(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 907 941**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **06 09427**

(51) Int Cl[8] : **G 06 Q 30/00** (2006.01)

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.10.06.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 02.05.08 Bulletin 08/18.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *LELEU JEAN LUC* — FR.

(72) **Inventeur(s) :** LELEU JEAN LUC.

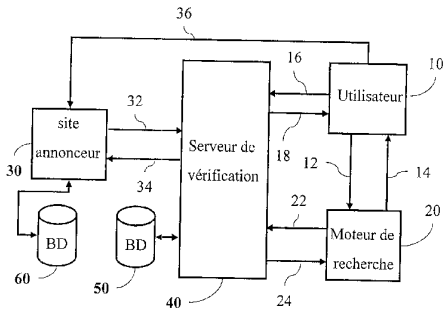
(73) **Titulaire(s) :**

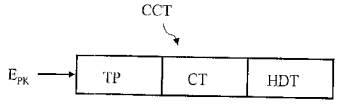
(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES.

(54) PROCEDE ET SYSTEME DE VALIDATION DE LA SELECTION D'UN HYPERLIEN DANS UNE PAGE WEB.

(57) L'invention concerne un procédé de validation de la sélection d'un d'hyperlien affiché dans une page web (14) fournie à un utilisateur (10), caractérisé en ce qu'il comprend:

- la création d'un certificat numérique (CCT) unique et sécurisé associé à l'hyperlien;
- l'insertion à la volée du certificat (CCT) dans l'hyperlien affiché dans la page web fournie à l'utilisateur;
- la vérification de l'intégrité du certificat associé à L'hyperlien, suite à la sélection par l'utilisateur de l'hyperlien activant une connexion (36) vers un site web correspondant, et
- la validation de la sélection de l'utilisateur comme étant légitime en cas de succès de la vérification, auquel cas la connexion de l'utilisateur au site web correspondant est établie.





FR 2 907 941 - A1

La présente invention concerne le domaine de la délivrance et de la gestion d'informations dans un réseau informatique tel que le réseau Internet, plus particulièrement en rapport avec les campagnes de publicité sur l'Internet basées sur le modèle économique dit du « coût par clic », mais aussi en rapport avec des modèles économiques de partages de revenus comme le « coût par action » (« cost per click » et « cost per actions » selon la terminologie anglo-saxonne).

L'invention propose plus précisément un procédé et un système de validation de la sélection d'un hyperlien dans une page web par un utilisateur dans le cadre de ces modèles, de modèles connexes ou, de manière générale, de modèles qui nécessitent une preuve sécurisée et une mesure de confiance (« rating » dans la terminologie anglo-saxonne) de la sélection d'un hyperlien et/ou l'authentification associée à une mesure de confiance du navigateur de l'utilisateur.

Le modèle économique du « coût par clic » repose sur la possibilité offerte par des sites portails ou des moteurs de recherche sur l'Internet, ou encore des sites qui leur sont affiliés ou même des sites qui sont affiliés des sites affiliés, d'afficher des annonces publicitaires, typiquement sous forme de liens hypertextes.

Dans le cas des moteurs de recherches, ces annonces sont affichées en fonction de mots clés entrés par un utilisateur à l'occasion d'une requête d'information.

Le principe général, dans ce cas, consiste donc pour un annonceur, à acheter des mots clefs qui permettent d'afficher son site en tête des résultats sur une requête donnée. Par exemple, dans le cadre du moteur de recherche Google®, ces liens sponsorisés prévus pour renvoyer vers les sites des annonceurs, s'affichent sur la droite du navigateur en réponse à une requête d'un utilisateur.

Lorsqu'un utilisateur voit l'annonce et clique sur le lien hypertexte correspondant, il est donc automatiquement dirigé vers le site Web de l'annonceur par le moteur de recherche ou le site portail. En échange, ces clics sont rémunérés dans la mesure où l'annonceur paie au moteur de recherche ou au portail un montant forfaitaire prédéfini (le coût par clic) pour chaque clic d'un utilisateur sur le lien et ce, indépendamment de l'action effectuée ultérieurement par l'utilisateur sur le site de l'annonceur (simple visite ou achat). Le coût du clic est généralement fixé par un système d'enchères en ligne sur les mots clés générant les liens sponsorisés.

Dans le modèle du « cost per action », l'annonceur ne paie le moteur de recherche ou le portail que lorsque l'utilisateur qui accède au site effectue une transaction sur ce site.

Les liens sponsorisés peuvent également être affichés via des sites Internet affiliés (ou affiliés d'affiliés) au moteur de recherche. Dans ce cas, le moteur ou le portail reverse une partie des montants à ces sites affiliés.

Ce système de liens sponsorisés, qui permet un mode de tarification des campagnes publicitaires sur Internet basé sur le nombre de clics enregistrés sur une annonce publicitaire, par exemple rattachée à un ou des mots clefs, a connu un essor très important, jusqu'à procurer une grande partie du chiffre d'affaire réalisé par les moteurs de recherches les plus populaires comme Google®. Dans le même temps, ce système doit également faire face à une dérive abusive.

En effet, il apparaît qu'un nombre conséquent de clics réalisés sur ces liens sponsorisés serait le fait d'utilisateurs mettant en œuvre des méthodes frauduleuses pour générer massivement des clics sur des annonces ciblées, mais n'ayant aucune intention de visiter le site de l'annonceur en question, ou visitant le site pour simuler le comportement d'un utilisateur intéressé.

Il peut s'agir de concurrents peu scrupuleux, qui souhaitent ainsi augmenter au maximum la facture qui sera adressée à l'annonceur ciblé, dans l'optique de le mettre en difficulté en épuisant son budget publicitaire rapidement.

Il peut également s'agir de personnes malintentionnées créant des sites factices, sur lesquels sont affichés des liens sponsorisés, dans le seul but d'être rémunérés en fonction du nombre de clics sur ces liens. Ces personnes ont alors tout intérêt à faire gonfler le nombre de clics sur les liens sponsorisés affichés sur leur site, pour augmenter ainsi le revenu publicitaire reversé par le moteur de recherche auquel le site est affilié.

Les méthodes frauduleuses mises en œuvre aux fins exposées ci-dessus peuvent consister, par exemple, en des clics manuels répétés ou simulant le comportement d'un utilisateur normal ou des clics générés par l'intermédiaire d'un robot, d'outils automatisés ou de tout autre logiciel de détournement de clics.

Cette fraude au clic, consistant donc à cliquer massivement sur les liens sponsorisés, soit pour augmenter artificiellement la facture dont des entreprises concurrentes, annonceurs via ces liens sponsorisés, devront s'acquitter, soit pour augmenter frauduleusement les revenus publicitaires de sites affiliés à des moteurs de recherche ou des sites portails affichant les liens sponsorisées sur leurs pages, est en train de prendre des proportions inquiétantes, susceptibles même de menacer la viabilité du modèle publicitaire des liens sponsorisés sur l'Internet.

Or, à l'heure actuelle, la seule solution à disposition des annonceurs pour lutter contre cette fraude au clic, consiste à surveiller leurs statistiques de clics et leurs taux de transformation (c'est-à-dire les clics qui ont effectivement générés une navigation sur le site de l'annonceur ou un acte d'achat sur le site par rapport au nombre total de clics), afin d'alerter le moteur de recherche prestataire en charge de l'affichage des liens sponsorisés et éventuellement demander des réparations financières pour les clics jugés non valides.

Parallèlement, les moteurs de recherche tentent de juguler la fraude au clic en mettant en place des

mécanismes d'analyse du trafic sur le web, pour tenter de détecter des comportements de clics jugés frauduleux et ainsi identifier les fraudeurs.

Toutefois, ces solutions d'analyse du trafic, en plus d'être fastidieuses, ne sont de toute façon pas complètement satisfaisantes au regard des moyens de plus en plus sophistiqués utilisés par les fraudeurs au clic, notamment ceux reposant sur l'utilisation de réseaux d'ordinateurs zombies, quasiment indétectables. Aucune solution n'a permis jusqu'alors d'enrayer efficacement la fraude au clic.

La présente invention vise à résoudre ces inconvénients, en permettant de garantir automatiquement et en temps réel la légitimité d'un clic sur un lien hypertexte, et notamment qu'il est effectivement émis par un utilisateur réel.

Un autre but de l'invention est aussi de pouvoir authentifier un comportement non frauduleux d'un utilisateur cliquant sur un lien hypertexte, mais aussi de pouvoir lui assigner un niveau de confiance (« rating » selon la terminologie anglo-saxonne) particulier en fonction de son comportement.

Avec ces objectif en vue, l'invention a pour objet un procédé de validation de la sélection d'un d'hyperlien affiché dans une page web fournie à un utilisateur, caractérisé en ce qu'il comprend :

- la création d'un certificat numérique unique et sécurisé associé à l'hyperlien ;

- l'insertion à la volée du certificat dans l'hyperlien affiché dans la page web fournie à l'utilisateur ;

- la vérification de l'intégrité du certificat associé à l'hyperlien, suite à la sélection par l'utilisateur de l'hyperlien activant une connexion vers un site web correspondant, et

- la validation de la sélection de l'utilisateur comme étant légitime en cas de succès de la vérification, auquel cas la connexion de l'utilisateur au site web correspondant est établie.

De préférence, l'étape de validation de la sélection de l'utilisateur comprend en outre la vérification d'un historique d'un nombre de sélections légitimes associé à l'utilisateur, mémorisant les certificats représentatifs respectivement de chaque sélection légitime précédente réalisée par l'utilisateur.

Le procédé comprend avantageusement une étape de mise à jour de l'historique du nombre de sélections légitimes associé à l'utilisateur, consistant à mémoriser le certificat vérifié.

De préférence, la vérification de l'historique du nombre de sélections légitimes associé à l'utilisateur comprend la vérification de l'intégrité de chaque certificat mémorisé et la détermination d'un niveau de confiance associé à l'utilisateur en fonction du nombre de sélections légitimes.

Avantageusement, le procédé comprend, pour chaque sélection validée comme étant légitime, la sauvegarde du certificat associé à l'hyperlien et de l'historique du nombre de sélections légitimes associé à l'utilisateur au niveau du site web auquel l'utilisateur se connecte via la sélection.

Selon un mode de réalisation, la création du certificat unique associé à chaque hyperlien affiché comprend la concaténation d'un premier ensemble de données relatives à l'hyperlien et/ou au site web correspondant à l'hyperlien, d'un deuxième ensemble de données relatives à des données d'authentification du certificat et d'un troisième ensemble de données relatives à une date d'expiration du certificat.

De préférence, le premier ensemble de données est constitué par l'adresse URL du site web correspondant à l'hyperlien affiché.

De préférence, le deuxième ensemble de données est représenté par des collisions de fonction de hachage.

Avantageusement, les premier, deuxième et troisième ensembles de données sont concaténées de manière chiffrée.

Selon un mode de réalisation, la vérification de l'intégrité du certificat consiste à vérifier l'intégrité du deuxième ensemble de données.

Avantageusement, la vérification de l'intégrité du certificat consiste en outre à vérifier sa validité temporelle.

Selon un mode de réalisation, la page web est une page de résultats, fournie par un moteur de recherche, ou un site web affilié au moteur de recherche, en réponse à une requête d'information reçue de l'utilisateur comprenant un ou plusieurs mots clés associés à une annonce affichée sous forme d'hyperlien dans la page.

L'invention concerne également un système de validation de la sélection d'un d'hyperlien affiché dans une page web, caractérisé en ce qu'il comprend :

- des moyens de fourniture de la page web à un utilisateur,
- un serveur de vérification, comprenant des moyens pour créer un certificat numérique unique, sécurisé, associé à l'hyperlien affiché dans la page web,

les moyens de fourniture de la page web comprenant des moyens pour insérer à la volée le certificat dans l'hyperlien affiché dans la page web fournie à l'utilisateur,

le serveur de vérification comprenant en outre :

- des moyens de réception du certificat associé à l'hyperlien affiché, suite à la sélection par l'utilisateur de l'hyperlien dans la page web, activant une connexion vers un site web correspondant à l'hyperlien,
- des moyens de vérification de l'intégrité du certificat associé à l'annonce, et
- des moyens de validation de la sélection de l'utilisateur comme étant légitime et pour établir la connexion de l'utilisateur au site web correspondant, en cas de succès de la vérification de l'intégrité du certificat.

De préférence, le serveur de vérification comprend en outre :

- des moyens de récupération d'un module d'authentification associé à l'utilisateur, prévu pour conserver un historique d'un nombre de sélections

légitimes réalisées précédemment par l'utilisateur, en mémorisant pour chaque sélection légitime, le certificat correspondant,

- des moyens de détermination d'un niveau de confiance associé à l'utilisateur en fonction dudit historique, le niveau de confiance déterminé étant pris en compte par les moyens de validation de la légitimité de la sélection de l'utilisateur,

- des moyens de mise à jour du module d'authentification avec le certificat reçu et vérifié, et

- des moyens pour transmettre le module d'authentification mis à jour à l'utilisateur.

Avantageusement, le serveur de vérification comprend des moyens de transmission du module d'authentification mis à jour vers le site web correspondant à l'hyperlien.

Avantageusement, site web correspondant à l'hyperlien et le serveur de vérification comprennent des moyens de sauvegarde du module d'authentification mis à jour pour chaque sélection validée comme étant légitime.

Selon un mode de réalisation, le certificat unique associé à l'hyperlien affiché comprend un premier ensemble de données relatives à l'hyperlien et/ou au site web correspondant à l'hyperlien, un deuxième ensemble de données relatives à des données d'authentification du certificat et un troisième ensemble de données relatives à une date d'expiration du certificat.

Selon un mode de réalisation, les moyens de fourniture de la page web comprennent un moteur de recherche ou un site web affilié au moteur de recherche, fournissant la page web en réponse à une requête d'information reçue de l'utilisateur comprenant un ou plusieurs mots clés associés à une annonce affichée sous forme d'hyperlien dans la page fournie.

L'invention concerne encore un serveur de vérification, caractérisé en ce qu'il comprend :

- des moyens pour créer un certificat numérique unique, sécurisé, associé à un hyperlien affiché dans une page web fournie à un utilisateur par des moyens de fourniture de pages web,

- des moyens de transmission du certificat aux moyens de fourniture, prévus pour insérer à la volée le certificat dans l'hyperlien affiché la page web fournie,

- des moyens de réception du certificat associé à l'hyperlien affiché, suite à la sélection par l'utilisateur de l'hyperlien dans la page web, activant une connexion vers un site web correspondant à l'hyperlien,

- des moyens de vérification de l'intégrité du certificat associé à l'annonce, et

- des moyens de validation de la sélection de l'utilisateur comme étant légitime et pour établir la connexion de l'utilisateur au site web correspondant, en cas de succès de la vérification de l'intégrité du certificat.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante donnée à titre d'exemple illustratif et non limitatif dans le cas de l'utilisation du système avec un moteur de recherche, et faite en référence aux figures annexées dans lesquelles :

-la figure 1 illustre un mode de réalisation d'une architecture réseau pour la mise en œuvre du procédé et du système selon la présente invention, et

-la figure 2 illustre un mode de réalisation d'un certificat numérique unique associé à une annonce publicitaire dans le cadre de la présente invention.

En référence à la figure 1, un utilisateur 10 dispose d'un terminal connecté à Internet, lui permettant d'avoir accès à des pages web par un programme appelé « navigateur », installé sur son terminal. Une technique notamment mise en œuvre par le navigateur web est connue sous le nom de « hyperlien », qui permet aux fournisseurs de pages web de créer des liens vers d'autres pages web que les utilisateurs peuvent alors récupérer par sélection du lien sur le navigateur web via un dispositif de pointage approprié. Le terme « clic » est couramment utilisé pour décrire l'action de sélection du lien en question dans la page web par le dispositif de pointage.

Dans le cas d'une recherche d'information sur le web en utilisant un moteur de recherche Internet 20, ou un site web affilié à un tel moteur de recherche, l'utilisateur 10 émet une requête 12, via son navigateur connecté au moteur de recherche, comprenant

un ou plusieurs mots clés relatifs à la recherche d'informations.

En réponse à cette requête, le moteur de recherche utilise les mots clés de la requête utilisateur pour créer en temps réel un listage de pages web, fourni à l'utilisateur dans une page de résultats 14. L'utilisateur peut alors atteindre ces pages web par sélection d'un hyperlien correspondant dans la page de résultats s'affichant dans son navigateur.

Comme exposé précédemment, des annonces publicitaires sont classiquement publiées sous forme d'un hyperlien dans la page web de résultats fournie à l'utilisateur, à côté des résultats de recherche, en fonction des mots clés entrés par celui-ci dans sa requête d'information.

Selon l'invention, à chaque annonce de ce type publiée dans une page de résultats fournie par le moteur de recherche à une requête d'information d'un utilisateur, est associé un certificat numérique unique, non forgeable et vérifiable. Comme on le comprendra par la suite, l'objectif du certificat associé à chaque annonce publiée, est de pouvoir garantir qu'un clic effectué par l'utilisateur sur l'annonce en question est un clic légitime, à savoir notamment qu'il n'est pas généré par l'intermédiaire d'un robot, d'outils automatisés ou de tout autre logiciel de détournement de clics.

Le fonctionnement est le suivant. Tout d'abord, lorsqu'un annonceur 40 souhaite diffuser une annonce sur le moteur de recherche 20, il s'inscrit auprès du service correspondant du moteur de recherche, afin de

soumettre l'annonce à diffuser et la liste des mots clés en rapport avec cette annonce.

Selon un premier mode de réalisation, une requête 32 de soumission d'une telle annonce émise par l'annonceur vers le moteur de recherche est interceptée par un serveur de vérification 30, intercalé entre l'annonceur et le moteur de recherche, aux fins de créer un certificat numérique associée à cette annonce et, plus précisément une pluralité de certificats numériques uniques, disponibles chacun à la demande pour chaque publication de l'annonce sur le moteur de recherche.

Un tel certificat numérique unique, disponible pour une publication de l'annonce sur le moteur de recherche, est symbolisé à la figure 2.

Pour créer ce certificat numérique unique CCT, le serveur de vérification 30 génère tout d'abord un premier ensemble de données TP, relatives à l'annonce et/ou au site web auquel est prévue de renvoyer l'annonce lorsqu'elle est sélectionnée. Ce premier ensemble de données TP peut par exemple comprendre le texte de l'annonce et/ou l'adresse URL du site web correspondant et/ou la liste des mots clés associés à l'annonce.

Le certificat numérique unique CCT est également constitué d'un deuxième ensemble de données CT, relatives à des données d'authentification du certificat, dont le rôle est de garantir de façon sûre l'origine et l'intégrité du certificat.

Un champ spécifique peut ainsi être inséré dans ce deuxième ensemble de données, représentatif de l'entité productrice du certificat.

Selon un exemple de réalisation, les données d'authentification CT du certificat sont obtenues selon une méthode décrite dans l'article intitulé « PayWord and Micromint - Two Simple Micropayment Schemes », par R.L. RIVEST et A. SHAMIR et présenté le 26 janvier 1996 lors de la conférence RSA de 1996. Cet article décrit un système de fabrication de pièces de monnaie électroniques, représentées par des chaînes de bits dont la validité peut être vérifiée par n'importe qui, mais qui sont extrêmement difficiles à reproduire. Dans ce système, les pièces de monnaie électronique sont représentées par des collisions de fonction de hachage.

Ainsi, selon cet exemple, les données d'authentification CT du certificat sont constituées par une pluralité de chaînes de bits obtenues par des collisions de fonction de hachage, notée h. Ainsi, soient par exemple X0, X1, X2 et X3 de telles chaînes de bits formant les données d'authentification CT du certificat, il est possible de vérifier très facilement la validité de ces données, et par là même l'intégrité du certificat, en contrôlant que : $h(X0) = h(X1) = h(X2) = h(X3)$.

Enfin, le certificat numérique unique CCT peut également comprendre un troisième ensemble de données d'horodatage HDT, relatives par exemple à une date d'expiration du certificat, au-delà de laquelle ce dernier n'est plus valide. Ainsi, un même certificat ne pourra pas être réutilisé à des fins frauduleuses. On

choisit par exemple une durée de validité de l'ordre de quelques secondes.

Les trois ensembles de données précédemment décrits sont alors concaténés par le serveur de vérification pour former une chaîne de données unique, associée à l'annonce publiée sur le moteur de recherche et donc au lien hypertexte correspondant affiché. Les trois ensembles de données sont avantageusement concaténées de façon chiffrée, par exemple par application d'un algorithme de chiffrement à clé publique E_{PK}, par exemple un algorithme de type RSA.

Dans un autre exemple de réalisation le résultat du calcul d'une fonction de type MD5 sur la chaine de données unique pourra simplement être concaténé à cette première chaine pour constituer une nouvelle chaine de données unique.

La chaîne de données ainsi obtenue forme donc un certificat unique et sécurisé, dont le deuxième ensemble de données CT peut être assimilé à une clé unique, non forgeable, permettant d'assurer l'intégrité de l'ensemble et d'authentifier ainsi le certificat.

Le serveur de vérification est apte à générer un tel certificat unique valable pour chaque publication possible de l'annonce sur le moteur de recherche, consécutive à une requête utilisateur, en remplaçant, à chaque nouvelle publication de l'annonce, le deuxième ensemble de données d'authentification CT. Chaque certificat associé à chaque publication d'une l'annonce sur le moteur de recherche est donc unique en ce qu'il comprend un ensemble de données d'authentification CT qui lui est propre.

Ainsi, à la réception d'une requête d'information 12, le moteur de recherche 20, simultanément à la création de la page de résultats à fournir à l'utilisateur, envoie à destination du serveur de vérification 30, une requête 22 de récupération du certificat numérique unique associé respectivement à chaque annonce destinée à être publiée dans la page de résultats à fournir.

Les certificats uniques associés à chaque annonce devant être publiée dans la page de résultats sont générés selon les principes exposés plus haut et sont fournis dans une réponse 24 à la requête 22 du moteur de recherche.

Le moteur de recherche insère alors chaque certificat unique récupéré dans la page de résultats 14 renvoyée à l'utilisateur. Chaque certificat peut par exemple être inséré dans l'adresse URL correspondant à l'annonce associée dans la page de résultats.

Ainsi, pour une annonce donnée publiée dans la page de résultats reçue par le navigateur de l'utilisateur, un certificat unique est associé. La légitimité d'un clic utilisateur sur une annonce publiée dans la page de résultat repose donc tout d'abord, selon l'invention, sur l'existence d'un certificat, intègre et valide, associé à cette annonce lorsque l'utilisateur clique dessus dans son navigateur.

Il convient en outre de noter qu'un tel certificat ne peut avantageusement être récupéré dans le navigateur de l'utilisateur qu'à la seule condition que l'utilisateur ait effectivement émis une requête

d'information, comprenant le ou les mots clés associés à l'annonce, vers le moteur de recherche ou le site affilié.

Ainsi, le système selon l'invention rend inefficaces les méthodes de fraude au clic reposant sur l'utilisation de réseaux de PC zombies, puisque ces derniers fonctionnent en détournant une requête utilisateur quelconque sur l'Internet, sans aucun lien avec une demande d'information relative à une annonce publicitaire destinée à être publiée sur un moteur de recherche ou un site affilié, pour rediriger de façon transparente et abusive l'utilisateur vers un site commercial correspondant à une telle annonce.

Dans ce schéma, aucun certificat tel que décrit précédemment ne peut donc être récupéré par le navigateur de l'utilisateur pour valider la légitimité de la redirection vers le site commercial.

Une fois la page de résultats reçue par l'utilisateur, dans laquelle sont insérés les certificats uniques associés à chaque annonce publiée dans cette page, un clic de l'utilisateur sur un lien correspondant à une de ces annonces déclenche, de manière transparente pour l'utilisateur, l'envoi 16 du certificat associé à cette annonce vers le serveur de vérification 40 à des fins de vérification.

Pour ce faire, après déchiffrement du certificat, l'intégrité du deuxième ensemble de données CT est vérifiée par le serveur 40. Ainsi, selon l'exemple de réalisation, le serveur vérifie que les données constitutives de ce deuxième ensemble forment bien des

collisions de fonction de hachage, garantissant ainsi l'authenticité du certificat.

En outre, le serveur vérifie que la validité du certificat n'a pas expiré au regard de sa date d'expiration, fournie par le troisième ensemble de données HDT.

Si ces opérations de vérification sont menées avec succès, le serveur de vérification 40 valide alors le clic de l'utilisateur sur l'annonce publiée dans la page de résultats comme étant un clic légitime. Dans le même temps, une connexion 36 de l'utilisateur (plus précisément de son navigateur) vers le site web 30 correspondant à l'annonce cliquée est activée.

Le serveur de vérification 40 comprend avantageusement des moyens de sauvegarde 50, permettant de constituer un journal référençant l'ensemble des clics utilisateur ayant été validés comme légitimes pour chaque annonce destinée à être publiée sur le moteur de recherche ou le site affilié. Un clic utilisateur légitime sur une annonce est par exemple référencé avec l'adresse URL du site correspondant, le certificat unique disponible pour ce clic et l'adresse IP du terminal utilisateur.

Ces informations sont également transmises dans une étape 34 par le serveur de vérification 40 vers le site de l'annonceur 30, qui dispose également de moyens de sauvegarde 60 de ces informations, lui permettant de constituer de son côté un journal référençant l'ensemble des clics légitimes sur son annonce.

Selon un mode de réalisation particulièrement avantageux de l'invention, la validation de la

légitimité d'un clic utilisateur sur une annonce est effectuée en prenant en compte, non seulement la vérification de l'authenticité et de la validité d'un certificat unique disponible pour ce clic, comme expliqué précédemment, mais également un niveau de confiance associé à l'utilisateur (ou plus précisément son navigateur), permettant d'authentifier cet utilisateur comme étant un utilisateur légitime.

Ainsi, selon ce mode de réalisation, un clic de l'utilisateur sur un lien sponsorisé correspondant à une annonce publiée dans la page de résultats reçue par cet utilisateur déclenche, en plus de la réception par le serveur de vérification du certificat unique associé à la publication de l'annonce, la création par ce serveur d'un module d'authentification utilisateur, si ce dernier n'existe pas encore, destiné à stocker le certificat reçu et vérifié, représentatif de la légitimité du clic utilisateur sur l'annonce.

Selon un exemple de réalisation, le module d'authentification utilisateur est un cookie (fichier témoin), qui est transmis par le serveur de vérification au navigateur de l'utilisateur lorsque ce dernier clique pour la première fois sur une annonce, et qui peut être récupéré par le serveur lors de clics subséquents pour y stocker le certificat associé reçu et vérifié pour chaque clic, de manière à pouvoir constituer un historique du nombre de clics validés comme légitimes associé à cet utilisateur (ou plus précisément à son navigateur). Ce dernier pourra alors être authentifié en fonction du nombre de clics légitimes qu'il aura réalisé.

Ainsi, chaque nouveau clic de l'utilisateur sur une annonce publiée dans une page de résultats reçue déclenche d'une part, l'envoi 16 au serveur de vérification 40 du certificat unique associé à la publication de l'annonce et, d'autre part, la récupération par le serveur du cookie associé à cet utilisateur.

En plus de la vérification du certificat unique comme précédemment exposé, le serveur 40 vérifie alors également la validité du cookie récupéré. Pour ce faire, le serveur vérifie l'intégrité de chaque certificat stocké dans le cookie.

Puis, en fonction du nombre de certificats stockés dans le cookie, comme autant de preuves du nombre de clics légitimes réalisés précédemment par l'utilisateur, le serveur détermine un niveau de confiance associé à l'utilisateur (plus précisément son navigateur), d'autant plus élevé que le nombre de certificats stockés est élevé.

Le niveau de confiance associé à ce clic utilisateur peut également être déterminé en fonction d'autres informations obtenues à partir des certificats stockés, relatives par exemple à l'adresse URL des sites visités et/ou à la fréquence de clic sur des annonces.

Le niveau de confiance déterminé est alors utilisé par le serveur pour valider la légitimité du clic courant, c'est-à-dire celui qui fait l'objet du processus de validation à un moment donné.

L'accumulation des preuves du nombre de clics légitimes réalisés précédemment par l'utilisateur est

ainsi utilisée en tant que mécanisme de validation du clic courant réalisé par utilisateur, lequel est donc validé par le système en fonction, notamment, du nombre de clics légitimes déjà réalisés.

Le niveau de confiance plus ou moins élevé qui en découle permet au serveur, en fonction de règles pré-établies, d'authentifier l'utilisateur (en fait son navigateur) comme ayant un comportement normal, c'est-à-dire non frauduleux, relativement à son historique de clics.

Dans le cas contraire, lorsque l'examen de l'historique des clics légitimes n'est pas concluant, ou que les certificats associés ne sont pas valides, le système peut refuser la redirection en temps réel de la requête hyperlien et bloquer toute nouvelle requête provenant de ce navigateur au niveau du serveur de vérification.

Ainsi, lorsque le système est utilisé par le site de l'annonceur, celui-ci pourra rejeter ou bloquer en temps réel, via le serveur de vérification, le trafic frauduleux provenant du site portail ou du moteur de recherche. Le bénéfice étant que dans ce cas, ce trafic ne fera pas l'objet d'une facturation du site ayant effectué la redirection.

La validation du clic courant de l'utilisateur comme étant légitime, après la vérification réussie du certificat reçu pour ce clic courant et de l'historique du nombre de clics légitimes associé à l'utilisateur, entraîne la mise à jour du cookie, consistant à y stocker le certificat reçu et vérifié prouvant la légitimité du clic courant. Le cookie mis à jour est

transmis dans une étape 18 par le serveur de vérification au navigateur de l'utilisateur.

Le cookie ayant une taille limité, il est possible dans un exemple de réalisation de remplacer avantageusement une série de n certificats déjà stockés dans le cookie par un nouveau certificat unique représentant et associé à ces n certificats dans le journal des certificats stockés sur le serveur. Ce nouveau certificat peut être d'un type différent et avoir un mode de construction différent. Par exemple, un certificat représentant 10 clics légitimes certifiés peut être associé à une chaine de données X0, X1,X2,X3,X4 tel que h(X0)=h(X1)=h(X2)=h(X3)=h(X4).

De préférence, le cookie est stocké de façon sécurisée sur le navigateur de l'utilisateur. Pour ce faire, à la création du cookie transmis au navigateur de l'utilisateur lors du premier clic de l'utilisateur sur une annonce, une clé secrète propre au navigateur lui est associée, qui est utilisée pour sécuriser l'accès au cookie sur le navigateur de l'utilisateur.

Selon cette variante, le serveur de vérification doit donc maintenir une base de données, par exemple au niveau de ses moyens de sauvegarde 50, pour mémoriser la clé secrète associée à chaque navigateur auquel un cookie a été transmis, pour pouvoir y accéder lors d'un processus de validation d'un clic utilisateur ultérieur. La clé secrète utilisée par le serveur pour accéder au cookie sur le navigateur de l'utilisateur peut également faire avantageusement office de moyens d'identification du navigateur.

Par ailleurs, pour chaque clic sur une annonce validé par le serveur de vérification selon les principes exposés ci-dessus, le cookie utilisateur correspondant mis à jour est sauvegardé par les moyens de sauvegarde 50 du serveur, parmi d'autres informations, comme par exemple l'adresse URL du site correspondant, l'adresse IP du terminal utilisateur, de sorte à constituer, au niveau du serveur de vérification, un journal référençant l'ensemble des clics utilisateur ayant été validés comme légitimes avec les moyens de preuve associés.

D'autre part et par exemple dans le cas du modèle « cost per click », le serveur de vérification pourra mettre à disposition d'un système de facturation du moteur de recherche ou du portail les informations relatives à chaque clic utilisateur légitime et notamment son niveau de confiance associé.

Dans un exemple de réalisation, le serveur pourra générer un ticket de facturation de clic légitime, incluant une valeur représentant le niveau de confiance associé au clic. Le système de facturation du moteur de recherche ou du portail pourra par exemple collecter ces tickets et les consolider pour chaque annonceur en utilisant la valeur représentative du niveau de confiance pour calculer un cout au clic qui pourra alors avantageusement être fonction de cette valeur, ceci afin d'établir une facture globale à l'annonceur.

Ainsi, le niveau de confiance associé à un clic utilisateur légitime, en plus de permettre d'authentifier le comportement de cet utilisateur comme étant non frauduleux, peut aussi servir à quantifier la

valeur de cet utilisateur et donc à permettre une facturation différenciée du clic qu'il a effectué. Dans l'exemple du modèle « cost per click », le moteur de recherche pourra donc envisager un tarif au clic plus important pour les utilisateurs ayant un plus grand niveau de confiance.

Les informations sauvegardées au niveau du serveur de vérification sont également transmises au cours de l'étape 34 par le serveur de vérification 40 au site de l'annonceur 30 vers lequel l'utilisateur est redirigé, permettant au site annonceur de constituer également de son côté, via les moyens de sauvegarde 60, un journal référençant l'ensemble des clics validés comme légitimes sur son annonce.

Ces informations pourront alors permettre en cas de litige entre le site annonceur et le moteur de recherche ou le portail d'effectuer un processus de réconciliation, sur la base des informations référencées par leurs journaux de clics légitimes, comme c'est le cas aujourd'hui entre les operateurs télécoms avec les CDRs (Call Detail Records selon la terminologie anglo-saxonne), qui contiennent toutes les traces des appels effectues.

Un autre intérêt d'affecter un niveau de confiance à chaque clic utilisateur selon les principes évoqués plus haut, est de pouvoir effectuer une mesure de confiance des sites affiliés, en fonction des quantités de clics frauduleux qu'ils redirigent vers les moteurs de recherche ou portails publiant des annonces. Cette mesure de confiance des sites affiliés, découlant des niveaux de confiance associés à chaque clic redirigé

par ceux-ci, permet alors de prendre des décisions économiques ou techniques (blocage) en fonction.

REVENDICATIONS

1. Procédé de validation de la sélection d'un d'hyperlien affiché dans une page web (14) fournie à un utilisateur (10), caractérisé en ce qu'il comprend :

- la création d'un certificat numérique (CCT) unique et sécurisé associé à l'hyperlien ;

- l'insertion à la volée du certificat (CCT) dans l'hyperlien affiché dans la page web fournie à l'utilisateur ;

- la vérification de l'intégrité du certificat associé à l'hyperlien, suite à la sélection par l'utilisateur de l'hyperlien activant une connexion (36) vers un site web correspondant, et

- la validation de la sélection de l'utilisateur comme étant légitime en cas de succès de la vérification, auquel cas la connexion de l'utilisateur au site web correspondant est établie.

2. Procédé selon la revendication 1, caractérisé en ce que l'étape de validation de la sélection de l'utilisateur comprend en outre la vérification d'un historique d'un nombre de sélections légitimes associé à l'utilisateur, mémorisant les certificats représentatifs respectivement de chaque sélection légitime précédente réalisée par l'utilisateur.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend une mise à jour de l'historique du

nombre de sélections légitimes associé à l'utilisateur, consistant à mémoriser le certificat vérifié.

4. Procédé selon les revendications 2 ou 3, caractérisé en ce que la vérification de l'historique du nombre de sélections légitimes associé à l'utilisateur comprend la vérification de l'intégrité de chaque certificat mémorisé et la détermination d'un niveau de confiance asscié à l'utilisateur en fonction du nombre de sélections légitimes.

5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce qu'il comprend, pour chaque sélection validée comme étant légitime, la sauvegarde du certificat associé à l'hyperlien et de l'historique du nombre de sélections légitimes associé à l'utilisateur au niveau du site web auquel l'utilisateur se connecte via la sélection.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que la création du certificat (CCT) unique associé à chaque hyperlien affiché comprend la concaténation d'un premier ensemble de données (TP) relatives à l'hyperlien et/ou au site web correspondant à l'hyperlien, d'un deuxième ensemble de données (CT) relatives à des données d'authentification du certificat et d'un troisième ensemble de données (HDT) relatives à une date d'expiration du certificat.

7. Procédé selon la revendication 6, caractérisé en ce que le premier ensemble de données (TP) est constitué

par l'adresse URL du site web correspondant à l'hyperlien affiché.

8. Procédé selon la revendication 6 ou 7, caractérisé en ce que le deuxième ensemble de données (CT) est représenté par des collisions de fonction de hachage.

9. Procédé selon la revendication 6, caractérisé en ce que les premier, deuxième et troisième ensembles de données sont concaténées de manière chiffrée.

10. Procédé selon l'une quelconque des revendications 6 à 9, caractérisé en ce que la vérification de l'intégrité du certificat consiste à vérifier l'intégrité du deuxième ensemble de données.

11. Procédé selon la revendication 9, caractérisé en ce que la vérification de l'intégrité du certificat consiste en outre à vérifier sa validité temporelle.

12. Prccédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la page web (14) est une page de résultats, fournie par un moteur de recherche (20), ou un site web affilié au moteur de recherche, en réponse à une requête (12) d'information reçue de l'utilisateur (10) comprenant un ou plusieurs mots clés associés à une annonce affichée sous forme d'hyperlien dans la page.

13. Système de validation de la sélection d'un d'hyperlien affiché dans une page web (14), caractérisé en ce qu'il comprend :

- des moyens de fourniture (20) de la page web à un utilisateur (10),
- un serveur de vérification (40), comprenant des moyens pour créer un certificat numérique (CCT) unique, sécurisé, associé à l'hyperlien affiché dans la page web,

les moyens de fourniture de la page web comprenant des moyens pour insérer à la volée le certificat dans l'hyperlien affiché dans la page web fournie à l'utilisateur,

le serveur de vérification comprenant en outre :

- des moyens de réception du certificat associé à l'hyperlien affiché, suite à la sélection par l'utilisateur de l'hyperlien dans la page web, activant une connexion vers un site web (30) correspondant à l'hyperlien,
- des moyens de vérification de l'intégrité du certificat associé à l'annonce, et
- des moyens de validation de la sélection de l'utilisateur comme étant légitime et pour établir la connexion de l'utilisateur au site web correspondant, en cas de succès de la vérification de l'intégrité du certificat.

14. Système selon la revendication 13, caractérisé en ce que le serveur de vérification comprend en outre :

- des moyens de récupération d'un module d'authentification associé à l'utilisateur, prévu pour conserver un historique d'un nombre de sélections

légitimes réalisées précédemment par l'utilisateur, en mémorisant pour chaque sélection légitime, le certificat correspondant,

- des moyens de détermination d'un niveau de confiance associé à l'utilisateur en fonction dudit historique, le niveau de confiance déterminé étant pris en compte par les moyens de validation de la légitimité de la sélection de l'utilisateur,
- des moyens de mise à jour du module d'authentification avec le certificat reçu et vérifié, et
- des moyens pour transmettre le module d'authentification mis à jour à l'utilisateur.

15. Système selon la revendication 14, caractérisé en ce que le serveur de vérification comprend des moyens de transmission du module d'authentification mis à jour vers le site web correspondant à l'hyperlien.

16. Système selon la revendication 15, caractérisé en ce que le site web correspondant à l'hyperlien comprend des moyens de sauvegarde (60) du module d'authentification mis à jour pour chaque sélection validée comme étant légitime.

17. Système selon l'une quelconque des revendications 14 à 16, caractérisé en ce que le serveur de vérification comprend des moyens de sauvegarde (50) du module d'authentification mis à jour pour chaque sélection validée comme étant légitime.

18. Système selon l'une quelconque des revendications 13 à 17, caractérisé en ce que le

certificat (CCT) unique associé à l'hyperlien affiché comprend un premier ensemble de données (TP) relatives à l'hyperlien et/ou au site web correspondant à l'hyperlien, un deuxième ensemble de données (CT) relatives à des données d'authentification du certificat et un troisième ensemble de données (HDT) relatives à une date d'expiration du certificat.

19. Système selon la revendication 18, caractérisé en ce que le premier ensemble de données est constitué par l'adresse URL du site web correspondant à l'hyperlien affiché.

20. Système selon la revendication 18 ou 19, caractérisé en ce que le deuxième ensemble de données est représenté par des collisions de fonction de hachage.

21. Système selon l'une quelconque des revendications 13 à 20, caractérisé en ce que les moyens de fourniture (20) de la page web comprennent un moteur de recherche ou un site web affilié au moteur de recherche, fournissant la page web (14) en réponse à une requête (12) d'information reçue de l'utilisateur (10) comprenant un ou plusieurs mots clés associés à une annonce affichée sous forme d'hyperlien dans la page fournie.

22. Serveur de vérification (40), caractérisé en ce qu'il comprend :

- des moyens pour créer un certificat numérique (CCT) unique, sécurisé, associé à un hyperlien affiché

dans une page web fournie à un utilisateur (10) par des moyens de fourniture (20) de pages web,

- des moyens de transmission du certificat (CCT) aux moyens de fourniture, prévus pour insérer à la volée le certificat dans l'hyperlien affiché la page web fournie,

- des moyens de réception du certificat associé à l'hyperlien affiché, suite à la sélection par l'utilisateur de l'hyperlien dans la page web, activant une connexion vers un site web (30) correspondant à l'hyperlien,

- des moyens de vérification de l'intégrité du certificat associé à l'annonce, et

- des moyens de validation de la sélection de l'utilisateur comme étant légitime et pour établir la connexion de l'utilisateur au site web correspondant, en cas de succès de la vérification de l'intégrité du certificat.

23. Serveur selon la revendication 22, caractérisé en ce qu'il comprend :

- des moyens de récupération d'un module d'authentification associé à l'utilisateur, prévu pour conserver un historique d'un nombre de sélections légitimes réalisées précédemment par l'utilisateur, en mémorisant pour chaque sélection légitime, le certificat correspondant,

- des moyens de détermination d'un niveau de confiance asscié à l'utilisateur en fonction dudit historique, le niveau de confiance déterminé étant pris en compte par les moyens de validation de la légitimité de la sélection de l'utilisateur,

- des moyens de mise à jour du module d'authentification avec le certificat reçu et vérifié, et
- des moyens pour transmettre le module d'authentification mis à jour à l'utilisateur.

24. Serveur de vérification selon les revendications 22 ou 23, caractérisé en ce qu'il comprénd des moyens de transmission du module d'authentification mis à jour vers le site web correspondant à l'hyperlien.

25. Serveur selon l'une quelconque des revendications 22 à 24, caractérisé en ce qu'il comprend des moyens de sauvegarde (50) du module d'authentification mis à jour pour chaque sélection validée comme étant légitime.

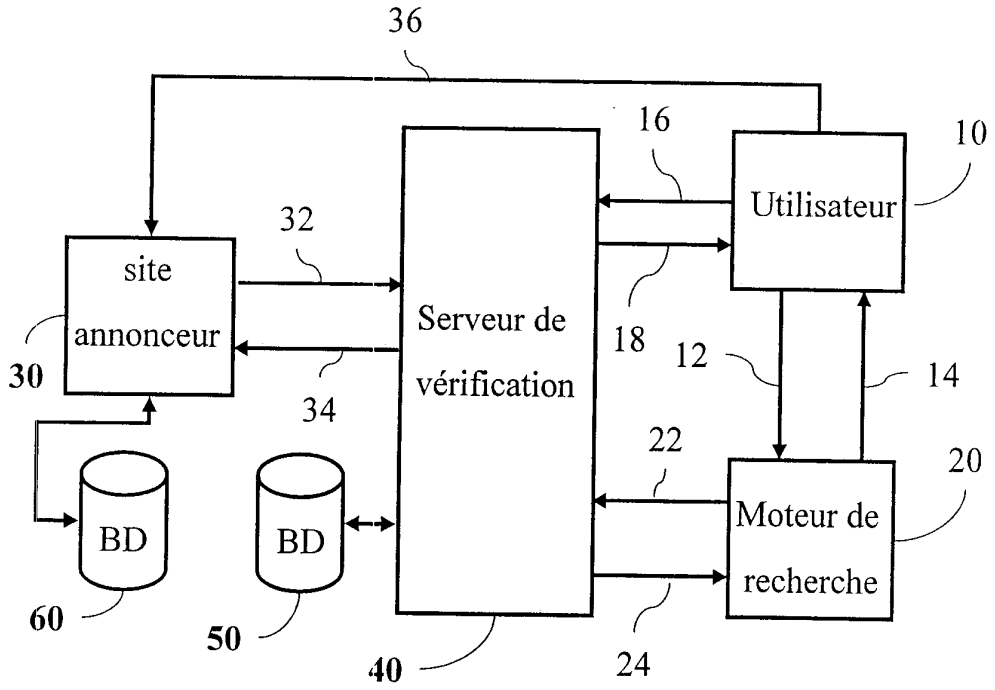

36
16
10
Utilisateur
32
site
annonceur
30
Serveur de
vérification
18
12
14
34
22
20
Moteur de
recherche
BD
BD
60
50
40
24

Fig.1

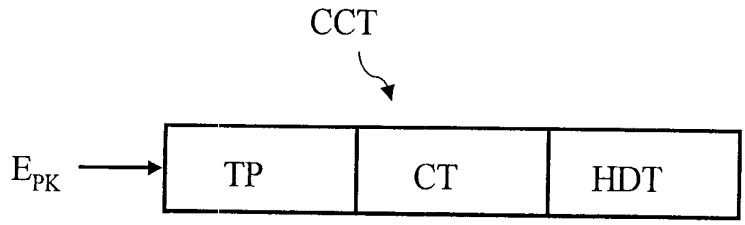

CCT
E_{PK}
TP
CT
HDT

Fig.2

RÉPUBLIQUE FRANÇAISE

2907941

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 685927
FR 0609427

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X Y	US 2006/136294 A1 (LINDEN JOHN [US] ET AL) 22 juin 2006 (2006-06-22) * alinéas [0038] - [0049], [0059] - [0061]; figure 3 * -----	1-7, 11-19, 21-25 8-10,20	G06Q30/00
Y	US 5 892 904 A (ATKINSON ROBERT G [US] ET AL) 6 avril 1999 (1999-04-06) * colonne 2, ligne 61 - colonne 3, ligne 40 * * colonne 6, ligne 59 - colonne 7, ligne 10; figures * -----	8-10,20	
A	US 2005/198536 A1 (BRICKELL ERNIE F [US] ET AL) 8 septembre 2005 (2005-09-08) * alinéas [0009] - [0028]; figures 1-3 * -----	1-25	
A	US 2004/153365 A1 (SCHNEIDER MELISSA [US] ET AL) 5 août 2004 (2004-08-05) * alinéas [0016] - [0020], [0023] * -----	1-5,13, 14,22,23	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06F H04L

Date d'achèvement de la recherche	Examinateur
20 avril 2007	Herry, Tzvetanka

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0609427 FA 685927

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 20-04-2007
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2006136294 A1	22-06-2006	AUCUN	
US 5892904 A	06-04-1999	AUCUN	
US 2005198536 A1	08-09-2005	US 6965881 B1	15-11-2005
US 2004153365 A1	05-08-2004	WO 2005094199 A2	13-10-2005

EPO FORM P0465