Groupe de tarvail Réseau
Request for Comments : 3693
Catégorie : Information

Traduction Claude Brière de L'Isle

J. Cuellar, Siemens AG
J. Morris, Center for Democracy & Technology
D. Mulligan, Samuelson Law, Technology & Public Policy Clinic
J. Peterson, NeuStar
J. Polk, Cisco
février 2004

Exigences pour Geopriv

Résumé
Les services fondés sur la localisation, applications de navigation, services d'urgence, gestion d'équipements sur le terrain, et autres services dépendants de la localisation ont besoin d'informations de localisation géographique sur une cible (comme un utilisateur, une ressource ou autre entité). Il y a un besoin de rassembler en toute sécurité et transférer les informations de localisation pour les services de localisation, tout en protégeant en même temps la confidentialité des individus impliqués.

Le présent document se concentre sur les exigences d'autorisation, de sécurité et de confidentialité pour de tels services dépendants de la localisation. Précisément, il décrit les exigences pour l'objet de localisation (LO) Geopriv et pour les protocoles qui utilisent cet objet de localisation. Ce LO est envisagé comme étant la principale structure de données utilisée dans tous les échanges de protocole Geopriv pour transférer en toute sécurité les données de localisation.

Table des Matières

1. Vue d'ensemble

Les services fondés sur la localisation (applications qui requièrent des informations de localisation géographique en entrée) deviennent de plus en plus courants. La collecte et le transfert des informations de localisation sur une cible particulière peuvent avoir d'importantes implications de confidentialité. Un objectif clé du protocole décrit dans le présent document est de faciliter la protection de la confidentialité conformément aux règles de confidentialité établies par "l'utilisateur/possesseur de la cible" (ou plus précisément dans la terminologie du présent document donnée à la Section 3 et au paragraphe 5.4, le "faiseur de règle").

La capacité de rassembler et générer la localisation d'une cible, et d'accéder à la localisation déduite ou calculée, est un élément clé de l'équation de confidentialité des services fondés sur la localisation. Centrales pour la confidentialité d'une cible sont (a) l'identité des entités qui ont accès aux données de localisation brutes, déduisent ou calculent la localisation, et/ou ont accès aux informations de localisation déduites ou calculées, et (b) si ces entités peuvent être de confiance quant à la connaissance et au suivi des règles de confidentialité de l'utilisateur.

Les principaux principes qui guident les exigences décrites dans le présent document sont :

1) La sécurité de la transmission de l'objet de localisation est essentielle pour garantir l'intégrité et la confidentialité des informations de localisation. Cela inclut d'authentifier l'envoyeur et le receveur de l'objet de localisation, et de sécuriser l'objet de localisation lui-même.

2) un rôle critique est joué par les règles de confidentialité contrôlées par l'utilisateur, qui décrivent les restrictions imposées ou les permissions données par "l'utilisateur" (ou, comme défini ci-dessous, le "faiseur de règle"). Les règles de confidentialité spécifient les conditions nécessaires qui permettent au serveur de localisation de transmettre les informations de localisation à un receveur de localisation, et les conditions et l'objet pour lesquelles les informations de localisation peuvent être utilisées.

3) Un type de règles de confidentialité spécifie comment les informations de localisation devraient être filtrées, selon qui est le receveur. Le filtrage est le processus de réduction de la précision ou de la résolution des données. Une règle typique peut être de la forme : "ma localisation ne peut être divulguée qu'au possesseur de tels accréditifs dans telle précision ou résolution" (par exemple, "on peut dire à mes camarades de travail dans quelle ville je me trouve actuellement").

4) L'objet de localisation devrait être capable de porter un ensemble limité mais central de règles de confidentialité. La forme exacte ou l'expressivité de ces règles dans l'ensemble central ou dans l'ensemble complet n'est pas discuté plus avant dans le présent document, mais sera discuté de façon plus extensive dans les documents futurs produits par ce groupe de travail.

5) Chaque fois qu'approprié, les informations de localisation ne devraient pas être reliées à l'identité réelle de l'utilisateur ou un identifiant statique facilement relié à l'identité réelle de l'utilisateur (c'est-à-dire, des informations personnellement identifiables comme un nom, une adresse de messagerie électronique, un numéro de téléphone, un numéro de sécurité sociale, une adresse ou nom d'utilisateur de messagerie électronique). Plutôt, l'utilisateur devrait être capable de spécifier quel identifiant local, pseudonyme sans lien, ou identifiant privé doit être lié aux informations de localisation.

6) L'utilisateur peut vouloir cacher les identités réelles de lui-même et de ses partenaires, non seulement aux espions mais aussi aux autres entités qui participent au protocole.

Bien qu'un anonymat complet puisse n'être pas approprié pour certaines applications à cause de contraintes légales ou parce que certains services de localisation puissent en fait avoir besoin d'une identification explicite, le plus souvent les services de localisation ont seulement besoin d'un certain type d'informations d'autorisation et/ou peut-être d'identifiants anonymes des entités en question.

2. Conventions utilisées dans ce 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].

Noter que les exigences discutées ici sont des exigences sur l'objet de localisation générique et sur l'utilisation des protocoles pour les services de localisation. Donc, pour la plus grande part, les exigences discutées dans le présent document se réfèrent aux capacités qu'il est obligatoire de mettre en œuvre. Par exemple, exiger que les mises en œuvre prennent en charge la protection de l'intégrité n'est pas la même chose que d'exiger que tout le trafic de protocole soit authentifié. À l'opposé, un exemple d'exigence d'utilisation obligatoire (pas juste de mise en œuvre obligatoire) pourrait être celle qui déclare que l'utilisateur reçoit toujours une notification lorsque les données de localisation n'étaient pas authentifiées. Cette pratique est d'utilisation obligatoire, pas simplement de mise en œuvre.

3. Glossaire

Pour faciliter les références et la lisibilité, on présente ci-dessous les termes de base qui seront définis de façon plus formelle et complète plus loin dans le présent document.

Générateur de localisation (LG, *Location Generator*) : entité qui détermine ou rassemble initialement la localisation de la cible et crée les objets de localisation qui décrivent la localisation de la cible.

Objet de localisation (LO) : objet qui porte les informations de localisation (et éventuellement des règles de confidentialité) auxquelles les mécanismes de sécurité Geopriv et les règles de confidentialité sont à appliquer.

Receveur de localisation (LR, *Location Recipient*) : entité qui reçoit les informations de localisation. Il peut avoir demandé explicitement cette localisation (en envoyant une interrogation à un serveur de localisation) ou il peut recevoir cette localisation de façon asynchrone.

Serveur de localisation (LS, *Location Server*) : entité à laquelle le LG publie les objets de localisation, le receveur des interrogations provenant des receveurs de localisation, et l'entité qui applique les règles conçues par le faiseur de règle.

Précision : nombre de chiffres significatifs auxquels une valeur a été mesurée de façon fiable.

Principal : détenteur/sujet des accréditifs, par exemple, une station de travail d'utilisateur ou un serveur réseau.

Résolution : finesse de détail qui peut être distinguée dans une zone mesurée. Appliquée à Geopriv, cela signifie la zone finie au sein de bordures fournies et closes (par exemple, des limites de latitude et longitude).

Détenteur de règle *(Rule Holder)* : entité qui fournit les règles associées à une cible particulière pour la distribution des informations de localisation. Il peut "pousser" les règles à un serveur de localisation, ou un serveur de localisation peut "tirer" les règles d'un détenteur de règle.

Faiseur de règle *(Rule Maker)* : autorité qui crée les règles qui gouvernent l'accès aux informations de localisation pour une cible (normalement, c'est la cible elle-même).

Règle, ou règle de confidentialité : directive qui régule les activités d'une entité par rapport aux informations de localisation, incluant la collecte, l'utilisation, la divulgation, et la rétention des informations de localisation.

Cible : personne ou autre entité dont la localisation est communiquée par un objet de localisation Geopriv.

Protocole utilisateur : protocole qui porte un objet de localisation.

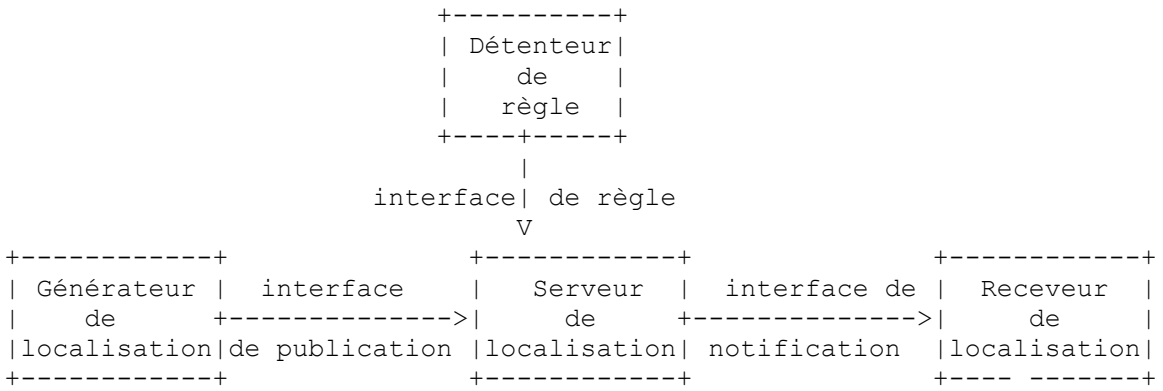
Visionneur : principal qui consomme les informations de localisation qui sont communiquées par un objet de localisation Geopriv, mais ne passe pas ces informations plus loin.

Résolution et précision sont des termes très proches. Leur qualité peut être "réduite" pour rendre plus grossières les informations de localisation : la "résolution", en définissant un périmètre hors centre autour de la localisation d'un utilisateur ou en élargissant d'autre façon la zone considérée (disons de la région au pays) et la "précision" en éliminant des

chiffres significatifs d'informations de positionnement (disons, en arrondissant la longitude et la latitude des secondes aux minutes). Un autre document du groupe de travail discute de cela plus en détails.

4. Principales entités Geopriv

Le schéma suivant montre les principales entités Geopriv dans une architecture de base simple, sans prétendre être complet ni suggérer que les entités identifiées doivent dans tous les cas être des entités physiquement séparées.



Les quatre principales entités sont décrites comme suit :

Générateur de localisation (LG, *Location Generator*) : entité qui détermine ou rassemble initialement la localisation de la cible et crée des objets de localisation décrivant cette localisation. Les LG publient les objets de localisation sur les serveurs de localisation. La manière dont le générateur de localisation apprend les informations de localisation sort du domaine d'application du protocole Geopriv.

Serveur de localisation (LS, *Location Server*) : le LS est un élément qui reçoit les publications d'objets de localisation des générateurs de localisation et peut recevoir des abonnements de la part des receveurs de localisation. Le LS applique les règles (qu'il apprend du détenteur de règle) aux LO qu'il reçoit des LG, et notifie alors aux LR les LO résultants comme nécessaire.

Receveur de localisation (LR, *Location Recipient*) : le LR est un élément qui reçoit des notifications d'objets de localisation des serveurs de localisation. Le LR peut rendre ces LO de certaines façons à un utilisateur ou à un automate .

Détenteur de règle (RH, *Rule Holder*) : le RH est un élément qui héberge les règles de confidentialité pour la réception, le filtrage et la distribution des objets de localisation pour des cibles spécifiques. Un LS peut interroger un RH sur un ensemble de règles, ou les règles peuvent être poussées du RH à un LS. Les règles dans le détenteur de règle sont remplies par le faiseur de règle.

Donc la génération de localisation est le processus de rassemblement des informations de localisation, peut-être à partir de multiples sources, chez une entité Geopriv fondée sur IP, le LG, qui communique avec les autres entités Geopriv.

Les règles DOIVENT être authentifiées et protégées. Comment cela est fait et en particulier comment distribuer les clés au RM et aux autres autorités sort du domaine d'application du présent document. Voir aussi le paragraphe 8.2, "Sécurisation des règles de confidentialité".

Les interfaces entre les entités Geopriv ne sont pas nécessairement des interfaces du protocole ; elles pourraient être des interfaces internes au sein d'un seul appareil composé. Dans certaines architectures, le générateur de localisation, le détenteur de règles, et le serveur de localisation peuvent tous être mis en œuvre dans le même appareil. Il peut y avoir plusieurs détenteurs de règles qui appliquent les règles de confidentialité chez un serveur de localisation particulier.

5. Autre terminologie Geopriv

La terminologie et les définitions détaillées ci-dessous incluent des termes qui, en dehors des entités Geopriv principales, (1) sont utilisées dans la section exigences du présent document, et (2) fournissent des détails supplémentaires sur le modèle d'usage envisagé pour l'objet de localisation Geopriv. Ces derniers termes seront utilisés dans un autre document de scénarios et ailleurs.

5.1 Informations de localisation et visée

L'objet du groupe de travail Geopriv est les informations sur la localisation d'une cible qui NE se fonde PAS sur des sources généralement ou publiquement disponibles, mais plutôt sur des informations privées fournies ou créées par une cible, un appareil d'une cible, ou le réseau ou le fournisseur de service d'une cible. En dépit de cette focalisation sur les informations de localisation privées, l'objet de localisation Geopriv pourrait certainement être utilisé pour porter des informations de localisation à partir de sources publiquement disponibles.

Informations de localisation : façon relativement spécifique de décrire où est situé un appareil.

Ces informations de localisation peuvent avoir été déterminées de nombreuses façons différentes, incluant : (a) déduites ou calculées à partir d'informations généralement non disponibles au public général (comme des informations principalement disponibles pour un fournisseur de réseau ou de service) (b) déterminées par un appareil qui peut n'être pas généralement adressable ou accessible au public, ou (c) des entrées ou autres fournies par une cible.

Comme exemples, les informations de localisation pourraient inclure (a) les informations calculées par triangulation sur un signal sans fil par rapport aux tours de téléphone cellulaire, (b) les informations de latitude et longitude déterminées par un appareil avec des capacités de positionnement global par satellite (GPS, *global positioning satellite*) (c) des informations entrées manuellement dans un téléphone cellulaire ou une tablette par une cible en réponse à une interrogation, ou (d) automatiquement livrées par quelque autre protocole IP, comme à une configuration d'appareil via DHCP.

On exclu de cette définition la détermination des informations de localisation qui sont entièrement à l'insu ou sans le consentement de la cible (ou du réseau ou fournisseur de service d'accès de la cible) sur la base des informations généralement disponibles comme une adresse IP ou de messagerie électronique. Dans certains cas, des informations comme l'adresse IP peuvent permettre à quelqu'un d'estimer (au moins grossièrement) une localisation. Il existe des services commerciaux qui fournissent des informations de localisation grossières sur la base des adresses IP. Actuellement, ce type d'informations de localisation est normalement moins précis que le type d'informations de localisation visées par le présent document. Bien que ce type de calcul de localisation soulève aussi de potentiellement sérieuses questions de confidentialité et de protection de la vie privée, de tels scénarios sortent généralement du domaine d'application du présent document.

Dans toute transaction fondée sur la localisation, la détermination INITIALE de la localisation (et donc la création initiale des informations de localisation) est appelée un pointage *(Sighting)* :

Pointage : détermination initiale de localisation fondée sur des informations non publiques (comme expliqué dans la définition des informations de localisation) et création initiale d'informations de localisation. Une variante des informations de pointage est incluse dans l'objet de localisation. De façon abstraite, il consiste en deux champs de données séparés : (Identifiant, Localisation) où l'identifiant est l'identifiant alloué à une cible qui est pointée, et Localisation est la position actuelle de cette cible qui est pointée. Toutes les entités peuvent ne pas avoir accès à exactement les même éléments d'informations de pointage. Un pointage peut être transformé en une nouvelle paire de pointage : (Identifiant-1, Localisation-1) avant qu'il soit fourni par un générateur de localisation ou serveur de localisation au receveur de localisation. Dans ce cas, Identifiant-1 peut être un pseudonyme, et Localisation-1 peut avoir moins de précision ou résolution que la valeur originale.

5.2 Objet de localisation et protocole utilisateur

Un des principaux objectifs du groupe de travail Geopriv est de définir un objet de localisation (LO), à utiliser pour convoyer à la fois les informations de localisation et les instructions de base de protection de la confidentialité :

Objet de localisation (LO) : ces données contiennent les informations de localisation de la cible, et d'autres champs incluant une identité ou un pseudonyme de la cible, des informations horaires, les règles cœur de confidentialité, des authentifiants, etc. La plupart de ces champs sont facultatifs, y compris les informations de localisation elles-mêmes.

Rien n'est dit sur la sémantique d'un champ manquant. Par exemple, un objet partiellement rempli PEUT être compris implicitement comme une demande de le compléter. Ou, si aucune information horaire n'est incluse, cela PEUT implicitement signifier "au moment présent" ou "très récemment", mais cela pourrait être interprété différemment, selon le contexte.

Le "protocole utilisateur" est le protocole qui utilise (lit ou modifie) l'objet de localisation. Un protocole qui transporte juste le LO comme une chaîne de bits, sans les regarder (comme un protocole de mémorisation IP pourrait le faire) n'est pas un protocole utilisateur, mais seulement un protocole de transport. Néanmoins, l'entité ou protocole qui a causé déplacement

du LO est responsable de la distribution, protection, usage, rétention, et mémorisation appropriées du LO sur la base des règles qui s'appliquent à ce LO.

Les mécanismes d'amélioration de la sécurité et de la confidentialité utilisés pour protéger le LO sont de deux types : d'abord, la définition de l'objet de localisation DOIT inclure les champs ou mécanismes utilisés pour sécuriser le LO en tant que tel. Le LO PEUT être sécurisé, par exemple, en utilisant des sommes de contrôle cryptographiques ou un chiffrement au titre du LO lui-même. Ensuite, le protocole utilisateur peut aussi fournir des mécanismes de sécurité pour transporter l'objet de localisation en toute sécurité.

Lors de la définition du LO, la conception devrait respecter que les mécanismes de sécurité de l'objet de localisation lui-même doivent être préférés. Donc la définition du LO DOIT inclure une fonctionnalité de chiffrement minimale (Req. 14 et 15). De plus, si le RM spécifie l'utilisation d'un mécanisme de sécurité de LO particulier, il DOIT être utilisé (Req. 4).

5.3 Flux de données de confiance et non de confiance

Les informations de localisation peuvent être utilisées dans des environnements très différents. Dans certains cas, les participants vont avoir des relations à long terme, tandis que dans d'autres, les participants peuvent avoir des interactions éphémères sans contact contractuel ou autre préalable.

Les relations différentes soulèvent des problèmes différents pour la mise en œuvre des règles de confidentialité, incluant le besoin de communiquer les règles de confidentialité. Un détenteur de règle public, par exemple, peut être inutile dans un environnement de confiance où existent des méthodes plus efficaces pour régler les problèmes de confidentialité. Les termes suivants distinguent les deux types de base de flux de données :

Flux de données de confiance : flux de données qui est gouverné par une relation contractuelle préexistante qui traite la confidentialité de la localisation.

Flux de données qui n'est pas de confiance : le flux de données n'est pas gouverné par une relation contractuelle préexistante qui traite la confidentialité de la localisation.

5.4 Autres principaux Geopriv

Cible : entité dont la localisation est désirée par le receveur de localisation. Dans de nombreux cas, la cible sera l'utilisateur humain d'un appareil ou objet comme un véhicule ou un conteneur auquel l'appareil est rattaché. Dans certaines instances, la cible sera l'appareil lui-même.

Appareil : appareil technique par lequel la localisation est retracée comme un mandataire pour la localisation d'une cible. Un appareil peut, par exemple, être un téléphone cellulaire, un receveur de satellite de positionnement mondial (GPS, *Global Positioning Satellite*) une tablette équipée d'un appareil d'accès sans fil, ou un émetteur qui produit un signal qui peut être retracé ou localisé. Dans certaines situations, comme lorsque une cible entre manuellement des informations de localisation (peut-être avec un navigateur de la Toile) la cible effectue la fonction d'un appareil.

Faiseur de règle (RM, *Rule Maker*) : individu ou entité qui a l'autorisation d'établir les règles de confidentialité applicables à une cible Geopriv potentielle. Dans de nombreux cas, ce sera le possesseur de l'appareil, et dans d'autres cas, ce peut être l'utilisateur qui est en possession de l'appareil. Par exemple, des parents peuvent contrôler ce qui arrive aux informations de localisation déduites du téléphone cellulaire de leur enfant. Une entreprise, à l'opposé, peut posséder et fournir un téléphone cellulaire à un employé mais lui permettre d'établir les règles de confidentialité. Il y a quatre scénarios dans lesquels des formes de contrainte ou d'outrepassement peuvent être imposées aux règles de confidentialité du faiseur de règle :

1. Dans le cas de services d'urgence (comme le E911 aux États-Unis) les lois locales ou nationales peuvent exiger que des informations de localisation précises soient transmises dans certaines situations d'appel d'urgence définies. Le groupe de travail Geopriv DOIT faciliter ces situations.

2. Dans le cas d'interception légale, le RM peut n'être pas au courant d'une directive d'outrepassement imposée par une autorité légale. Il n'est pas attendu du groupe de travail que des dispositions particulières soient prises pour faciliter cette situation.

3. Dans le contexte d'une relations de travail ou autres relations contractuelles, le possesseur d'une localisation particulière (comme sur un campus d'entreprise) peut imposer des contraintes à l'utilisation des règles de confidentialité par un faiseur de règle. Il n'est pas attendu du groupe de travail que des dispositions particulières soient prises pour faciliter

cette situation.

4. Il est concevable qu'une autorité gouvernementale puisse chercher à imposer des contraintes sur l'utilisation de règles de confidentialité par un faiseur de règle dans des situations qui ne sont pas d'urgence. Il n'est pas attendu du groupe de travail que des dispositions particulières soient prises pour faciliter cette situation.

Visionneur : individu ou entité qui reçoit des données de localisation sur une cible et ne transmet pas les informations de localisation ou les informations fondées sur la localisation d'une cible (comme des directions de conduite vers ou depuis la cible) à toute autre partie que la cible ou le faiseur de règle.

Transporteur de données : entité ou réseau qui reçoit et transmet les données sans les traiter ou les altérer. Un transporteur de données pourrait théoriquement être impliqué dans presque toutes les transmissions entre un appareil et un serveur de localisation, un serveur de localisation et un second serveur de localisation, ou un serveur de localisation et un visionneur. Certains scénarios de retraçage de localisation peuvent ne pas impliquer de transporteur de données.

Fournisseur d'accès (AP, *Access Provider*) : domaine qui fournit l'accès réseau initial ou d'autres services de communications de données essentiels pour le fonctionnement des fonctions de communications de l'appareil ou de l'équipement informatique dans lequel fonctionne l'appareil. Souvent, l'AP – qui sera un transporteur sans fil, un fournisseur d'accès Internet, ou un réseau d'entreprise interne – contient le LG. Parfois, le AP a un LG "sourd", qui transmet les LO Geopriv mais n'utilise aucune partie de l'objet de localisation Geopriv. D'autres cas peuvent ne pas impliquer d'AP, ou l'AP peut agir seulement comme transporteur de données.

Mémorisation de localisation : appareil ou entité qui mémorise des informations de localisation brutes ou traitées, comme une base de données, pour toute durée supérieure à la durée nécessaire pour achever une transaction immédiate concernant les informations de localisation.

L'existence et la pratique de la mémorisation des données de la mémorisation de localisation est cruciale pour les considérations de confidentialité, parce que cela peut influencer quelles informations de localisation seront finalement révélées (par la distribution ultérieure, une rupture technique, ou un processus légal).

5.5 Règles de confidentialité

Les règles de confidentialité sont les règles qui régulent les activités d'une entité à l'égard de la localisation et autres informations, incluant, sans s'y limiter, la collecte, l'utilisation, la divulgation, et la rétention des informations de localisation. De telles règles se fondent généralement sur des pratiques d'information équitables, comme précisé dans (par exemple) les lignes directrices de l'OCDE sur la protection de la confidentialité et les flux transfrontières de données personnelles [OECD].

Règle de confidentialité : règle ou ensemble de règles qui régulent les activités d'une entité à l'égard des informations de localisation, incluant la collecte, l'utilisation, la divulgation, et la rétention des informations de localisation. En particulier, la règle décrit comment les informations de localisation peuvent être utilisées par une entité et quelles informations de localisation transformées peuvent être livrées à quelles entités dans quelles conditions. Les règles doivent être respectées ; elles ne sont pas facultatives.

Un ensemble complet de règles de confidentialité va probablement inclure à la fois des règles qui n'ont qu'une seule signification technique possible, et des règles qui seront affectées par les lois et coutumes prévalentes du lieu. Par exemple, une règle de distribution de la forme "ma localisation ne peut être divulguée qu'au possesseur de tels accréditifs et dans telle précision ou résolution" a des implications clairement tranchées pour le protocole qui utilise le LO. Mais d'autres règles, comme des règles de rétention ou d'usage, peuvent avoir des conséquences techniques moins claires pour le protocole ou pour les entités impliquées. Par exemple, la portée précise d'une règle de rétention déclarant "vous ne devez pas mémoriser ma localisation pendant plus de deux jours" peut en partie s'opposer à des lois ou coutumes locales.

5.6 Identifiants, authentification et autorisation

L'anonymat est la propriété de n'être pas identifiable (au sein d'un ensemble de sujets). L'anonymat sert de cas de base pour la confidentialité : sans la capacité de rester anonymes, les individus peuvent être dans l'incapacité de contrôler leur propre vie privée. L'impossibilité de faire un lien avec un individu assure à un utilisateur qu'il peut faire plusieurs utilisations d'une ressource ou d'un service sans que d'autres soient capables de faire le lien entre ces diverses utilisations. L'impossibilité de faire un lien avec un individu exige que les entités soient incapables de déterminer si le même utilisateur a causé certaines opérations spécifiques dans le système [ISO99]. Un pseudonyme est simplement une chaîne binaire qui est unique comme identifiant et convient pour être utilisée pour l'authentification de point d'extrémité.

Pseudonyme non relié : pseudonyme où le lien entre le pseudonyme et son détenteur n'est, au moins initialement, connu de personne à l'exception possible du détenteur lui-même ou d'un serveur de confiance pour l'utilisateur. Voir [Pfi01] (le terme qui y est utilisé est "Pseudonyme non relié initialement").

Le mot d'authentification est utilisé de différentes manières. Certaines exigent que l'authentification associe une entité à une identité plus ou moins bien connue. Cela signifie fondamentalement que si A authentifie une autre entité B comme étant "id-B", alors l'étiquette "id-B" est une identité bien connue, ou au moins reliable à l'entité. Dans ce cas, l'étiquette "id-B" est appelée un identifiant connu publiquement, et l'authentification est "explicite".

Authentification explicite : acte de vérifier une identité revendiquée comme seule génératrice d'un message (authentification de message) ou comme point d'extrémité d'un canal (authentification d'entité). De plus, cette identité est facilement reliée à l'identité réelle de l'entité en question, par exemple en étant une étiquette statique préexistante provenant d'un espace de noms prédéfini (numéro de téléphone, nom, etc.)

Autorisation : acte de déterminer si un droit particulier, comme d'accéder à certaines ressources, peut être accordé au présentateur d'un accréditif particulier.

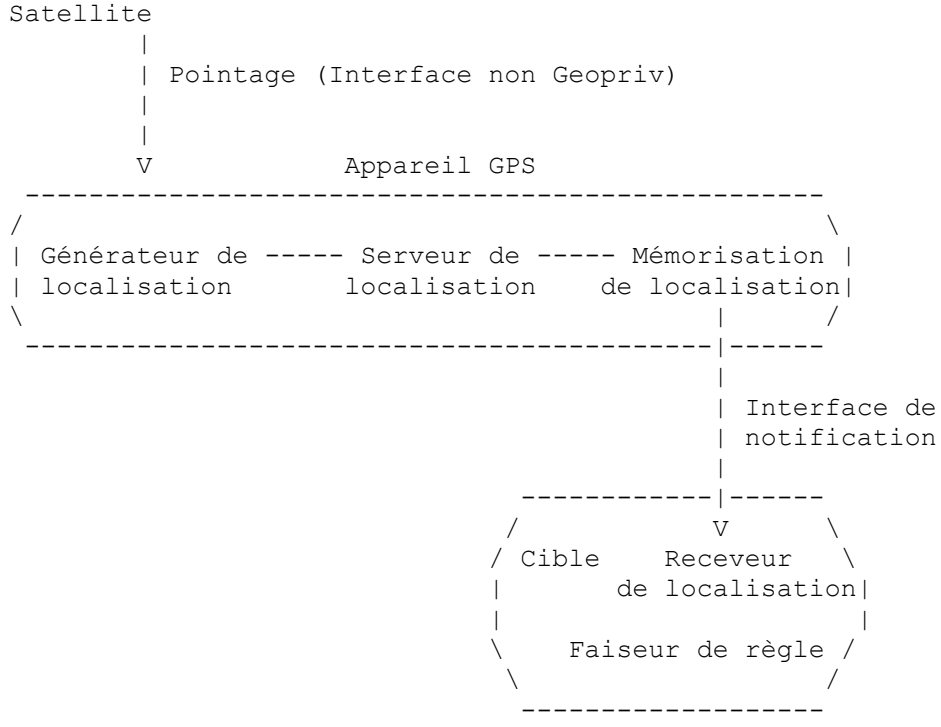
Selon le type d'accréditif, l'autorisation peut impliquer ou non une authentification explicite.

6. Scénarios et explications

On présente dans cette Section de courts scénarios qui illustrent comment ces termes et attributs décrivent les transactions d'informations de localisation. Des scénarios illustratifs supplémentaires sont présentés dans un document séparé.

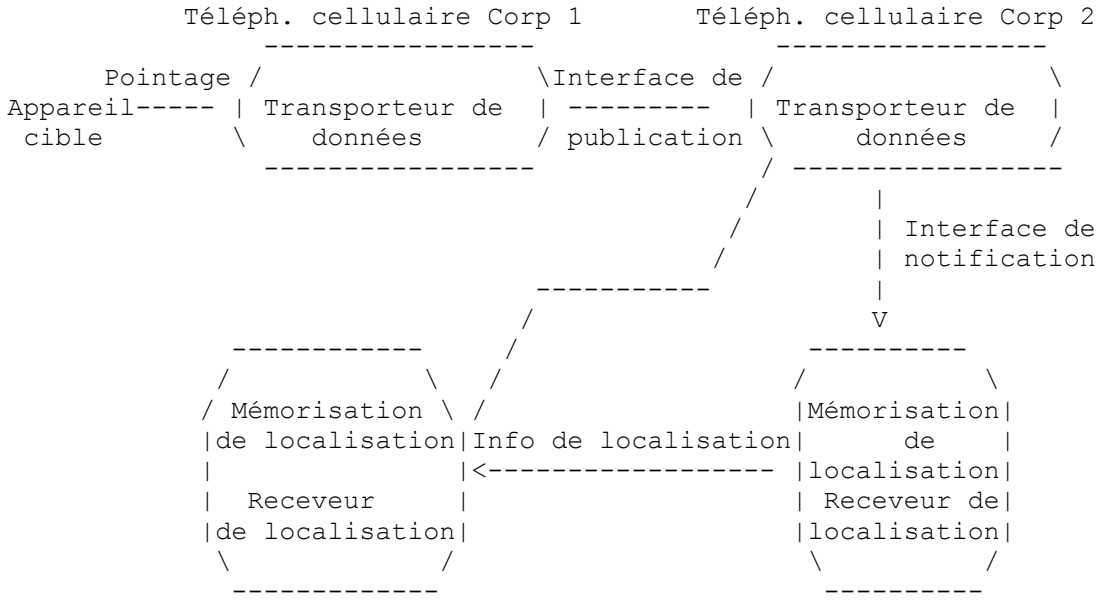
Scénario 1 : Appareil GPS avec puissance de calcul interne : système clos

Dans cet exemple, la cible souhaite connaître sa localisation en utilisant le système mondial de positionnement (GPS, *Global Positioning System*) et l'appareil est capable de traiter indépendamment les données brutes pour déterminer sa localisation. La localisation est déduite comme suit : l'appareil reçoit les transmissions du satellite GPS, calcule en interne et affiche la localisation. C'est un système clos. Pour les besoins de cet exemple et des suivants, on suppose que le satellite GPS diffuse un signal, et n'a pas d'information sur l'identité ni les tenants et aboutissants des appareils qui utilisent le signal.



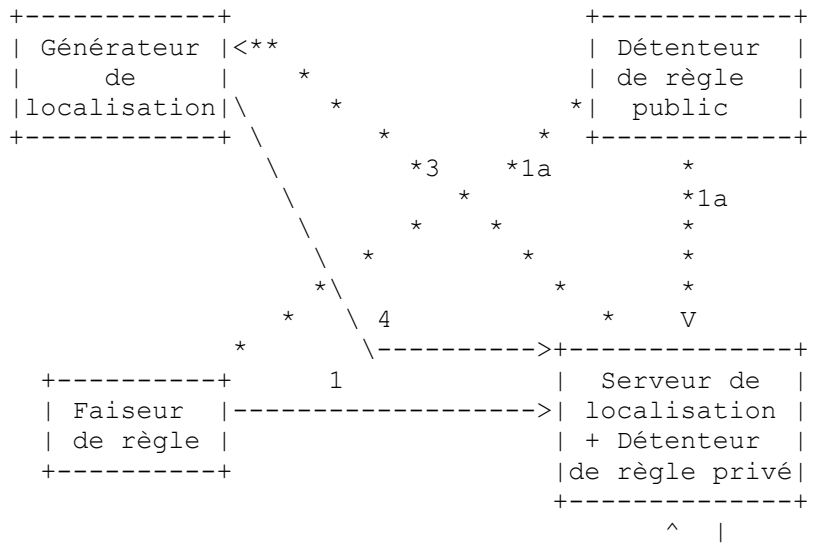
Dans ce scénario l'appareil GPS est à la fois l'AP et le LG. L'interaction survient dans un environnement de confiance parce que elle se fait dans l'appareil du faiseur de règle.

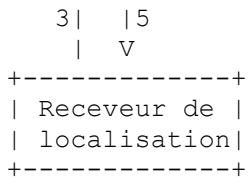
Scénario 2 : Itinérance de téléphone cellulaire
Dans cet exemple, un téléphone cellulaire est utilisé en dehors de sa zone de service de rattachement (en itinérance). Aussi, le fournisseur du service de téléphone cellulaire (téléphone cellulaire Corp 2) a exporté la comptabilité de l'usage du téléphone cellulaire. Le téléphone cellulaire n'a pas la capacité GPS. La localisation est déduite par le réseau de téléphone cellulaire dans lequel la cible et l'appareil sont en itinérance. Quand la cible souhaite utiliser le téléphone cellulaire, "téléphone cellulaire Corp 1" (AP) fournit le service d'itinérance pour la cible, qui envoie les données brutes sur l'usage (par exemple, la durée de l'appel, la localisation dans le réseau d'itinérance, etc.) à "téléphone cellulaire Corp 2", le fournisseur de service de rattachement. "Téléphone cellulaire Corp 2 soumet les données brutes à la société de facturation, qui traite les données brutes pour les déclarations comptables. Finalement, les données brutes sont envoyées à un centre de traitement de données ou les données brutes sont mémorisées dans un serveur de localisation (par exemple, serveur informatique).



Ici, "téléphone cellulaire Corp 1" est l'AP e t le LG. Dans ce scénario, "téléphone cellulaire Corp 2" est vraisemblablement une entité de confiance, mais "téléphone cellulaire Corp 1" peut être non de confiance.

Scénario 3 : Communautés mobiles et services fondés sur la localisation
La figure ci-dessous montre un scénario courant, où un utilisateur veut trouver ses amis ou collègues ou veut partager sa position avec eux ou avec un fournisseur de service fondé sur la localisation. Certains des messages utilisent un objet de localisation pour porter, par exemple, des identités ou des pseudonymes, des accréditifs et des preuves de leur possession, des informations de données de règles et de localisation, incluant des types de données de précision ou résolution. Les messages qui n'utilisent pas d'objet de localisation et sortent du domaine d'application de Geopriv, mais devraient être mentionnés pour la compréhension sont montrés dans la figure par des flèches à étoiles ("***>").





Supposons que le faiseur de règle et la cible soient enregistrés au serveur de localisation. Le RM a prouvé d'une certaine manière au LS qu'il est bien le possesseur des droits de confidentialité de la cible (la cible est généralement un appareil qui appartient au faiseur de règle). Le faiseur de règle et le serveur de localisation se sont accordés sur l'ensemble de clés ou accréditifs et matériel cryptographique qu'ils vont utiliser pour s'authentifier l'un l'autre, et en particulier, pour authentifier ou signer les règles. Comment cela a pu être fait sort du domaine d'application de ce document.

1 : Transfert de règle : le faiseur de règle envoie une règle au serveur de localisation. Cette règle peut être ou non un champ dans un objet de localisation.

1a : Règle signée : comme solution de remplacement, le faiseur de règle peut écrire une règle et la placer dans un détenteur de règle public. L'entité accède au répertoire pour lire les règles signées.

2 : Demande d'informations de localisation : le receveur de localisation demande des informations de localisation pour une cible. Dans cette demande, le receveur de localisation peut choisir quel type de données d'informations de localisation il préfère. Une façon de demander des informations de localisation PEUT être d'envoyer un objet de localisation partiellement rempli, incluant seulement les identités de la cible et du receveur de localisation et le type de données désirées avec leur précision ou résolution, et en fournissant une preuve de possession des accréditifs requis. Mais que le protocole utilisateur comprenne cet objet partiellement rempli comme une demande PEUT dépendre du protocole utilisateur ou du contexte. Le receveur de localisation pourrait aussi spécifier le besoin de mises à jour périodiques des informations de localisation, mais ceci sort probablement du domaine d'application de Geopriv.

3 : Localisation : quand un serveur de localisation reçoit une demande d'informations de localisation pour une cible qui n'a pas d'informations de localisation actuelles, le serveur peut demander au générateur de localisation de localiser la cible.

4 : Informations de localisation : le générateur de localisation envoie les informations de localisation "complètes" au serveur de localisation. Ces informations de localisation peuvent être ou non incorporées dans un objet de localisation.

5 : Informations de localisation filtrées : le serveur de localisation envoie les informations de localisation au receveur de localisation. Les informations peuvent être filtrées en ce sens qu'en général une version moins précise ou calculées des informations est livrée.

7. Exigences

7.1 Objet de localisation

On rappelle que le présent document est principalement destiné à spécifier les exigences pour la définition du LO. Certaines exigence disent : "La définition de LO DOIT contenir le champ 'A' comme champ facultatif". Cette exigence signifie que :
- o le document qui définit le LO DOIT définir le champ de LO 'A',
- o le champ 'A' DOIT être défini comme d'utilisation facultative (une instance de LO PEUT ou non contenir le champ 'A').

Certaines exigences disent : "La définition de LO DOIT contenir le champ 'A', qui PEUT être un champ facultatif". Cette exigence signifie que :
- o le document qui définit le LO DOIT définir le champ de LO 'A',
- o le champ 'A' PEUT être défini comme d'utilisation facultative ou non. Si il est défini comme d'utilisation facultative, toute instance d'un LO PEUT ou non contenir le champ 'A' ; si il n'est pas facultatif, toutes les instances de LO DOIVENT contenir le champ 'A'.

Req. 1. (généralité sur l'objet de localisation)

1.1) Geopriv DOIT définir un objet de localisation (LO) – sa syntaxe et sa sémantique – qui doivent être prises en charge par toutes les entités Geopriv.

1.2) Certains champs de l'objet de localisation PEUVENT être facultatifs. Cela signifie qu'une instance d'un objet de

localisation PEUT ou non contenir les champs.

1.3) Certains champs de l'objet de localisation PEUVENT être définis comme des "extensions". Cela signifie que la syntaxe ou la sémantique de ces champs n'est pas complètement définie dans la définition de base de l'objet de localisation, mais que leur utilisation peut être réservée à un ou plusieurs des protocoles utilisateurs.

1.4) L'objet de localisation DOIT être extensible, permettant la définition de nouveaux attributs ou champs.

1.5) L'objet DOIT convenir pour demander et recevoir une localisation.

1.6) L'objet DOIT permettre (mais pas exiger) que les règles de confidentialité soient appliquées par un tiers.

1.7) L'objet DOIT être utilisable dans divers protocoles, comme HTTP et SIP, ainsi que dans des API locales.

1.8) L'objet DOIT être utilisable de façon sûre même par des applications sur des appareils contraints.

Req. 2. (champs de l'objet de localisation)
La définition de l'objet de localisation DOIT contenir les champs suivants, qui PEUVENT être d'utilisation facultative :

2.1) Identifiant de cible

2.2) Identité du receveur de localisation. Cette identité peut être une identité de diffusion groupée ou de groupe, utilisée pour inclure l'objet de localisation dans les protocoles utilisateurs fondés sur la diffusion groupée.

2.3) Accréditif de receveur de localisation

2.4) Preuve de possession de l'accréditif du receveur de localisation

2.5) Champ de localisation
2.5.1) Vecteurs de mouvement et de direction. Ce champ DOIT être facultatif.

2.6) Type de données de localisation
Lors de la transmission de l'objet de localisation, l'envoyeur et le receveur doivent s'accorder sur le type des données d'informations de localisation. Le protocole utilisateur peut spécifier que les informations de type de données font partie de l'objet de localisation ou que l'envoyeur et le receveur se sont mis d'accord avant le transfert de données réel.

2.7) Informations d'instant :
(a) Quand les informations de localisation sont elles pertinentes (moment du pointage)
(b) Jusqu'à quand sont elles considérées comme actuelles ? Durée de vie (TTL, *Time-to-live*) (C'est différent d'une règle de confidentialité mettant une limite à la rétention des données).

2.8) Champ Règle : ce champ PEUT être une référence à une règle applicable (par exemple, un URI à une règle complète) ou il PEUT contenir une règle limitée (voir la Req. 11) ou les deux.

2.9) En-tête et en queue de sécurité (par exemple des informations de chiffrement, des hachages, ou signatures) (voir les Req. 14 et 15).

2.10) Numéro de version

Req. 3. (Types de données de localisation)

3.1) L'objet de localisation DOIT définir au moins un type de données de localisation à prendre en charge par tous les receveurs Geopriv (entités qui reçoivent des LO).

3.2) L'objet de localisation DEVRAIT définir deux types de données de localisation : un pour les coordonnées de latitude/longitude/altitude et un pour les localisations civiles (commune, rue, numéro) prises en charge par tous les receveurs Geopriv (entités qui reçoivent les LO).

3.3) Le type de données latitude/longitude/altitude DEVRAIT aussi prendre en charge un format de différences en plus d'un en valeur absolue, utilisé afin de réduire la taille des paquetages ou les besoins de sécurité et confidentialité.

3.4) La définition de l'objet de localisation DEVRAIT s'accorder sur les autres types de données de localisation pris en

charge par certaines entités Geopriv et définis par d'autres organisations.

7.2 Protocole utilisateur

Req. 4. Le protocole utilisateur doit obéir aux instructions de confidentialité et de sécurité codées dans l'objet de localisation et dans les règles correspondantes concernant la transmission et la mémorisation du LO.

Req. 5. Le protocole utilisateur va normalement faciliter le transport des clés associées aux accréditifs aux parties respectives, c'est-à-dire, que l'établissement des clés est de la responsabilité du protocole utilisateur.

Req. 6. (Transfert d'un seul message) En particulier, pour tracer de petits appareils cibles, la conception devrait permettre la transmission d'un seul message/paquet de localisation comme une transaction complète.

D'autres exigences sur le protocole utilisateur sortent du domaine d'application du présent document, mais pourraient être l'objet de futurs travaux de ce groupe de travail. Voir aussi la Section 9 (Questions de protocole et de LO remises à plus tard).

7.3 Transfert de données de localisation fondé sur la règle

Req. 7. (Règles de LS) La décision d'un serveur de localisation de donner à un receveur de localisation l'accès aux informations de localisation DOIT se fonder sur des règles de confidentialité définies par le faiseur de règle.

Il sort de notre domaine d'application de dire comment les règles de confidentialité sont gérées et comment un serveur de localisation a accès aux règles de confidentialité. Noter qu'il se pourrait que certaines règles contiennent des informations privées non destinées à des parties qui ne sont pas de confiance.

Req. 8. (Règles de LG) Même si un générateur de localisation n'a pas connaissance et n'a pas accès à toutes les règles de confidentialité définies par le faiseur de règle, le générateur de localisation DOIT transmettre les informations de localisation conformément aux instructions établies par le faiseur de règle. Une telle conformité PEUT être accomplie par le générateur de localisation ne transmettant le LO qu'à un URI désigné par le faiseur de règle.

Req. 9. (Règles de visionnage) Un visionneur n'a pas besoin de connaître toutes les règles définies par le faiseur de règle (parce que un visionneur NE DEVRAIT PAS retransmettre les informations de localisation) et donc un visionneur DEVRAIT recevoir seulement le sous ensemble de règles de confidentialité nécessaire pour que le visionneur traite le LO en conformité avec toutes les règles de confidentialité (comme une instruction sur la durée pendant laquelle le LO peut être conservé).

Req. 10. (Langage de règle complet) Geopriv PEUT spécifier un langage de règle capable d'exprimer une large gamme de règles de confidentialité concernant les informations de localisation. Ce langage de règle PEUT être un langage existant, une adaptation d'un existant ou un nouveau langage de règle, et il DEVRAIT être aussi simple que possible.

Req. 11. (Langage de règle limité) Geopriv DOIT spécifier un langage de règle limité capable d'exprimer un ensemble limité de règles de confidentialité concernant les informations de localisation. Ce langage de règle PEUT être un langage existant, une adaptation d'un langage existant ou un nouveau langage de règle. L'objet de localisation DOIT inclure des champs et des données suffisants pour exprimer l'ensemble limité de règles de confidentialité.

7.4 Confidentialité et sécurité de l'objet de localisation

7.4.1 Protection de l'identité

Req. 12. (Protection de l'identité) L'objet de localisation DOIT prendre en charge l'utilisation de pseudonymes sans lien dans les champs d'identification correspondants de faiseur de règle, cible, appareil, et receveur de localisation. Comme les pseudonymes sans lien sont simplement des chaînes binaires qui ne sont pas liées initialement à une identité bien connue, cette exigence revient à dire que l'espace de noms pour les identifiants utilisé dans le LO doit être assez grand pour contenir de nombreuses chaîne non utilisées.

7.4.2 Exigences d'authentification

Req. 13. (Exigences d'accréditifs) Le protocole utilisateur et l'objet de localisation DEVRAIENT permettre l'utilisation de

différents types d'accréditifs, incluant des accréditifs améliorant la confidentialité (par exemple, ceux décrits dans [Bra00] ou [Cha85]).

7.4.3 Actions à sécuriser

Req. 14. (Caractéristiques de sécurité) L'objet de localisation DOIT prendre en charge des champs convenables pour la protection de l'objet qui fournissent les caractéristiques de sécurité suivantes :

14.1) Authentification mutuelle de point d'extrémité : le protocole utilisateur est capable d'authentifier les deux parties dans une transmission d'objet de localisation,

14.2) Intégrité de l'objet de données : le LO est sécurisé contre la modification par des entités non autorisées durant la transmission et la mémorisation,

14.3) Confidentialité de l'objet de données : le LO est sécurisé contre l'espionnage (lecture non autorisée) durant la transmission et la mémorisation, et

14.4) Protection contre la répétition : un vieux LO ne peut pas être répété par un adversaire ou par la même entité qui a utilisé le LO lui-même (sauf peut-être durant une petite fenêtre temporelle qui est configurable ou acceptée par le faiseur de règle).

Req. 15. (Chiffrement minimal)

15.1) Geopriv DOIT spécifier une sécurité minimum de mise en œuvre obligatoire de l'objet de localisation, incluant des algorithmes de chiffrement de mise en œuvre obligatoire pour les algorithmes de signature numérique et les algorithmes de chiffrement.

15.2) Il PEUT aussi définir d'autres mécanismes de sécurité de mise en œuvre obligatoire pour l'objet de localisation pour les codes d'authentification de message (MAC) ou d'autres objets.

15.3) Le protocole DEVRAIT permettre un contournement si l'authentification échoue dans un appel d'urgence.

La question visée dans le dernier point est qu'un appel d'urgence dans certaines situations défavorables peut ne pas être établi si l'authentification minimale échoue. Ce n'est probablement pas ce que l'utilisateur voudrait voir arriver. L'utilisateur peut préférer un appel non authentifié à un serveur d'urgence non authentifié plutôt que pas d'appel du tout, même au risque de parler à un attaquant ou que ces informations ne soient pas sécurisées.

7.5 Non exigences

Non-Req. 1. (Pontages sur des réseaux non IP) La spécification Geopriv NE DEVRAIT PAS spécifier le pontage à des réseaux non IP (RTPC, etc.).

8. Considérations pour la sécurité

Le but de l'objet de localisation Geopriv et des exigence pour le protocole utilisateur est de permettre une divulgation contrôlée par des règles de confidentialité des informations de localisation pour les services de localisation.

8.1 Analyse de trafic

Les informations portées dans l'objet de localisation sont sécurisées d'une façon conforme aux règles de confidentialité et de sécurité du faiseur de règle, mais d'autres informations, portées dans d'autres objets ou en-têtes ne sont en général pas sécurisées de la même façon. Cela signifie que Geopriv ne peut pas d'une façon générale, sécuriser la cible contre les attaques générales d'analyse de trafic ou autres formes de violations de la confidentialité.

8.2 Sécurisation des règles de confidentialité

Les règles de confidentialité du faiseur de règles concernant la localisation de la cible peuvent être accessibles à un serveur de localisation dans un détenteur de règle public ou non public, ou elles peuvent être portées par l'objet de localisation, ou elles peuvent être présentées par le receveur de localisation comme des capacités ou des jetons. Chaque type de règle doit être sécurisé de sa propre façon particulière.

Les règles dans un détenteur de règle non public sont normalement authentifiées en utilisant un code d'authentification de

message (MAC, *Message Authentication Code*) ou une signature, selon le type de clés utilisées. Les règles dans un détenteur de règle public (qui peut en principe être accédé directement par plusieurs entités, par exemple, plusieurs serveurs de localisation) sont normalement signées numériquement.
Les champs de règles dans un LO sont sécurisés au titre du LO lui-même. Un jeton Geopriv (jeton ou ticket produit par le faiseur de règle à un receveur de localisation, exprimant le consentement explicite du faiseur de règle à l'accès à ces informations de localisation) est authentifié ou signé.

8.3 Cas d'urgence

Considérons la situation où l'authentification échoue dans un appel d'urgence parce que le centre d'authentification ne réussit pas à s'authentifier lui-même. Dans ce cas, une façon de mettre en œuvre le contournement de l'authentification pour les appels d'urgence (mentionnée dans la Req 15.3) est de laisser l'utilisateur avoir le choix d'écrire une règle qui dit :
- "Si le serveur d'urgence ne s'authentifie pas lui-même, envoyer les informations de localisation quand même", ou
- "Si le serveur d'urgence ne s'authentifie pas lui-même, laisser l'appel échouer".

Ensuite, dans le cas où l'authentification de l'appel d 'urgence échoue parce que l'utilisateur ne peut pas s'authentifier lui-même, la question se pose : quelle règle utiliser ? Il est raisonnable d'utiliser une règle par défaut : ces informations de localisation ne peuvent être envoyées qu'à un centre d'urgence.

La troisième situation, qui devrait être étudiée plus en détail, est : que faire si non seulement l'utilisateur échoue à s'authentifier, mais aussi si le centre d'urgence n'est pas authentifiable ? Il est raisonnable d'envoyer les informations de localisation quand même, mais y a t-il des menaces pour la sécurité qui doivent être prises en compte ?

8.4. Identités et anonymat

L'utilisation de pseudonymes sans lien est nécessaire pour conserver l'anonymat.

L'objet de l'utilisation de pseudonymes sans lien est le suivant : le protocole utilisateur devrait être capable de cacher l'identité réelle du faiseur de règle, de la cible, et de l'appareil, aux serveurs de localisation ou aux receveurs de localisation, si c'est exigé par le RM. Aussi, le protocole utilisateur DEVRAIT être capable de cacher l'identité réelle du receveur de localisation au serveur de localisation.

Dans ce dernier cas, la cible n'est pas concernée par le fait que le serveur l'identifie et connaisse sa localisation, mais par le fait d'identifier ses partenaires commerciaux, et donc ses habitudes, etc. Les raisons de cacher les identités réelles des receveurs de localisation incluent (a) que cette connaissance peut être utilisée pour déduire l'identité de la cible, (b) que la connaissance de l'identité du receveur de localisation peut embarrasser la cible ou divulguer des informations confidentielles, et (c) que le dossier disant qui a obtenu les informations de localisation d'une cible sur une longue période peut donner des informations sur les habitudes, les mouvements, etc. Même si les fournisseurs de service de localisation sont d'accord pour respecter la vie privée de l'utilisateur, sont obligés par les lois ou règlements de protéger la vie privée de l'utilisateur, et que le mauvais comportement ou la négligence du serveur de localisation peut être sanctionné, il y a quand même un risque que des données personnelles puissent devenir disponibles à des personnes non autorisées à travers des attaques de l'extérieur, un accès non autorisé de l'intérieur, des erreurs techniques ou humaines, ou des processus légaux.

Dans certaines occasions, un serveur de localisation doit savoir qui fournit les règles de confidentialité pour une cible particulière, tandis que dans d'autres situations il sera suffisant de savoir que le fournisseur des règles est autorisé à le faire.

8.5 Cible involontaire

Une cible involontaire est une personne ou objet tracé à proximité de la cible. Ce cas particulier se produit le plus souvent si la cible n'est pas une personne. Par exemple, la cible peut être une voiture de location équipée d'un GPS, utilisé pour tenir l'inventaire de véhicules. La société de location de voitures peut ne pas se soucier de la localisation du conducteur, mais la vie privée du conducteur est implicitement affectée.

Geopriv peut ou non protéger ou affecter la confidentialité de cibles involontaires, mais l'impact sur les cibles involontaires devrait être reconnu.

9. Questions de protocole et de LO remises à plus tard

Cette section discute brièvement des questions relatives à l'objet de localisation ou au protocole qui ont émergé durant la

discussion de versions antérieures du présent document.

9.1 Plusieurs localisations dans un LO

Un champ Localisation est destiné à représenter un point ou une région dans l'espace (1, 2, ou 3 dimensions). La possibilité d'inclusion de plusieurs localisations est discutée dans un autre document. Le consensus actuel est le suivant : la définition du LO PEUT permettre que le champ Localisation soit facultatif, pour apparaître exactement une fois ou pour se produire plusieurs fois. Chaque champ Localisation peut contenir une ou plusieurs "représentations de localisation", dont chacune est destinée à représenter une mesure différente ou un formatage différent de la même position. Mais il y a d'autres possibilités d'utiliser plusieurs champs Localisation et plusieurs représentations : peut-être plusieurs champs Localisation seront utilisés pour rapporter le même pointage dans différents formats, ou plusieurs pointages à des instants différents, ou plusieurs capteurs de localisations pour le même appareil, ou pour d'autres objets, qui pourraient aussi dépendre du protocole utilisateur. Tout cela sera examiné plus tard.

9.2 Champs de traduction

Il est possible d'inclure des champs pour indiquer qu'une des localisations est une traduction d'une autre. Si cela est fait, il est aussi possible d'avoir un champ pour identifier le traducteur, en identité et en méthode.

9.3 Fanion de vérité

Geopriv DOIT être neutre sur la vérité ou la non vérité des informations de localisation contenues dans le LO. Donc, le LO NE DOIT PAS fournir dans un objet un attribut disant "Je vous dis (ou ne vous dis pas) l'entière vérité".

9.4 Format des informations d'instant

Le format des informations d'instant sort du domaine d'application de ce document.

9.5 Espace de noms des identifiants

Qui définit les identités : le protocole utilisateur peut il définir les identifiants ou le protocole utilisateur doit il utiliser et authentifier les pseudonymes proposés par les règles, choisis indépendamment du protocole utilisateur ? Bien sûr, si le protocole utilisateur a un espace de noms approprié, contenant de nombreux noms inutilisés qui peuvent servir de pseudonymes et peuvent être remplacés régulièrement par de nouveaux, alors l'objet de localisation peut être capable d'utiliser l'espace de noms. À cette fin, l'utilisateur va probablement devoir écrire ses règles en utilisant cet espace de noms. Noter qu'il est nécessaire de changer régulièrement les pseudonymes utilisés, parce que l'identification de l'utilisateur derrière un pseudonyme sans lien peut être très simple.

Il y a plusieurs avantages à laisser le protocole utilisateur définir l'espace de noms :
- o l'authentification incorporée serait plus facile, car le protocole utilisateur a souvent déjà les accréditifs pour l'identité d'authentification en place et l'authentification "incorporée" serait indépendante de la forme des identifiants,
- o la taille des noms serait fixe.

D'un autre côté, les avantages du choix des identifiants par la règle sont que :
- o l'utilisateur a le contrôle de son anonymat, et
- o l'interfonctionnement de plusieurs systèmes avec objets de localisation à travers les frontières de protocole est facilité.

10. Remerciements

Nous souhaitons remercier les membres du groupe de travail Geopriv de l'IETF pour leurs commentaires et suggestions. Aaron Burstein, Mehmet Ersue, Allison Mankin, Randall Gellens, et les participants aux réunions Geopriv de San Diego et Yokohama ont fourni des commentaires détaillés ou du texte.

11. Références

11.1 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)

11.2 Références pour information

[Bra00] Stefan A. "Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy", MIT Press; ISBN: 0262024918; 1ère édition, août 2000

[Cha85] Chaum, David:" Security without Identification, Card Computers to make Big Brother Obsolete". Version originale dans : Communications of the ACM, vol. 28 n°10, octobre 1985, pages 1030-1044. Version révisée disponible à http://www.chaum.com/articles/

[ISO99] Norme internationale ISO 15408, 1999, http://www.commoncriteria.org/ .

[OECD] Lignes directrices de l'OCDE sur la protection de la confidentialité et des flux transfrontières de données personnelles, http://www.oecd.org .

[Pfi01] Pfitzmann, Andreas ; Koehntopp, Marit : "Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology", dans H Federrath (éd.) : "Designing Privacy Enhancing Technologies". Compte rendu de l'atelier sur les questions de conception de l'anonymat et de l'inobservabilité. LNCS 2009; 2001; 1-9. Des versions plus récentes sont disponibles à http://www.koehntopp.de/marit/pub/anon

12. Adresse des auteurs

Jorge R Cuellar
Siemens AG
Corporate Technology
CT IC 3
81730 Munich, Germany
mél : Jorge.Cuellar@siemens.com

John B. Morris, Jr.
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, D.C. 20006 USA
mél : jmorris@cdt.org
URI: http://www.cdt.org

James M. Polk
Cisco Systems
2200 East President George Bush
Richardson, Texas 75082 USA
mél : jmpolk@cisco.com

Deirdre K. Mulligan
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall School of Law
University of California
Berkeley, CA 94720 USA
mél : dmulligan@law.berkeley.edu
URI: http://www.law.berkeley.edu/cenpro/samuelson/

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 5707
Concord, CA 94520 USA
mél : jon.peterson@neustar.biz
URI: http://www.neustar.biz/

13. Déclaration complète de droits de reproduction

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.