(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 104 867**

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

(21) **N° d'enregistrement national :** **19 14647**

(51) Int Cl[8] : ***H 04 L 9/08*** *(2019.12), G 06 F 21/44, H 04 L 9/28*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.12.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.06.21 Bulletin 21/24.

(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 :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES Etablissement Public* — FR.

(72) **Inventeur(s) :** LAURENT Frédéric et OLIVEREAU Alexis.

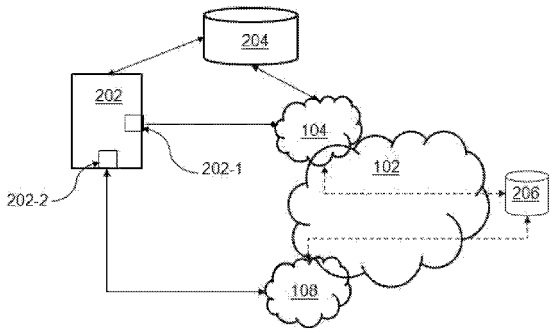
(73) **Titulaire(s) :** COMMISSARIAT A L'ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES Etablissement Public.

(74) **Mandataire(s) :** Marks & Clerk France.

(54) Procédé et dispositif de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation.

(57) L'invention concerne un dispositif et un procédé mis en œuvre par ordinateur de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation opérée par différents opérateurs, pour un utilisateur ayant des droits d'accès à la plateforme collaborative d'anonymisation par un premier opérateur ou fournisseur d'accès. Le procédé comprend les étapes de :- émettre une requête d'accès à la plateforme collaborative d'anonymisation pour accéder à un service de la plateforme ;- recevoir une liste de couples {Math 1 (PEi; Cléi)} où chaque couple contient un identifiant d'un point d'entrée PEi vers la plateforme pour le premier opérateur et une clé publique Cléi aléatoire générée pour le point d'entrée ;- générer de manière aléatoire, une valeur aléatoire privée X ; - sélectionner un premier couple (PE1, Clé1) opéré par le premier opérateur, et au moins un second couple (PE2, Clé2) opéré par un second opérateur ;- communiquer au premier opérateur via le point d'entrée PE1 sélectionné, une première clé privée (X x Clé2), et au second opérateur via le point d'entrée PE2 sélectionné, une seconde clé privée (X x Clé1) ; - mettre en œuvre sur la plateforme collaborative d'anonymisation, un algorithme de vérification et de validation de clés privées entre les deux opérateurs sur la base des premières et secondes clés privées; et- valider ou refuser à l'utilisateur l'accès à la plateforme collaborative d'anonymisation via le second opérateur.

Figure pour l'abrégé : Fig. 2.



FR 3 104 867 - A1

Description

Titre de l'invention : Procédé et dispositif de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation

[0001] L'invention se situe dans le domaine des protocoles de communication, et concerne plus particulièrement un procédé et un dispositif de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation.

[0002] La sécurité des données et l'accès contrôlé à divers systèmes collaboratifs sont des défis majeurs auxquels les organisations doivent faire face pour limiter les risques d'intrusion et d'attaques. Les plateformes collaboratives d'anonymisation existantes offrent peu ou pas de contrôle d'accès, et donc pas de sécurité en tant que tel.

[0003] Aujourd'hui les solutions de communication présentant les meilleurs niveaux de « privacy » (anglicisme pour anonymat) sont des solutions gratuites et collaboratives basées sur des protocoles pair-à-pair (P2P) comme les protocoles Tor (« *The Onion Router* ») ou I2P (« *Invisible Internet Project* »). Ces solutions ne requièrent aucun mécanisme d'authentification et d'accès particulier d'une part parce qu'elles sont gratuites, mais également et surtout parce que par nature, un mécanisme d'authentification et d'accès est a priori incompatible avec un haut niveau d'anonymisation.

[0004] Une solution améliorée décrite dans la demande de brevet FR3072238 de la Demanderesse, présente une plateforme collaborative d'anonymisation ayant un niveau de privacy et de sécurité potentiellement largement supérieur aux solutions existantes, mais aussi des performances en termes de qualité de service compatibles avec des usages Internet modernes et professionnels, tout en permettant de garder un certain contrôle sur les échanges afin de limiter des usages criminels de la plateforme.

[0005] L'ensemble de ces solutions décrivent le fonctionnement nominal du système global. Or, il est également nécessaire pour ne pas amoindrir l'intérêt de la plateforme d'anonymisation en mode nominal de garantir que l'anonymat ne soit pas compromis lors de la phase transitoire. Typiquement il y a lieu de permettre que l'accès à un service souhaité se fasse sans aucune compromission du niveau de privacy et de sécurité de l'utilisateur.

[0006] Par ailleurs, au-delà du seul accès à la plateforme, des services (restreints, voire commerciaux) souhaitant bénéficier de réelles propriétés d'anonymisation (i.e. de la couche réseau jusqu'à la couche applicative) peuvent être envisagés au-dessus de la plateforme, comme par exemple un service de traitement d'images pour la santé reposant sur un moteur d'intelligence artificielle hébergé dans un centre de calcul distant, ou des services de communication sécurisés de type « Telegram Messenger »

ou « Signal », ou encore des applications d'échange d'informations sur la fraude bancaire.

[0007] Il existe ainsi le besoin d'une solution qui permette de contrôler l'accès à une plateforme d'anonymisation collaborative sans compromettre l'anonymat du demandeur d'accès.

[0008] Un demandeur d'accès à une plateforme d'anonymisation collaborative peut s'appuyer sur plusieurs fournisseurs d'accès à cette plate-forme, qui sont dans le cas général plusieurs opérateurs de communication et au moins un opérateur du service d'anonymisation. Parmi les opérateurs de communication, l'un est supposé avoir octroyé les droits d'accès à la plateforme d'anonymisation collaborative, par exemple moyennant la souscription d'une option dans un contrat d'abonnement à un service d'accès à Internet. Comme l'utilisation de la plateforme d'anonymisation collaborative pour pouvoir être établie, requière des interactions entre le demandeur d'accès et les fournisseurs d'accès à cette plate-forme, il importe que ces interactions, tout en garantissant l'anonymat du demandeur d'accès, ne puissent s'effectuer que dans la mesure où celui-ci peut prouver qu'il s'est effectivement vu octroyer les droits d'accès à la plateforme collaborative.

[0009] Des solutions basées sur des mécanismes d'itinérance ou « roaming » en anglais, utilisées dans le secteur de la téléphonie mobile permettent à un opérateur tiers d'authentifier le client d'un opérateur d'origine sans pour autant connaître le secret à long terme qui est partagé entre le client et son opérateur d'origine pour le chiffrement des échanges. Ces mécanismes dans lesquels l'opérateur d'origine remet à l'opérateur tiers des éléments à échanger avec son client afin de l'autoriser ensuite à communiquer, permettent à l'usager d'un service s'étant vu octroyer les droits (dans l'exemple de la téléphonie, les droits pour un service de communication), de bénéficier de droits équivalents auprès d'un autre fournisseur de service, sans en être connu de la manière dont il était connu par son opérateur d'origine.

[0010] Ces mécanismes ne sont pas satisfaisants du point de vue de la problématique considérée, pour la raison principale qu'ils impliquent un dialogue direct en mode roaming et une connaissance mutuelle entre les deux opérateurs du client, i.e. l'opérateur réseau d'origine auprès duquel l'utilisateur a souscrit son abonnement et l'opérateur réseau tiers auprès duquel il demande à être connecté. Une connaissance mutuelle des deux opérateurs représente une faille potentielle inacceptable.

[0011] Une approche permettant de masquer l'auteur d'une transaction connue comme « Ring signatures » est décrite dans l'article 'How to leak a secret' de Ron Rivest, Adi Shamir, and Yael Tauman, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science, pages 552–565. Les « Ring Signatures » sont mises en œuvre en particulier dans le cadre de la cryptomonnaie « CryptoNote », et permettent de

masquer l'auteur d'une transaction parmi un ensemble de candidats. Bien qu'un homme du métier pourrait dériver une application de ce principe au contexte de l'invention où un opérateur ayant octroyé des droits d'accès à une plateforme à un utilisateur, camouflerait celui-ci via l'utilisation d'une ring signature construite sur la base de son identité et de celle de plusieurs autres clients candidats, cette solution ne serait pas généralisable car le nombre de candidats resterait relativement limité.

[0012] Par ailleurs, l'opérateur ayant octroyé les droits d'accès serait identifiable en tant qu'opérateur des différents clients candidats mentionnés dans la signature, ce qui représenterait une faille potentielle inacceptable.

[0013] Il existe ainsi le besoin d'une solution qui soit applicable à un grand nombre de clients d'un ou plusieurs fournisseurs de service et qui souhaitent se connecter à une plateforme d'anonymisation. Une telle solution doit protéger l'identité de tout opérateur ayant octroyé des droits d'accès.

[0014] Un autre mécanisme proche du roaming, est le mécanisme d'échange de type « Push » décrit dans la RFC 2904 qui permet à un client d'accéder à un service en prouvant au fournisseur de celui-ci l'existence d'une interaction passée avec un serveur d'autorisation. Bien qu'un homme du métier pourrait généraliser ce système avec un serveur d'autorisation qui ne remettrait pas la preuve d'interaction à l'utilisateur lui-même mais la stockerait dans une base de données éventuellement consultée par le fournisseur de service ultérieurement, un tel système n'offrirait pas de support pour l'anonymat des transactions.

[0015] Aussi, il existe le besoin d'une solution qui permette de préserver un anonymat total tant pendant la phase transitoire de connexion à une plateforme collaborative que pendant le mode nominal d'utilisation de la plateforme.

[0016] La présente invention permet de pallier les inconvénients des approches connues et de répondre aux besoins précités.

[0017] Ainsi, un objet de l'invention est de fournir une solution d'accès anonyme à une plateforme d'anonymisation.

[0018] Le principe général de l'invention est basé sur un mécanisme d'autorisation qui vise à autoriser l'accès à une plateforme collaborative d'anonymisation, de manière totalement anonyme, sécurisée et sans tiers de confiance, et/ou autoriser l'accès à un service nécessitant des propriétés d'anonymat reposant sur une telle plateforme.

[0019] Avantageusement, le mécanisme d'accès à une plateforme d'anonymisation repose sur un principe de distribution de rôles entre utilisateurs et opérateurs afin de s'affranchir d'un tiers de confiance, le tiers de confiance étant la limitation des solutions connues de privacy.

[0020] L'invention est particulièrement avantageuse pour compléter le fonctionnement en phase nominale de la plateforme collaborative d'anonymisation développée par la De-

manderesse et décrite dans la demande de brevet précitée, en apportant une solution pour la phase « transitoire » qui permet de garantir un anonymat total lors de la phase de connexion à la plateforme tout en proposant un mécanisme de contrôle d'accès à la plateforme.

[0021] L'invention s'applique avantageusement à tout service anonyme payant et/ou restreint, commercialisé et/ou offert par un ou des opérateurs d'une plateforme collaborative d'anonymisation. Ces services peuvent être de natures très diverses tels que : des bases de données financières pour garantir l'anonymat des utilisateurs (et par exemple ne pas dévoiler les secteurs ou les entreprises étudiés en vue d'investissements futurs), des services d'intelligence artificielle pour la « esanté » (où les traitements qui sont faits de manière déportée sur des centres de calculs qui connaissent les données (typiquement : images (radios, scanner…), les praticiens (docteur de ville, chirurgien), voire les individus directement, mettent en péril le secret médical).

[0022] Pour obtenir les résultats recherchés, il est proposé un procédé mis en œuvre par ordinateur de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation opérée par différents opérateurs, pour un utilisateur ayant des droits d'accès à la plateforme collaborative d'anonymisation par un premier opérateur ou fournisseur d'accès. Le procédé comprend les étapes de :

- émettre une requête d'accès à la plateforme collaborative d'anonymisation pour accéder à un service de la plateforme ;
- recevoir une liste de couples {(PEi; Cléi)} où chaque couple contient un identifiant d'un point d'entrée PEi vers la plateforme pour le premier opérateur et une clé publique Cléi aléatoire générée pour le point d'entrée ;
- générer de manière aléatoire, une valeur aléatoire privée X ;
- sélectionner un premier couple (PE1, Clé1) opéré par le premier opérateur, et au moins un second couple (PE2, Clé2) opéré par un second opérateur ;
- communiquer au premier opérateur via le point d'entrée PE1 sélectionné, une première clé privée (X x Clé2), et au second opérateur via le point d'entrée PE2 sélectionné, une seconde clé privée (X x Clé1) ;
- mettre en œuvre sur la plateforme collaborative d'anonymisation, un algorithme de vérification et de validation de clés privées entre les deux opérateurs sur la base des premières et secondes clés privées; et
- valider ou refuser à l'utilisateur l'accès à la plateforme collaborative d'anonymisation via le second opérateur.

[0023] Selon des modes de réalisation alternatifs ou combinés:

- l'étape de communication des clés privées comprend les étapes de :

calculer un premier nombre dit « premier nombre privé utilisateur » (X x Clé2) à

partir de la valeur aléatoire privée X et de la clé publique Clé2 associée au point d'entrée du second opérateur ; et

- calculer un second nombre dit « second nombre privé utilisateur » (X x Clé1) à partir de la valeur aléatoire privée X et de la clé publique Clé1 associée au point d'entrée du premier opérateur.

- l'étape de mise en œuvre sur la plateforme collaborative d'anonymisation, d'un algorithme de vérification et de validation de clés privées entre les deux opérateurs, comprend des étapes de :

- pour le premier opérateur :

- générer à partir du premier nombre privé utilisateur reçu et de la clé publique associée au point d'entrée du premier opérateur, un nombre dit « premier nombre privé utilisateur-opérateur » ((X x Clé2) x Clé1) ; et

- enregistrer via la plateforme collaborative d'anonymisation, le premier nombre privé utilisateur-opérateur ((X x Clé2) x Clé1) dans une base de données de clés privées ;

- pour le second opérateur :

- générer à partir du second nombre privé utilisateur reçu et de la clé publique associée au point d'entrée du second opérateur, un nombre dit « second nombre privé utilisateur-opérateur » ((X x Clé1) x Clé2) ; et

- vérifier via la plateforme collaborative d'anonymisation, si le second nombre privé utilisateur-opérateur » ((X x Clé1) x Clé2) est enregistré dans ladite base de données de clés privées.

- l'étape d'enregistrement dans la base de données de clés privées d'un nombre privé utilisateur-opérateur, comprend de plus l'enregistrement d'un paramètre de durée de vie dudit nombre.

- le procédé comprend de plus après l'étape d'enregistrement une étape de décomptage du paramètre de durée de vie.

- l'étape de sélection des couples est faite de manière automatique selon des critères de sélection prédéfinis.

- les clés privées sont obtenues par une opération de chiffrage prédéfinie transitive et commutative.

- l'opération de chiffrage est une opération de type élévation à une puissance modulaire.

- l'opération de chiffrage est une opération dite « one-way accumulators».

[0024] L'invention couvre un produit programme d'ordinateur comprenant des instructions de code non transitoire permettant d'effectuer les étapes du procédé revendiqué, lorsque le programme est exécuté sur un ordinateur.

[0025] L'invention couvre de plus un dispositif de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation opérée par différents opérateurs, pour un uti-

lisateur ayant des droits d'accès à la plateforme collaborative d'anonymisation par un premier opérateur ou fournisseur d'accès, le dispositif comprend des moyens pour mettre en œuvre les étapes du procédé selon l'une quelconque des revendications.

[0026] D'autres caractéristiques, détails et avantages de l'invention ressortiront à la lecture de la description faite en référence aux dessins annexés donnés à titre d'exemple et qui représentent, respectivement :

[0027] [fig.1] est une représentation topologique d'une infrastructure permettant d'implémenter l'invention;

[0028] [fig.2] illustre une représentation d'un exemple de mise en œuvre de l'invention selon la topologie de la figure 1;

[0029] [fig.3] illustre les procédures exécutées entre les entités de la figure 2 dans un mode de réalisation de l'invention; et

[0030] [fig.4] illustre les étapes opérées par la méthode de l'invention dans un mode de réalisation.

[0031] La figure 1 illustre un environnement général 100 dans lequel l'invention est implémentée avantageusement par exemple tel qu'illustré par la figure 2. L'environnement comprend une plateforme collaborative d'anonymisation 102 (aussi désignée comme service « anonyme ») qui est opérée de manière collaborative par au moins trois opérateurs indépendants dont au moins deux opérateurs indépendants (104, 108) sont utilisés pour accéder à la plateforme.

[0032] Pour s'affranchir d'un tiers de confiance, la plateforme a besoin d'au moins trois opérateurs indépendants. Dans le contexte de l'invention décrit, une connexion au service d'anonymisation pour se connecter à la plateforme d'anonymisation de manière anonyme, requière la connexion à au moins deux opérateurs indépendants (OP1, OP2).

[0033] Le service anonyme peut être un service réseau ou un service applicatif, pour lequel un utilisateur/client bénéficie d'un droit d'accès octroyé par un des opérateurs de la plateforme collaborative d'anonymisation. Dans un mode de réalisation, l'opérateur est le fournisseur de service internet (ISP) (« Internet Service Provider » en anglais) du client.

[0034] Le dispositif client pour accéder au service anonyme comprend au moins deux interfaces physiques (202-1, 202-2) connectées chacune à un opérateur réseau (104, 108), dont l'ISP du client.

[0035] Pour des raisons de simplicité de description et non de limitation de l'invention, bien que les exemples des figures 1 et 2 ne montrent qu'un nombre fini d'opérateurs (104, 108), l'homme du métier peut étendre les principes décrits à une pluralité d'opérateurs tout en apportant des modifications et/ou des variantes d'implémentation résultant de la généralisation. Ainsi le dispositif client peut avoir une seule ou plus que deux interfaces physiques pour établir une ou plus que deux connexions avec une pluralité

d'opérateurs.

[0036] Dans un mode de réalisation de l'invention dite au niveau logique, c'est-à-dire quand la connexion à deux opérateurs de la plateforme est faite via une unique interface réseau physique, le service anonyme s'appuie alors sur un service d'anonymisation au niveau réseau qui présente les deux caractéristiques précédentes (connexion à deux opérateurs indépendants et droit d'accès accordé). Dans ce cas-là, le client peut se connecter de manière logique (et non physique) à deux opérateurs de la plateforme d'anonymisation.

[0037] Revenant à la figure 1, les opérateurs réseaux présentent chacun des points d'entrée PEi sur la plateforme 102. Chaque PEi est opéré par un des opérateurs de la plateforme collaborative d'anonymisation. Ainsi par exemple, le premier opérateur OP1 104, qui pour la suite de la description est désigné comme étant l'opérateur historique ou fournisseur d'accès internet ISP du client 202 (ou encore le fournisseur du service applicatif anonyme), gère des points d'entrée à la plateforme (106-1 à 106-i), et le second opérateur OP2 108 gère des points d'entrée à la plateforme (110-1 à 110-j).

[0038] La figure 2 illustre de plus une base de données ou registre de données 204 de clés publiques (Reg._clés_publiques) auquel le dispositif client accède lors de la mise en œuvre du procédé de connexion, et une base de données (AC) de clés privées 206 couplée aux opérateurs 104, 108 et utilisée comme base de données temporaire pendant le processus de connexion anonyme.

[0039] Chaque point d'entrée opérateur (PEi) à la plateforme collaborative d'anonymisation génère de manière aléatoire une clé publique (Cléi), pouvant ou non être mise à jour, et qui est stockée dans la base de données publique 204. La base contient ainsi un ensemble de couples « point d'entrée, clé publique » {(PEi; Cléi)}. Une telle base est accessible directement via le fournisseur d'accès à internet ou via la plateforme collaborative d'anonymisation pour le mode de réalisation de l'invention au niveau applicatif.

[0040] Dans un mode de réalisation où les clés sont mises à jour, des attributs additionnels bien connus de l'homme de l'art peuvent être ajoutés aux couples « point d'entrée, clé publique », comme par exemple une durée de vie (« Time-To-Live » en anglais (TTL)) indiquant le temps pendant lequel les clés sont conservées.

[0041] Les figures 3 et 4 décrivent une mise en œuvre du procédé de l'invention selon un mode de réalisation, où la figure 3 montre les flux existants entre les différentes entités de la figure 2 et où la figure 4 illustre les étapes de la méthode de l'invention impliquant deux opérateurs.

[0042] Il est à noter que les mêmes références sont reprises sur les différentes figures pour les éléments identiques.

[0043] Le principe général de connexion anonyme d'un client 202 à une plateforme colla-

borative d'anonymisation 102, consiste au niveau du client en ce qu'il :

- 300 : récupère l'ensemble des couples point d'entrée, clés publique {(PEi; Cléi)} contenus dans le registre public 204;
- 302 : génère de manière aléatoire une valeur aléatoire privée X ;
- 304 : envoie respectivement à chaque opérateur sélectionné ISP et OP2, via un de ses points d'entrée, un nombre dit « nombre privé utilisateur » (X x Clé2) et (X x Clé1), calculé à partir de la valeur aléatoire privée X et de la clé publique associée au point d'entrée de l'autre opérateur; et
- 310 : reçoit du second opérateur OP2 une autorisation d'accéder à la plateforme 102 (ou un rejet).

[0044] Par ailleurs, le procédé comprend des phases réalisées au niveau de chaque opérateur indépendant, et qui consistent en ce que :

- 306 : le premier opérateur (ISP) enregistre via la plateforme collaborative d'anonymisation, dans la base de données de clés privées 206, un nombre dit « nombre privé utilisateur-opérateur » ((X x Clé2) x Clé1), généré à partir du nombre privé utilisateur calculé pour cet opérateur et de la clé publique associée au point d'entrée de cet opérateur ; et
- 308 : le second opérateur OP2 vérifie via la plateforme collaborative d'anonymisation, si un « nombre privé utilisateur-opérateur » ((X x Clé1) x Clé2), généré à partir du nombre privé utilisateur calculé pour cet opérateur et de la clé publique associée au point d'entrée de cet opérateur, est stocké dans la base de données de clés privées 206, afin de renvoyer ou non une autorisation d'accès à l'utilisateur.

[0045] La figure 4 illustre les étapes du procédé 400 de connexion anonyme de l'invention. Le procédé débute quand un utilisateur/client qui dispose de droits d'accès à une plateforme collaborative d'anonymisation via son opérateur historique (en général l'ISP, son fournisseur d'accès à internet), souhaite accéder à un service opéré sur la plateforme collaborative d'anonymisation par un opérateur OP2 ou par un autre opérateur. L'utilisateur émet une requête d'accès 402 vers son opérateur. Le procédé permet ensuite que le client reçoive 404 une liste de couples {(PEi; Cléi)} où chaque couple contient un identifiant d'un point d'entrée vers la plateforme par un opérateur et une clé publique associée au point d'entrée.

[0046] Dans une étape suivante 406, le procédé permet de générer de manière aléatoire une valeur privée X, et permet à l'utilisateur de sélectionner 408 un premier point d'entrée PE1 opéré par son ISP, et un second point d'entrée PE2 opéré par le second opérateur. Dans un mode de réalisation alternatif, l'ordre des étapes 406 et 408 peut être inversé. La sélection du point d'entrée pour chaque opérateur peut être selon des variantes de réalisation, soit discrétionnaire, soit automatisé selon des critères prédéfinis.

[0047] Dans une étape suivante 410, le procédé permet de générer pour chaque point

d'entrée sélectionné, un 'nombre privé utilisateur' définissant une clé privée. Chaque nombre privé utilisateur est généré à partir de la valeur aléatoire privée X et de la clé publique associée à l'autre point d'entrée sélectionné pour l'autre opérateur. Ainsi, pour le premier point d'entrée PE1 de l'opérateur historique, un premier nombre privé utilisateur (X x Clé2) est généré définissant une clé privée utilisateur côté premier opérateur, et pour le second point d'entrée PE2 du second opérateur, un second nombre privé utilisateur (X x Clé1) est généré définissant une seconde clé privée utilisateur côté second opérateur.

[0048] Dans un mode de réalisation avantageux, l'opération de chiffrage désignée par "x" pour la génération des nombres privés utilisateurs, est une opération de chiffrage prédéfinie telle que son opération inverse (i.e. retrouver 'a' et 'b' à partir de 'a x b') est extrêmement difficile à obtenir. Cette opération doit également être à la fois transitive et commutative.

[0049] Dans un mode de réalisation préférentielle, l'opération "x" est une fonction connue d'élévation à une puissance modulaire.

[0050] Dans une variante de réalisation, l'opération 'x' appliquée est connue par l'homme du métier selon l'anglicisme « accumulators », et peut être basée sur les « Merkle trees », et les « non-Merkle accumulators » qui peuvent par exemple être de type « RSA accumulators » ou « Elliptic Curve accumulators ».

[0051] Un exemple d'opération 'x' basée sur les « accumultairs » est décrite dans l'article de J. Benaloh and M. de Mare, « One-way accumulators: A decentralized alternative to digital signatures », Advances in Cryptology-Eurocrypt'93, LNCS, vol. 765, Springer-Verlag, 1993, pp. 274–285.).

[0052] Dans une étape suivante 412, le procédé permet de communiquer à chaque opérateur (l'ISP et le second opérateur) le nombre privé utilisateur lui correspondant. Ainsi dans l'exemple illustré, le procédé permet d'envoyer au premier opérateur 104, le nombre privé utilisateur (X x Clé2) généré à partir de la clé publique Clé2 associée à l'autre point d'entrée sélectionné pour l'autre opérateur, et d'envoyer au second opérateur 106, le nombre privé utilisateur (X x Clé1) généré à partir de la clé publique Clé1 associée au point d'entrée sélectionné pour l'opérateur ISP.

[0053] L'étape suivante 414 consiste sur la plateforme collaborative d'anonymisation, en la vérification et validation des clés privées. Particulièrement, le procédé permet que le premier opérateur ISP ajoute 306 dans la base de données privée (AC), accessible uniquement au travers de la plateforme collaborative d'anonymisation, un nombre 'privé utilisateur-opérateur' ((X x Clé2) x Clé1) définissant une clé privée utilisateur-premier opérateur, et généré par l'opération de chiffrage x à partir du nombre privé utilisateur reçu de l'utilisateur - (X x Clé2) - et de la clé - (Clé1) - associée au point d'entrée choisi pour le premier opérateur.

[0054] Dans une variante de réalisation, l'enregistrement du nombre 'privé utilisateur-opérateur' dans la base de données privée (AC) est associé à l'enregistrement d'un paramètre de durée de vie prédéfini. Ceci permet avantageusement un nettoyage automatique de la base de données privée (AC) suite par exemple à des tentatives de connexion infructueuses, ce qui permet d'éviter une croissance continue et inutile du contenu de la base.

[0055] L'étape 414 consiste de plus en ce que le second opérateur OP2 interroge 308, via la plateforme collaborative d'anonymisation, la base de données privée (AC) pour vérifier s'il y est enregistré un nombre privé utilisateur-opérateur - ((X x Clé1) x Clé2) - définissant une clé privée utilisateur-second opérateur, et généré par l'opération de chiffrage x à partir du nombre privé utilisateur reçu de l'utilisateur - (X x Clé1) - et de la clé (Clé2) associée au point d'entrée choisi pour le second opérateur.

[0056] Si le résultat de la vérification est positif, le procédé permet dans une étape suivante 416, d'envoyer à l'utilisateur une autorisation d'accès à la plateforme collaborative d'anonymisation. En effet, si à l'étape de vérification, le second opérateur reçoit une confirmation de l'existence de la clé privée dans la base de données privée (AC), cette information indique qu'une transaction passée a déjà eu lieu entre ce même utilisateur et un opérateur (i.e. l'opérateur historique), et le second opérateur peut donc autoriser l'utilisateur à accéder à la plateforme collaborative d'anonymisation via son réseau.

[0057] Ainsi avantageusement, le procédé de l'invention permet de garantir que :

- ni l'opérateur initial ayant octroyé les droits d'accès à la plateforme au client/utilisateur, ni le service d'anonymisation, ni le second opérateur (ou plus généralement ni les autres opérateurs) que le client utilise pour accéder à la plateforme d'anonymisation, ne sont en mesure de « casser » l'anonymisation, c'est-à-dire qu'aucun n'est en mesure par une analyse réseau des requêtes de connexion au service, d'associer à l'utilisateur du service, des données permettant son identification ;
- l'opérateur ayant octroyé les droits d'accès au client/utilisateur ne sera pas en mesure de connaître le ou les autres opérateurs utilisés par le client pour accéder à la plateforme d'anonymisation ;
- le second ou tous les autres opérateurs ne seront pas en mesure de connaître l'opérateur initial ayant octroyé les droits d'accès au client/utilisateur, ce qui est une différence majeure avec les mécanismes de « roaming » utilisés par exemple en téléphonie mobile ;
- la plateforme réseau ou la logique d'anonymisation ne sera pas en mesure de savoir quels opérateurs sont utilisés par le client : rien d'autre ne peut être déduit que l'information qu'une nouvelle connexion légitime à la plateforme a eu lieu.

[0058] L'exemple a été décrit sur la base de deux opérateurs, mais le procédé est applicable et généralisable pour une pluralité d'opérateurs, permettant en fonction des propriétés

de la plateforme d'anonymisation collaborative de renforcer le degré d'anonymat de l'utilisateur.

[0059] Ainsi, l'homme du métier peut dériver la généralisation selon le scénario suivant, similaire à celui décrit pour deux opérateurs :

- après avoir sélectionné 'n' couples (Point d'entrée (PEn) ; Clé (Clén)) d'opérateurs différents, parmi un ensemble de couples existant dans une base de donnée publique, les points d'entrée offrant un accès à une plateforme collaborative d'anonymisation par une pluralité d'opérateurs, et où chaque opérateur peut avoir un nombre identique ou différent de points d'entrée, un utilisateur envoie (i.e. le procédé permet d'envoyer depuis le dispositif client) à un premier point d'entrée PE1 sélectionné pour un premier opérateur (i.e. généralement l'opérateur historique du client ISP), un premier nombre privé utilisateur - ((X x Clé2 x …x Clén) - construit à partir d'une valeur aléatoire X et des clés associées aux 'n-1' points d'entrée sélectionnés pour les autres opérateurs ;

- le premier opérateur inscrit dans la base de données privée du dispositif de l'invention couplée à la plateforme, un enregistrement d'un nombre privé utilisateur-opérateur - ((X x Clé2 x…x Clén) x Clé1) – construit à partir du premier nombre privé utilisateur - ((X x Clé2 x …x Clén) - et de la clé - Clé1 - associée au premier point d'entrée PE1 ;

- l'utilisateur envoie à un point d'entrée PE2 d'un second opérateur, un second nombre privé utilisateur - (X x Clé1 x Clé3 x … x Clén) - construit à partir de la valeur aléatoire X et des clés associées aux 'n-1' points d'entrée sélectionnés pour les autres opérateurs ;

- le second opérateur OP2 interroge la base de données privée pour savoir si un enregistrement existe pour un nombre privé utilisateur-opérateur - ((X x Clé1 x Clé3 x … x Clén) x Clé2) - construit à partir du second nombre privé utilisateur - (X x Clé1 x Clé3 x … x Clén) - et de la clé - Clé2 - associée au point d'entrée PE2 du second opérateur ;

- l'utilisateur obtient une validation d'accès ou un refus d'accès à la plateforme collaborative d'anonymisation via le second opérateur.

- puis itérativement : l'utilisateur envoie pour chaque autre point d'entrée sélectionné jusqu'au nième - PEn - un nombre privé utilisateur correspondant - (X x Clé1 x … x Clén-1) - et chaque opérateur respectif interroge la base de données privées pour vérifier l'existence d'un nombre privé utilisateur-opérateur correspondant - ((X x Clé1 x … x Clén-1) x Clén) - et accorder ou refuser l'accès à la plateforme via l'opérateur correspondant.

[0060] Dans un autre mode de réalisation de l'invention, le premier opérateur peut inscrire dans la base de données privée l'enregistrement du nombre privé utilisateur-opérateur avec un paramètre de durée de vie (TTL) pour le nombre 'n'. Un compteur permet de décompter le paramètre TTL à chaque interrogation positive de la base de données par

un autre opérateur, afin que lorsque l'ensemble des 'n' points d'entrée a été vérifié le TTL est à zéro. La base de données privée d'accès peut effacer l'enregistrement.

[0061] L'invention décrite peut s'implémenter à partir d'éléments matériel et/ou logiciel. Elle peut être disponible en tant que produit programme d'ordinateur exécuté par un processeur qui comprend des instructions de code pour exécuter les étapes du procédé dans les différents modes de réalisation.

Revendications

[Revendication 1] Un procédé, mis en œuvre par ordinateur, de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation opérée par différents opérateurs (104, 108), pour un utilisateur (202) ayant des droits d'accès à la plateforme collaborative d'anonymisation par un premier opérateur ou fournisseur d'accès, le procédé comprenant les étapes suivantes :
- émettre (402) une requête d'accès à la plateforme collaborative d'anonymisation pour accéder à un service de la plateforme ;
- recevoir (404) une liste de couples (PEi; Cléi) où chaque couple contient un identifiant d'un point d'entrée PEi vers la plateforme pour le premier opérateur et une clé publique Cléi aléatoire générée pour le point d'entrée ;
- générer (406) de manière aléatoire, une valeur aléatoire privée X ;
- sélectionner (408) un premier couple (PE1, Clé1) opéré par le premier opérateur, et au moins un second couple (PE2, Clé2) opéré par un second opérateur ;
- communiquer (412) au premier opérateur via le point d'entrée PE1 sélectionné, une première clé privée (X x Clé2), et au second opérateur via le point d'entrée PE2 sélectionné, une seconde clé privée (X x Clé1) ;
- mettre en œuvre (414) sur la plateforme collaborative d'anonymisation, un algorithme de vérification et de validation de clés privées entre les deux opérateurs sur la base des premières et secondes clés privées; et
- valider (416) ou refuser à l'utilisateur l'accès à la plateforme collaborative d'anonymisation via le second opérateur.

[Revendication 2] Le procédé selon la revendication 1 dans lequel l'étape de communication des clés privées comprend les étapes (410) de :
- calculer un premier nombre dit « premier nombre privé utilisateur » (X x Clé2) à partir de la valeur aléatoire privée X et de la clé publique Clé2 associée au point d'entrée du second opérateur ; et
- calculer un second nombre dit « second nombre privé utilisateur » (X x Clé1) à partir de la valeur aléatoire privée X et de la clé publique Clé1 associée au point d'entrée du premier opérateur.

[Revendication 3] Le procédé selon la revendication 1 ou 2 dans lequel l'étape de mise en œuvre (414) sur la plateforme collaborative d'anonymisation, d'un algorithme de vérification et de validation de clés privées entre les deux opérateurs, comprend des étapes de :

- (306) pour le premier opérateur :
- générer à partir du premier nombre privé utilisateur reçu et de la clé publique associée au point d'entrée du premier opérateur, un nombre dit « premier nombre privé utilisateur-opérateur » ((X x Clé2) x Clé1) ; et
- enregistrer via la plateforme collaborative d'anonymisation, le premier nombre privé utilisateur-opérateur ((X x Clé2) x Clé1) dans une base de données de clés privées (206) ;
- (308) pour le second opérateur :
- générer à partir du second nombre privé utilisateur reçu et de la clé publique associée au point d'entrée du second opérateur, un nombre dit « second nombre privé utilisateur-opérateur » ((X x Clé1) x Clé2) ; et
- vérifier via la plateforme collaborative d'anonymisation, si le second nombre privé utilisateur-opérateur » ((X x Clé1) x Clé2) est enregistré dans ladite base de données de clés privées (206).

[Revendication 4] Le procédé selon la revendication 3 dans lequel l'étape d'enregistrement dans la base de données de clés privées d'un nombre privé utilisateur-opérateur, comprend de plus l'enregistrement d'un paramètre de durée de vie dudit nombre.

[Revendication 5] Le procédé selon la revendication 4 comprenant de plus après l'étape d'enregistrement une étape de décomptage du paramètre de durée de vie.

[Revendication 6] Le procédé selon l'une quelconque des revendications 1 à 5 dans lequel l'étape de sélection des couples est faite de manière automatique selon des critères de sélection prédéfinis.

[Revendication 7] Le procédé selon l'une quelconque des revendications 1 à 6 dans lequel les clés privées sont obtenues par une opération de chiffrage prédéfinie transitive et commutative.

[Revendication 8] Le procédé selon la revendication 7 dans lequel l'opération de chiffrage est une opération de type élévation à une puissance modulaire.

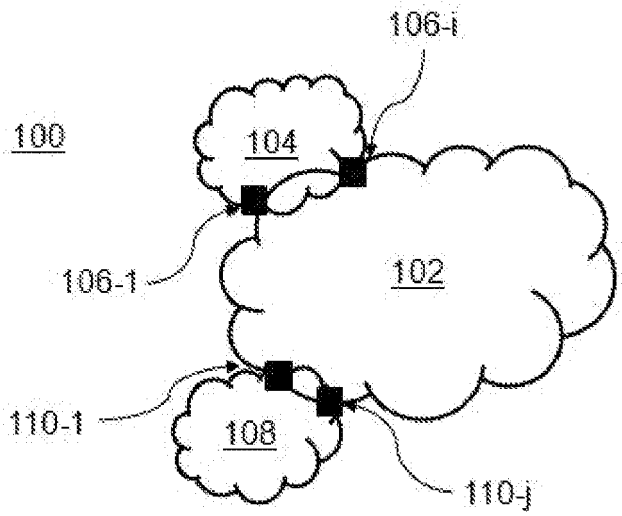
[Revendication 9] Le procédé selon la revendication 7 dans lequel l'opération de chiffrage est une opération dite « one-way accumulators ».

[Revendication 10] Un produit programme d'ordinateur, ledit programme d'ordinateur comprenant des instructions de code non transitoire permettant d'effectuer les étapes du procédé selon l'une quelconque des revendications 1 à 9, lorsque ledit programme est exécuté sur un ordinateur.

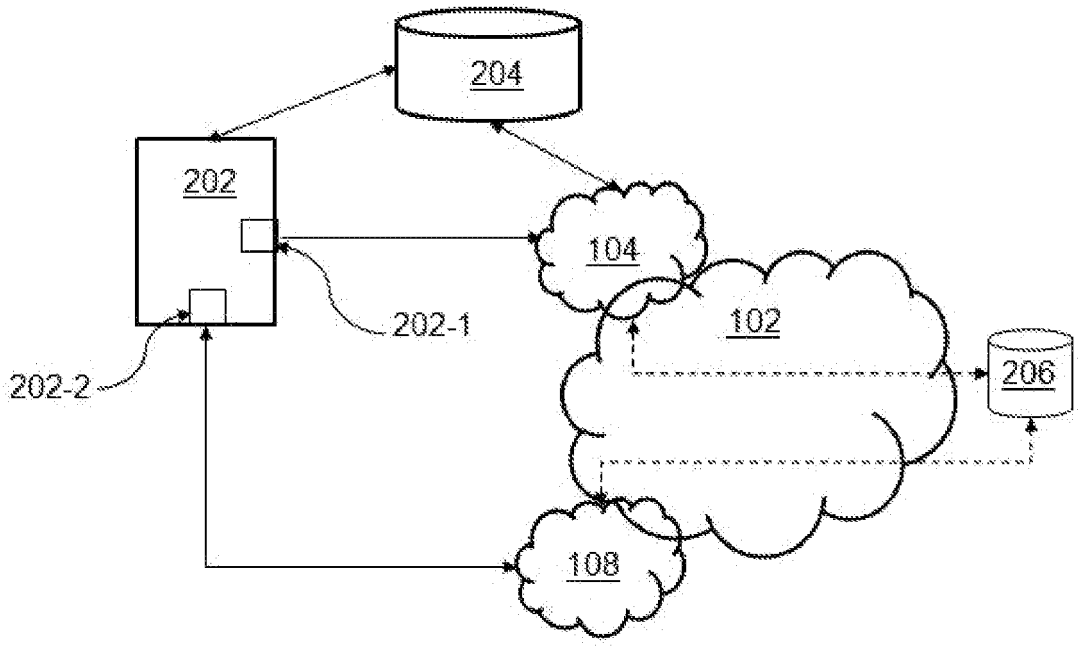
[Revendication 11] Un dispositif de contrôle d'accès anonyme à une plateforme collaborative d'anonymisation opérée par différents opérateurs (104, 108), pour un utilisateur (202) ayant des droits d'accès à la plateforme colla-

borative d'anonymisation par un premier opérateur ou fournisseur d'accès, le dispositif comprenant des moyens pour mettre en œuvre les étapes du procédé selon l'une quelconque des revendications 1 à 9.

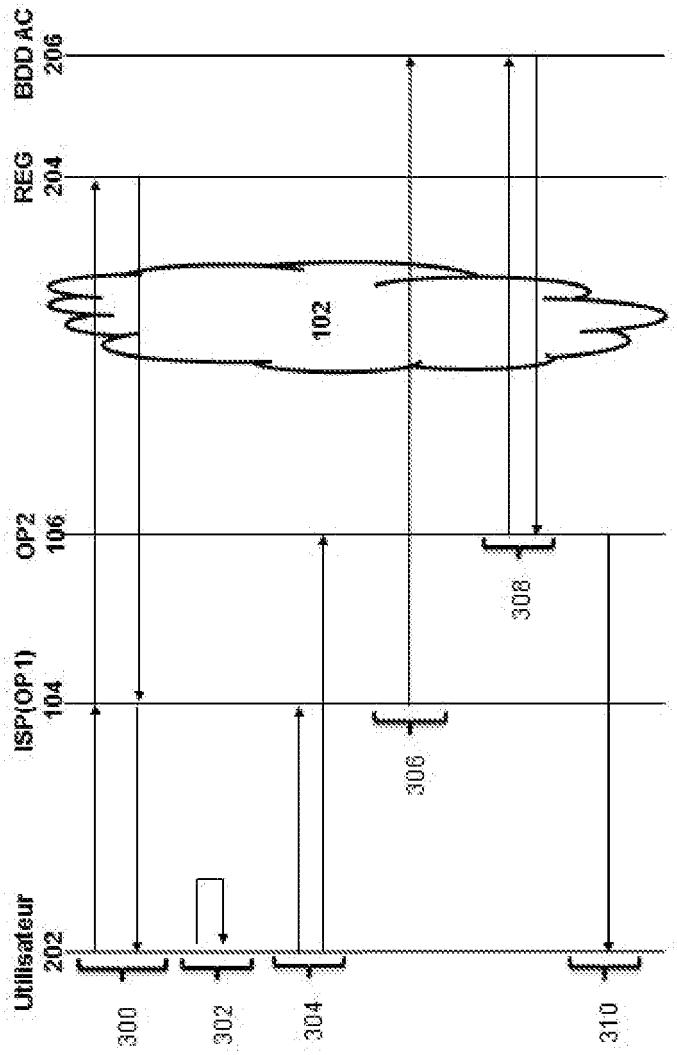
[Fig. 1]


106-i
100
104
106-1
102
110-1
108
110-j

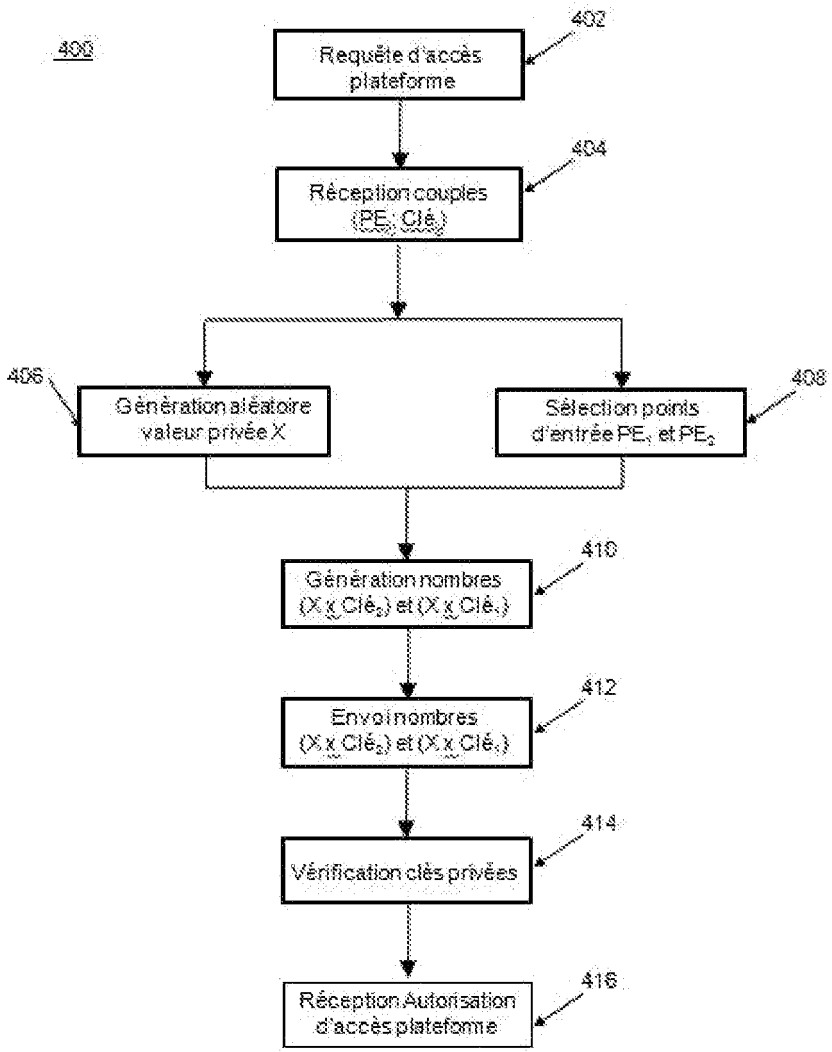
[Fig. 2]


204
202
104
202-1
102
206
202-2
108

[Fig. 3]


BDD AC
206
REG
204
102
OP2
106
308
ISP(OP1)
104
306
Utilisateur
202
300
302
304
310

[Fig. 4]


400
Requête d'accès plateforme
402
Réception couples (PE, Clé)
404
Génération aléatoire valeur privée X
406
Sélection points d'entrée PE1 et PE2
408
Génération nombres (X x Clé2) et (X x Clé1)
410
Envoi nombres (X x Clé2) et (X x Clé1)
412
Vérification clés privées
414
Réception Autorisation d'accès plateforme
416

RÉPUBLIQUE FRANÇAISE

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 878074
FR 1914647

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	Jaegwan Park ET AL: "Wireless Authentication Protocol Preserving User Anonymity", , 1 mars 2001 (2001-03-01), XP055714536, Extrait de l'Internet: URL:https://pdfs.semanticscholar.org/e49f/ab6ac42da5d14337bb8f00a63306299b88f1.pdf [extrait le 2020-07-14] * abrégé * * section 3.4 * * figure 4 * -----	1-11	H04L9/08 G06F21/44 H04L9/28
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L

Date d'achèvement de la recherche	Examinateur
12 août 2020	Yamajako-Anzala, A

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)