10:dataProvider
 Contact d'enregistrement : NENA, groupe de travail VoIP & groupe de travail GEOPRIV de l'IETF, (geopriv@ietf.org),
 Nadine Abbott (nabbott@telcordia.com).

XML :

DÉBUT

```
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN" http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd
>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
  <meta http-equiv="content-type"
    content="text/html; charset=iso-8859-1"/>
  <title>NENA dataProvider Schema for PIDF-LO</title>
</head>
<body>
  <h1>NENA dataProvider Schema for 'provided-by' in PIDF-LO</h1>
  <h2>urn:ietf:params:xml:ns:pidf:geopriv10:dataProvider</h2>
  <p>See <a href="ftp://ftp.rfc-editor.org/in-notes/rfc4119.txt">
    RFC4119</a>.</p>
</body>
</html>
FIN
```

A.1 Schéma XML dataProvider

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- édité avec XMLSPY v5 rel. 3 U (http://www.xmlspy.com) par Patricia Bluhm (HBF Group) -->
<xs:schema
  targetNamespace="urn:ietf:params:xml:ns:pidf:geopriv10:dataProvider"
  xmlns:tns="urn:ietf:params:xml:ns:pidf:geopriv10:dataProvider"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="nena" type="tns:DataProviderIDType"/>
  <xs:complexType name="DataProviderIDType">
<xs:annotation>
<xs:documentation>NENA registered Company ID for Service Provider supplying location information
</xs:documentation>
</xs:annotation>
  <xs:all>
    <xs:element name="DataProviderID"
      type="tns:NENACompanyIDType" minOccurs="0"/>
    <xs:element name="TelURI"
      type="tns:TelURI_24x7Type" minOccurs="0"/>
    <xs:element name="URL" type="xs:anyURI"
      minOccurs="0"/>
  </xs:all>
</xs:complexType>
  <xs:simpleType name="NENACompanyIDType">
    <xs:annotation>
      <xs:documentation>NENA registered Company ID.</xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:maxLength value="5"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="TelURI_24x7Type">
<xs:annotation>
<xs:documentation>24x7 Tel URI for the caller's [location data] service provider. To be used for contacting service
provider to resolve problems with location data. Possible values TN number, enumerated values when not
```

```

available.</xs:documentation>
  </xs:annotation>
  <xs:union memberTypes="xs:anyURI">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:maxLength value="10"/>
        <xs:enumeration value="NOT FOUND"/>
        <xs:enumeration value="UNAVAILABLE"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:union>
</xs:simpleType>
</xs:schema>

```

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](#))
- [RFC2392] E. Levinson, "Localisateur de ressource uniforme d'identifiant de contenu et d'identifiant de message", août 1998. (P.S.)
- [RFC3565] J. Schaad, "Utilisation de l'[algorithme de chiffrement de la norme de chiffrement évolué](#) (AES) dans la syntaxe de message cryptographique (CMS)", juillet 2003. (P.S.)
- [RFC3688] M. Mealling, "[Registre XML de l'IETF](#)", BCP 81, janvier 2004.
- [RFC3850] B. Ramsdell, éd., "Traitement de certificat d'extensions multi-objets/sécurisées de messagerie Internet (S/MIME) version 3.1", juillet 2004. (P.S.) (Remplacée par [RFC5750](#))
- [RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. (Remplacée par [RFC5751](#))
- [RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. (Remplacée par la [RFC5652](#))
- [RFC3859] J. Peterson, "[Profil commun pour les services de présence](#) (CPP)", août 2004. (P.S.)
- [RFC3863] H. Sugano et autres, "[Format des données d'information de présence](#) (PIDF)", août 2004.

Références pour information

- [OpenGIS] OpenGIS, "Open Geography Markup Language (GML) Implementation Specification", OGC 02-023r4, janvier 2003, < <http://www.opengeospatial.org/specs/?page=specs> >.
- [RFC2778] M. Day, J. Rosenberg et H. Sugano, "[Modèle pour Presence et la messagerie instantanée](#)", février 2000.
- [RFC3261] J. Rosenberg et autres, "SIP : [Protocole d'initialisation de session](#)", juin 2002. (Mise à jour par [RFC3265](#), [RFC3853](#), [RFC4320](#), [RFC4916](#), [RFC5393](#), [RFC6665](#), [RFC8217](#))
- [RFC3693] J. Cuellar et autres, "[Exigences pour Geopriv](#)", février 2004. (Information)
- [RFC3694] M. Danley et autres, "[Analyse des menaces](#) pour le protocole Geopriv", février 2004. (Information)
- [RFC4079] J. Peterson, "Architecture de présence pour la distribution d'objets de localisation GEOPRIV", juillet 2005. (Information)
- [[RFC6772](#)] H. Schulzrinne, éd., H. Tschofenig, éd., J. Cuellar, J. Polk, J. Morris et M. Thomson, "Politique de géolocalisation : format de document pour exprimer les préférences de confidentialité pour les informations de localisation", janvier 2013.

Adresse de l'auteur

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US

téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz
URI : <http://www.neustar.biz/>

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

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.